



Andalucía Emprende, Fundación Pública Andaluza
**CONSEJERÍA DE EMPLEO,
FORMACIÓN Y TRABAJO AUTÓNOMO**

LOPD

LA PROTECCIÓN DE LOS DATOS EN LAS EMPRESAS

*La prudencia consiste en la elección de lo que hay que hacer
y no hacer. Averroes.*



MANUAL DE LOPD

ÍNDICE

1. INTRODUCCIÓN	3
2. MARCO NORMATIVO	4
3. CONCEPTOS Y DEFINICIONES TRANSVERSALES EN LA LOPD	6
4. PRINCIPIOS GENERALES	13
5. DERECHOS DE LAS PERSONAS: DERECHOS ARCO	22
6. TRATAMIENTO PARA ACTIVIDADES DE PUBLICIDAD Y PROSPECCIÓN COMERCIAL. MARKETING PUBLICITARIO	28
7. LOS TIPOS DE FICHEROS: PÚBLICOS Y PRIVADOS	32
8. MEDIDAS DE SEGURIDAD	46
9. PREGUNTAS FRECUENTES Y RESOLUCIÓN DE DUDAS	51
10. ENLACES DE ORGANISMOS DE PROTECCIÓN DE DATOS.....	83
11. FORMULARIOS	86



1. INTRODUCCIÓN

Este manual tiene como finalidad esclarecer y ayudar a las empresas y a los emprendedores a profundizar en el conocimiento de la protección de datos en las empresas andaluzas.

Andalucía Emprende es una Fundación de la Junta de Andalucía, dependiente de la Consejería de Economía, Innovación, Ciencia y Empleo, cuya principal misión es contribuir al fortalecimiento de la actividad económica y al desarrollo empresarial de Andalucía, fomentando la cultura emprendedora, y la creación y consolidación de empresas y empleo en cualquier punto de la región.

Bajo estas premisas se ha elaborado este manual con la intención de ayudar a las empresas y a los emprendedores en una materia específica como la Protección de Datos de Carácter Personal que ha sufrido en los últimos años un desarrollo normativo en distintos ámbitos.

La Constitución Española, en su Título I “De los derechos y deberes fundamentales”, Capítulo II “Derechos y libertades” y artículo 18 garantiza el derecho al honor, a la intimidad personal y familiar, y a la propia imagen. En el apartado cuarto, se establece la necesidad de proteger estos derechos fundamentales, disponiendo que:

“La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”.

Como desarrollo legislativo de este mandato constitucional se promulgó la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal, más conocida como LORTAD (hoy no se encuentra vigente).

Posteriormente, en el marco de la Unión Europea, se promulgó la Directiva 95/46/CEE relativa a la protección de las personas físicas para el tratamiento de los datos personales y la libre circulación de éstos, cuya finalidad era armonizar la legislación de los países miembros de la Unión en materia de



protección de datos, garantizando, la protección y el respeto en todos los países de la Unión de este derecho fundamental del individuo. En esta Directiva, se recogen los principios mínimos que todos los países de la Unión Europea deberían garantizar en su legislación nacional interna para armonizarlos.

Al ser normativa europea de obligado cumplimiento, el Reino de España promulgó la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD), que supone la transposición de la Directiva 95/46/CE al derecho interno de nuestro país.

Siguiendo con esta exposición, el siguiente hito en la materia lo marca el Tribunal Constitucional en su sentencia 292/2000, al reconocer la protección de datos de carácter personal como un derecho constitucionalmente autónomo e independiente a la intimidad, siguiendo así el camino iniciado en la Carta de Derechos Fundamentales de la Unión Europea firmada en Niza el 7 de diciembre de 2000, cuyo artículo 8 establece que toda persona tiene derecho a la protección de los datos de carácter personal. Es por ello que el Tribunal Constitucional indica que este derecho está incardinado con el resto de los derechos fundamentales. Las consecuencias que se derivan de la cualidad de derecho fundamental son muy relevantes pues:

- a) Se considera irrenunciable.
- b) Su desarrollo se debe hacer por Ley Orgánica.
- c) Prevalece sobre el ejercicio de otros derechos no fundamentales.
- d) Posee una protección reforzada, pudiendo ejercitarse ante los Tribunales Ordinarios y ante el Tribunal Constitucional.

El siguiente paso fue la entrada en vigor del Real Decreto por el que se aprueba el Reglamento de Desarrollo de la LO 15/1999, de 13 de diciembre de 2008 de Protección de datos de Carácter Personal (en adelante RDLOPD).

Se puede identificar que el principal objetivo del RDLOPD es dotar de seguridad jurídica y contribuir a resolver las dudas interpretativas existentes.

Por otro lado, la gestión de los datos personales es un activo importante para cualquier empresa, por lo que gestionarlos de manera eficiente y segura es fundamental en la Sociedad actual y reporta al cliente, al proveedor y al empleado una tranquilidad y garantía de saber hacer empresarial que es muy beneficiosa.

2 MARCO NORMATIVO

El marco normativo en materia de protección de datos se recoge en las siguientes normas:

- a) Constitución Española: Como se ha indicado anteriormente, su Título I “De los derechos y deberes fundamentales”, Capítulo II “Derechos y libertades” y artículo 18 garantiza el derecho al honor, a la intimidad personal y familiar, y a la propia imagen. En el apartado cuarto, se establece la necesidad de proteger estos derechos fundamentales, disponiendo que: *“La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”*.
- b) Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. (BOE núm. 298, Martes 14 diciembre 1999).
- c) Real Decreto por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal (B.O.E. núm. 17, 19 de enero 2008).

La Ley Orgánica 15/99 se compone de 49 artículos, y se divide en VII Títulos, estructurados de la siguiente manera:

- Título I: Disposiciones generales (arts. 1-3).
- Título II: Principios de la Protección de Datos (arts. 4-12).
- Título III: Derechos de las Personas (arts. 13-19).
- Título IV: Disposiciones Sectoriales (arts.20-32).
 - Capítulo Primero: Ficheros de Titularidad Pública (arts. 20-24).

- Capítulo Segundo: Ficheros de Titularidad Pública (arts. 25-32).
- Título V: Movimiento Internacional de Datos (arts.33-34).
- Título VI: Agencia de Protección de Datos (arts.35-42).
- Título VII: Infracciones y Sanciones (arts.43-49).

3. CONCEPTOS Y DEFINICIONES TRANSVERSALES EN LA LOPD

La LOPD en su artículo 3 denominado “Definiciones” apunta una serie de conceptos transversales que nos iremos encontrando a lo largo de esta normativa y que es conveniente reflejar:

- a) Datos de carácter personal: cualquier dato de una persona física que lo identifique o a través del cual sea identificable.

En el artículo 5.-1.-f del Reglamento de desarrollo de la LOPD se indica que “Los datos de carácter personal será cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables”.

Como esta definición esclarece, al hablar la Ley de datos de carácter personal, no sólo hace referencia al nombre y apellidos de las personas, sino que, incluye de manera amplia, cualquier tipo de información (DNI, NIF, vídeos, fotografías, voz, huellas, etc...), que haga referencia a una persona física identificada (se conoce de quién es el dato) o identificable (no se conoce de quién es el dato, pero se puede averiguar).

Llegados a este punto, es interesante profundizar en los conceptos de persona física identificada o identificable. Así, se considera que una información hace referencia a una persona física identificada cuando nos indica a qué persona se refiere sin necesidad de realizar comprobaciones. Un ejemplo de ello lo tenemos en el DNI, que identifica claramente a una persona inconfundiblemente.

Por otro lado, se considera que una información hace referencia a una persona física identificable cuando a priori no nos indica a que persona



se refiere, pero la información es suficiente para poder llegar a averiguar su identidad. Un ejemplo muy clarificador es el ADN, que contiene información genética de una persona concreta, pero no sabremos de quién se trata hasta que no lo sometamos al procedimiento adecuado. El Reglamento de desarrollo de la LOPD indica en el artículo 5.-1.-o, que una persona es identificable cuando “su identidad puede determinarse directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona no se considera identificable si dicha identificación requiere plazo o actividades desproporcionadas”.

Vamos a hacer un ejercicio de análisis con el formulario NOTA de la Agencia Española de Protección de Datos para ver qué tipo de datos pueden estar incluidos en el concepto “datos de carácter personal”.

7 Tipos de datos, estructura y organización del fichero Validar Borrar ?

Datos especialmente protegidos :
 Los tratamientos de datos de carácter personal que revelen o hagan referencia a **ideología, afiliación sindical, religión o creencias**, deberán ampararse en alguno de los supuestos que la Ley establece al efecto para poder tratarlos.
 El tratamiento de estos datos sólo puede realizarse si se ha recabado el **consentimiento expreso y por escrito del afectado**. Para más información consulte la ayuda del formulario.

Datos especialmente protegidos

Ideología Afiliación sindical Religión Creencias

Otros Datos especialmente protegidos :
 Los tratamientos de datos de carácter personal que revelen o hagan referencia al **origen racial, la salud o la vida sexual** deberán ampararse en alguno de los supuestos que la Ley establece al efecto para poder tratarlos.
 Para el tratamiento de estos datos será obligatorio recabar el **consentimiento expreso del afectado** o que, por razones de interés general, así lo disponga una Ley.

Otros Datos especialmente protegidos

Origen racial o Étnico Salud Vida sexual

Datos de carácter identificativo

NIF / DNI N° SS / Mutualidad Nombre y apellidos Tarjeta Sanitaria
 Dirección Teléfono Firma / Huella
 Imagen / voz Marcas físicas Firma electrónica

Otros datos de carácter identificativo

Otros datos tipificados

CARACTERÍSTICAS PERSONALES
 CIRCUNSTANCIAS SOCIALES
 ACADEMICOS Y PROFESIONALES
 DETALLES DEL EMPLEO
 INFORMACION COMERCIAL
 ECONOMICOS, FINANCIEROS Y DE SEGUROS
 TRANSACCIONES DE BIENES Y SERVICIOS

> <

Otros tipos de datos

Sistema de tratamiento

Automatizado Manual Mixto

Analizando el fichero NOTA podemos concluir que son datos de carácter personal los siguientes:

- *Datos especialmente protegidos:* ideología, religión, creencias, afiliación sindical, origen racial o étnico, salud y vida sexual.
- *Datos de Carácter identificativo:* NIF/DNI, dirección, imagen teléfono, voz, número de la Seguridad Social o Mutualidad, marcas físicas, tarjeta sanitaria, firma, huella, nombre y apellidos, y firma electrónica.

- *Datos relativos a las características personales:* datos del estado civil, de la familia, fecha de nacimiento, edad, lugar de nacimiento, nacionalidad, sexo, características físicas y lengua materna.
- *Datos relativos a las circunstancias sociales:* Alojamiento, vivienda, situación familiar, posesiones, propiedades, aficiones, estilo de vida, pertenencias a clubes y asociaciones, licencias.
- *Datos académicos y profesionales:* Formación, titulaciones historial del estudiante, experiencia profesional, pertenencia a colegios o asociaciones profesionales.
- *Datos de empleo:* Profesión, puesto de trabajo, datos no económicos de la nómina.
- *Datos que aportan información comercial:* Actividades y negocios, licencias comerciales, suscripciones a publicaciones, medios de comunicación, creaciones artísticas, literarias, científicas o técnicas.
- *Datos económicos, financieros de seguro:* Ingresos, rentas, inversiones, patrimonio, créditos, préstamos, avales, datos bancarios, planes de pensiones, jubilación, datos económicos de la nómina, datos de impuestos, seguros, hipotecas, subsidios, beneficios, historial de créditos, tarjetas de créditos.
- *Datos relativos a transacciones de bienes y servicios:* Bienes o servicios suministrados, bienes o servicios recibidos por el afectado, transacciones financieras, compensaciones e indemnizaciones.

A sensu contrario, podemos delimitar que no se considera datos de carácter personal al encontrarnos ante datos referidos a:

- Personas jurídicas, ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.
 - Datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal.
 - Datos referidos a personas fallecidas.
 - Ficheros realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
 - Ficheros sometidos a la normativa sobre protección de materias clasificadas.
 - Ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos.
- b) Afectado o Interesado: persona física titular de los datos que sean objeto del tratamiento de datos de carácter personal.
- c) Cancelación: Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el

plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.

- d) 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.
- e) Destinatario o cesionario: la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos.
- f) Exportador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero.
- g) Fichero: conjunto organizado de datos de carácter personal, cualquiera que sea la forma o modalidad de creación, almacenamiento organización o acceso, es decir, esté informatizado, en soporte papel o se encuentre al mismo tiempo informatizado y en soporte papel.
Ejemplo: Fichero de Personal, Fichero de Contactos,...
- h) Ficheros de titularidad privada: los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.
- i) Ficheros de titularidad pública: los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público.

- j) Tercero: la persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.
- k) Tratamiento de datos: cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
- l) Responsable de Fichero o Tratamiento: persona física (autónomo) o jurídica (pyme o micropyme) que decide sobre la creación, finalidad y uso del Fichero o Tratamiento.
- m) Encargado de Tratamiento: persona física (autónomo) o jurídica (pyme o micropyme), autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate los datos personales por cuenta del responsable del tratamiento. El ejemplo característico es la Asesoría Laborales, Contables, Fiscales, Jurídicas, etc. que acceden a los datos de una empresa para la elaboración de nóminas,...

Una misma persona física o jurídica puede desempeñar un doble papel en lo que respecta a la protección de datos de carácter personal. Por ejemplo, una Asesoría de las citadas anteriormente será responsable de los ficheros que precise para el normal desarrollo de sus actividades como empresa (de sus propios ficheros de empleados, clientes, proveedores, contactos,...) y será al mismo tiempo encargado de tratamiento de los ficheros de sus clientes a los que precise acceder para prestarles a estos un servicio (ficheros de empleados de sus clientes para elaborar las nóminas,...).

- n) Cesión o comunicación de datos: revelación de datos de carácter personal a cualquier persona física o jurídica diferente del interesado (ejemplos típicos son: a otro autónomo, a otra empresa, a una

administración pública, a una mutua, etc.). No se considera cesión el acceso a los datos por parte de un Encargado de Tratamiento.

- o) Agencia Española de Protección de Datos (AEPD): es una autoridad de control independiente cuya principal misión es la de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación y, en especial, defender los derechos de los afectados. Es obligatorio que los Responsables de Fichero o Tratamiento le declararen los ficheros que utilizan (Entre otras cuestiones, se declaran los campos que contiene cada fichero, no el contenido concreto de los mismos).

4. PRINCIPIOS GENERALES

Como toda materia contiene una serie de principios generales que son transversales y que sirven de hilo conductor de la normativa. Así, la Ley orgánica 15/1999, de 13 de diciembre y el RDLOPD 1720/2007, regulan dentro de su título II los principios rectores que deben regir la protección de datos en España. La regulación gira sobre los siguientes principios básicos que han de ser respetados en todas las fases del tratamiento de los datos, cuando resulten aplicables. Estos principios son:

Calidad de los datos

Derecho de información en la recogida de datos

Consentimiento del interesado

Deber de secreto

Cesión o comunicación de datos

Acceso a los datos por terceros

- Calidad de los datos: Según lo dispuesto en el artículo 4 de la LOPD y 8 del RDLOPD, los datos de carácter personal deben cumplir tres características básicas tanto en la recogida como en su tratamiento:
 - a) ser adecuados y pertinentes
 - b) no excesivos
 - c) tratados de forma leal y lícita en relación con la finalidad legítima para la que se haya recabado.

La aplicación de este principio básico conlleva que:

- a) Los datos obtenidos no podrán usarse para finalidades incompatibles con aquéllas para las que fueron recogidos. En este caso, el término incompatible debe ser interpretado como distinto, según la sentencia del Tribunal Constitucional 292/2000.
- b) Los datos deberán ser exactos y puestos al día, respondiendo a la situación actual del interesado. Es decir, no podrán permanecer en el fichero por un tiempo superior al necesario para conseguir la finalidad para la que se recabaron. Si no son exactos, están incompletos, o dejan de ser necesarios o pertinentes, deberán ser cancelados o sustituidos por los correctos.

Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

INFRACCIONES A ESTE PRINCIPIO

INFRACCIÓN GRAVE

- *Art. 44.3. Son infracciones graves: d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.*
- *f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.*
- **SANCIÓN Art. 45.2: Multa de 60101,21 a 300506,05€**

INFRACCIÓN MUY GRAVE

- *Art. 44.4. Son infracciones muy graves: a) La recogida de datos en forma engañosa y fraudulenta. f) Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.*
- **SANCIÓN Art.45.3: Multa de 300506,05 € a 601012,10€**

- Derecho de información en la recogida de datos: El artículo 5 LOPD, nos indica que en el momento de la recogida de los datos personales se deberá informar al interesado de modo expreso, preciso e inequívoco de las siguientes circunstancias:
 - a) De la existencia de un fichero o tratamiento de datos de carácter personal, de su finalidad y de los destinatarios de la información.
 - b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que le sean planteadas.
 - c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
 - d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
 - e) De la identidad o dirección del responsable del tratamiento o, en su caso, de su representante, en el caso de que el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento medios situados en España.

En el supuesto que los datos se recojan de persona distinta del interesado, salvo que el titular hubiera sido informado con anterioridad de las siguientes circunstancias, el responsable del fichero tiene la obligación de informar al interesado de forma expresa, precisa e inequívoca, dentro de los **tres meses** siguientes al momento de su registro:

- a) del contenido del tratamiento
- b) de la procedencia de los datos
- c) de la existencia de un fichero o tratamiento
- d) de la finalidad de la recogida
- e) de los destinatarios de la información
- f) de la posibilidad de ejercitar sus derechos
- g) de la identidad y dirección del responsable del tratamiento
- h) o, en su caso, de su representante.

La carga de la prueba sobre el cumplimiento del principio de información, recae sobre el responsable del fichero, que deberá conservar el soporte en el que conste el cumplimiento de dicho deber mientras persista el tratamiento (art. 18 del RDLOPD).

INFRACCIONES A ESTE PRINCIPIO

INFRACCIÓN LEVE

- Art. 44.2. Son infracciones leves: d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley.
- SANCIÓN Art. 45.1: Multa de 601,01 a 60.101,21€

INFRACCIÓN GRAVE

- Art. 44.3. Son infracciones graves: l) Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado.
- SANCIÓN Art. 45.2: Multa de 60.101,21 a 300.506,05 €

INFRACCIÓN MUY GRAVE

- Art. 44.4. Son infracciones muy graves: l) No Atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.
- SANCIÓN Art. 45.3: Multa de 300.506,05 € a 601.012,10 €

- Consentimiento del Interesado: El consentimiento del interesado es el principio fundamental que debemos tener en cuenta para el tratamiento de datos de carácter personal. Así, siguiendo el artículo 6 LOPD, como regla general, puede afirmarse que todo tratamiento de datos de carácter personal requiere el consentimiento inequívoco del interesado.

Para que este consentimiento sea válido, debemos tener en cuenta que la LOPD requiere que los datos no se recaben por medios fraudulentos, desleales o ilícitos.

Los datos relativos al origen racial, salud o vida sexual, únicamente podrán recabarse cuando por razones de interés general así lo disponga una ley, o cuando el interesado consienta expresamente, por escrito o mediante alguna otra fórmula probatoria.

INFRACCIONES A ESTE PRINCIPIO

INFRACCIÓN GRAVE:

Art. 44.3. Son infracciones graves: c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en los que éste sea exigible.

•SANCIÓN: Art. 45.2: Multa de 60.101,21 a 300.506,05 €

INFRACCIÓN MUY GRAVE:

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

•SANCIÓN: Art.45.3: Multa de 300.506,05 € a 601.012,10 €

- Deber de secreto: En materia de protección de datos personales rige el principio general de deber de secreto. Así, el artículo 10 LOPD establece que tanto el responsable del fichero como aquellos que intervengan en cualquier fase del tratamiento de los datos, están obligados al secreto profesional respecto de los mismos y al deber de guardarlos. Estas obligaciones subsisten incluso después de finalizar las relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

INFRACCIONES A ESTE PRINCIPIO

INFRACCIÓN LEVE:

Art. 44.2. Son infracciones leves: e) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave.

SANCIÓN Art. 45.1: Multa de 601,01 a 60101,21 €

INFRACCIÓN GRAVE:

Art. 44.3. Son infracciones graves: c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en los que éste sea exigible.

SANCIÓN: Art. 45.2: Multa de 60.101,21 a 300.506,05 €

INFRACCIÓN MUY GRAVE:

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

SANCIÓN: Art.45.3: Multa de 300.506,05 € a 601.012,10 €

- Cesión o comunicación de datos y supuestos que lo legitiman: Si entendemos que el horizonte de toda esta normativa es la cautela y protección de los datos de carácter personal, la comunicación de datos es un punto de inflexión, pues mediante la cesión de datos a otros ficheros se posibilita la realización de cruces de los datos. Otra cuestión a tener en cuenta es que, a través de la comunicación de datos, se puede incurrir en el error de la utilización de los datos cedidos para un fin o uso determinado y concreto, con otro uso o finalidad distinta para el que se habían recabado.

El artículo 11 LOPD establece las condiciones en las que se podrá o no realizar la cesión o comunicación de datos de carácter personal,

determinando, que sólo se podrán ceder datos de carácter personal *“para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario”*.

Continuando con esta salvaguarda de datos, la Ley indica también que el consentimiento del interesado deba obtenerse con carácter previo a la cesión. Además, la solicitud de este consentimiento será nulo cuando no conste la finalidad a la que se destinarán los datos o el tipo de actividad a la que se dedica el cesionario.

En la Ley y en el Reglamento se establecen excepciones a la regla general del consentimiento en las que no es necesario la prestación del consentimiento:

- a) Cuando esté autorizada por Ley.
- b) Los datos objeto de tratamiento o de cesión figuren en fuentes accesibles al público.
- c) La cesión responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control comporte la comunicación de los datos. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

En definitiva, debe entenderse que la existencia de un grupo de empresas no impide que cada una de las sociedades integradas en el mismo mantenga diferenciada y plena su personalidad jurídica. Por tanto, a todos los efectos jurídicos, la circunstancia de que una sociedad esté participada por otra no afecta al hecho de que cada una de ellas tenga su propia personalidad jurídica, de modo que cada empresa

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

El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

INFRACCIONES A ESTE PRINCIPIO

INFRACCIÓN MUY GRAVE:

- c) Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7.
- SANCIÓN: Art.45.3: Multa de 300.506,05 € a 601.012,10 €

- Acceso a los datos por Terceros: El Artículo 12 de la Ley denominado “Acceso a los datos por cuenta de terceros” nos dice que no se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento. Esta relación deberá estar regulada en un contrato.

Esta relación contractual (artículo 12 LOPD y 20 del RDLOPD), es la de un arrendamiento de servicios (contrato por el que una persona se compromete a prestar algún servicio a otra a cambio de un precio), Es decir, lo esencial de este contrato es que el responsable del fichero (arrendatario de los servicios), continúa teniendo la dirección y la responsabilidad del tratamiento, de modo que el encargado del tratamiento (o arrendador de los servicios) sólo está legitimado para realizar aquello que se le encomienda por medio del contrato.

Así, como el acceso del prestador de servicios no supone una cesión o comunicación de datos, pero deberá devolver los datos o destruirlos al responsable del tratamiento y en caso de incumplimiento será también responsable del tratamiento. Se recomienda incluir estos puntos en el contrato comentado en el párrafo anterior.

Una característica relevante es que si el tercero somete a tratamiento los datos a los que accede para prestar el servicio, dicho tratamiento no requiere ni la previa información al titular de los datos, ni su consentimiento.

5. DERECHOS DE LAS PERSONAS: DERECHOS ARCO

La normativa de la abstracción de los principio baja a la concreción con una serie de derechos para la protección de los datos que garantizan a las personas que puedan acceder, rectificar, cancelar y oponerse al tratamiento de la información que les afecte.

No obstante, el los derechos incluidos en este Título de la Ley podemos distinguir dos grupos:

- a) Los derechos que constituyen la protección: derecho de acceso, rectificación, cancelación y oposición.
- b) Los derechos que constituyen la reclamación: derecho a impugnación, el derecho a indemnización y el derecho a la consulta del Registro General de Protección de Datos.

El motivo de la inclusión de estos derechos en la Ley es además de la protección de los datos de carácter personal, garantizar a la persona el conocimiento y la disposición sobre sus datos personales con el propósito de impedir su tráfico.

Derecho de acceso

Derecho de rectificación

Derecho de cancelación

Derecho de oposición

Derecho de impugnación

Derecho de indemnización

Derecho de consulta al Registro General de Protección de Datos

El ejercicio de estos derechos tiene carácter de personalísimo, no pudiendo ejercerlos una persona en nombre de otra, excepto cuando lo realice el representante legal del interesado en dos supuestos: cuando estamos ante una situación de incapacidad o ante una minoría de edad que le imposibilite el ejercicio personal de los mismos. No obstante, se posibilita en el Reglamento la representación voluntaria para su ejercicio. Además tienen carácter gratuito.

Por otra parte, el Reglamento califica a estos derechos como independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

- Derecho de acceso: Este derecho se identifica con la posibilidad que tiene el interesado de dirigirse al titular del fichero para solicitar y obtener información sobre sus datos de carácter personal sometidos a tratamiento, sobre su origen y las comunicaciones realizadas o que se prevean realizar de los mismos.

El afectado podrá optar por recibir la información a través de uno o varios de los siguientes sistemas de consulta:

- a) Visualización en pantalla.
- b) Escrito, copia o fotocopia remitida por correo, certificado o no.

- c) Telecopia.
- d) Correo electrónico u otros sistemas de comunicaciones electrónicas.
- e) Cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable.

Respecto al contenido del derecho de acceso, la información facilitada comprenderá (artículo 29 del RDLOPD):

- a) Los datos de base del afectado y los resultantes de cualquier elaboración o proceso informático.
- b) El origen de los datos.
- c) Los cesionarios de los mismos.
- d) La especificación de los concretos usos y finalidades para los que se almacenaron los datos.

El responsable del fichero está obligado a proporcionarle la información de forma gratuita en el plazo máximo de un mes, a contar desde la recepción de la solicitud. Si en este plazo no se ha resuelto de forma expresa, se entenderá que la solicitud ha sido denegada. En el supuesto de que la solicitud fuera estimatoria, el acceso se hará efectivo en el plazo de los diez días siguientes a la notificación de aquella.

El responsable del fichero deberá responder la solicitud que se le dirija, con independencia de que figuren o no datos de carácter personal del afectado en sus ficheros, de manera que se debe contestar siempre al interesado que ejercita su derecho de acceso.

Este derecho podrá ejercitarse a intervalos no inferiores a doce meses salvo que se acredite un interés legítimo por parte del interesado, en cuyo caso podrá ejercitarse antes.

- Derecho de Rectificación y Cancelación: La LOPD establece en su artículo 16 LOPD y 32.2. del RDLOPD, que “el responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días”.

El titular de los datos puede ejercitar estos derechos cuando los datos sean inexactos, incompletos o que el tratamiento que se está realizando no se ajuste a la LOPD.

Por otro lado, en base al artículo 4 (Principio de Calidad de los Datos), el responsable del fichero podrá modificar por propia iniciativa los datos que resulten incompletos o inexactos.

El responsable del fichero resolverá la solicitud en el plazo de 10 días desde la recepción de la solicitud. En el supuesto de que considere que no procede a la cancelación o rectificación solicitada por el interesado, deberá comunicárselo motivadamente dentro del mismo plazo de 10 días. Si transcurridos 10 días desde la recepción de la solicitud el responsable del fichero no se pronuncia al respecto se puede interponer la reclamación prevista en el artículo 18 LOPD.

Si los datos rectificadas o cancelados hubieran sido comunicados o cedidos previamente, el responsable del tratamiento deberá notificar en el mismo plazo de 10 días, la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la rectificación y cancelación.

- Derecho de Oposición: Es el derecho del interesado a que sus datos no lleguen a ser tratados o introducidos en un fichero. En la legislación sobre protección de datos puede distinguir dos clases de derecho de oposición:
 - a) La primera es la posibilidad de los titulares para oponerse a que sus datos sean tratados con una finalidad de marketing y prospección comercial.

b) La segunda es que el interesado se podrá oponer al tratamiento de sus datos cuando existan motivos fundados y legítimos relativos a una concreta situación personal, siempre que la Ley no disponga lo contrario.

Dichas clases de oposición aparecen reguladas en el artículo 30 y 6.4 LOPD respectivamente y en los arts. 34, 35 y 36 del RDLOPD.

- Derecho de impugnación: En el artículo 13 de la LOPD se indica que Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto. La valoración sobre el comportamiento de los ciudadanos basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.
- Derecho de indemnización: Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la LOPD por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas.

En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

- Derecho de consulta al Registro General: Además de los derechos anteriormente indicados, se reconoce en el artículo 14 de la LOPD el derecho de consulta al Registro General de Protección de Datos. Este derecho consiste en poder acudir a dicho registro para obtener información sobre los ficheros tanto de naturaleza pública como privada inscritos en él (el nombre del responsable del fichero y la finalidad del mismo), y el de impugnación de valoraciones, que permite impugnar las decisiones que tengan efectos jurídicos, basadas únicamente en una evaluación de sus características o personalidad resultado de un tratamiento de datos de carácter personal.
- El procedimiento para el ejercicio de derechos se regula en el art. 25 del RDLOPD. Dicho precepto establece que el ejercicio de los derechos deberá llevarse a cabo:
 - a) Nombre y apellidos del interesado; fotocopia de su documento nacional de identidad, o de su pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación. La utilización de firma electrónica identificativa del afectado eximirá de la presentación de las fotocopias del DNI o documento equivalente.
 - b) Petición en que se concreta la solicitud.
 - c) Dirección a efectos de notificaciones, fecha y firma del solicitante.
 - d) Documentos acreditativos de la petición que formula, en su caso.

El interesado deberá utilizar cualquier medio que permita acreditar el envío y la recepción de la solicitud. Cuando el responsable del fichero reciba la solicitud, deberá contestar a la misma, independientemente de que figuren o no datos



del solicitante en sus ficheros, utilizando también cualquier medio que permita acreditar el envío y la recepción.

En el supuesto de que la solicitud no reúna los requisitos mencionados anteriormente, el responsable del fichero deberá requerir al solicitante para que subsane la deficiencia detectada

El ejercicio de los derechos ARCO, no satisfechos por el responsable del fichero puede ser reclamados ante la Agencia Española que abrirá un procedimiento de tutela de derechos a fin de determinar si estos han sido vulnerados.

Las normas aplicables al cómputo de los plazos previsto por el RDLOPD, en los supuestos en que señale un plazo por días se computarán únicamente los hábiles. Cuando el plazo sea por meses, se computarán de fecha a fecha.

6. TRATAMIENTO PARA ACTIVIDADES DE PUBLICIDAD Y PROSPECCIÓN COMERCIAL. MARKETING PUBLICITARIO.

Ya hemos ido viendo que la regulación del consentimiento se establece en tres de los principios regulados en el Título II de la LOPD y del RDLOPD:

- Principio del consentimiento para el tratamiento
- Datos Especialmente Protegidos
- Comunicación de datos.

Si la entidad pretende enviar información sobre productos y servicios de terceras empresas, deberá previamente solicitar el consentimiento de los titulares para el envío de dicha información.

Por lo que respecta a las fuentes, origen del tratamiento de los datos con fines de publicidad y de prospección comercial, vienen recogidas en el artículo 30 de la LOPD y 45 del RDLOPD, donde se establece que se podrán utilizar nombres y direcciones u otros datos de carácter personal que figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesado u obtenidos con su consentimiento.

En este sentido, la generación de esta actividad de marketing la encontramos en:

- Las fuentes de acceso público,
- En datos facilitados por el propio interesado y
- En los datos obtenidos con el consentimiento del mismo.

En cuanto a las fuentes accesibles al público, se especifican en el artículo 3 j) de la LOPD y art. 7 del RDLOPD. Se trata de una lista de fuentes de acceso público en la que se recogen supuestos concretos:

- a) El censo promocional. Actualmente no está desarrollado este censo. No obstante, la aprobación de la Proposición no de ley sobre el censo promocional y el procedimiento de su formación por el Congreso de los Diputados, publicada en el Diario de Sesiones número 199, de 29 de octubre de 2012, supone que el Gobierno proceda al desarrollo reglamentario de la Ley Orgánica de Protección de Datos, dado que la Disposición transitoria segunda de la LOPD (utilización del censo promocional) establece que reglamentariamente se desarrollarán los procedimientos de formación del censo promocional, de oposición a aparecer en el mismo, de puesta a disposición de sus solicitantes, y de control de las listas difundidas.
- b) Las guías de servicios de comunicaciones electrónicas, según establezca la normativa específica en cuestión.
- c) 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.

- d) Los Diarios y Boletines oficiales.
- e) Los medios de comunicación social. Pueden considerarse incluidos los datos que hayan sido objeto de difusión a través de prensa, radio y televisión. Pero hay que indicar que Internet no es, a los efectos de protección de datos un “medio de comunicación social”, sino un “canal de comunicación”, por lo que no es fuente accesible al público.

En todo caso, para que estos supuestos puedan ser considerados fuentes accesibles al público, será precisa que su consulta pueda ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación.

Si atendemos al caso concreto de la realización de una “campaña de publicidad” en la que se opta por adquirir los datos a través de una empresa de bases de datos, debe exigir siempre, un compromiso sobre el origen de los datos (procedentes de fuentes de acceso público o recabados con el consentimiento del interesado) y establecerlo específicamente en el contrato que se firme.

A tenor del artículo 11.1 LOPD “los datos de carácter personal objeto de tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de los fines directamente relacionados con las funciones legítimas del cedente y cesionario, con el previo consentimiento del interesado”.

No obstante, la empresa responsable del fichero que ceda el fichero, deberá cumplir lo establecido en la LOPD, en el sentido de informar en el momento en el que se efectúe la primera cesión de datos (véase la página 18).

La adquisición de listados de personas físicas con datos procedentes de una empresa externa, se considerará cesión de datos a los efectos de la vigente Ley Orgánica 15/1999.

Esto hace referencia a los mailing dirigidos a personas que no son clientes ni solicitantes de información o catálogos, y que por tanto, no se encuentran registrados en los ficheros propios de nuestra empresa. Normalmente, para realizar esta actividad se utilizan listados de personas, adquiridos a empresas especializadas en marketing, publicidad directa y prospecciones comerciales, o simplemente bases de datos, en base a las especificaciones que se le realizan a estas empresas para la concreción del segmento de clientes a los que queremos acudir. No obstante, hay que indicar que estos datos tienen que haber sido obtenidos de fuentes accesibles al público o facilitados por los propios interesados u obtenidos con su consentimiento.

Cuando una empresa, se plantee la necesidad de alquilar listados de direcciones, para un solo uso o para varios, es necesario tener en cuenta los siguientes aspectos:

- Identificar las fuentes de información de las que se nutre el listado.
- Los datos que incluye el listado.
- La actualización de los datos (semanal, mensual, anual, etc.).
- La inscripción del fichero origen del listado en el Registro General de Protección de Datos.

Si analizados los apartados anteriores, se considera apropiado el arrendamiento del listado, debe prepararse un contrato que contenga los requerimientos que establece la LOPD. Este contrato debe de guardarse siempre.

Cuando acabe el plazo por el que se accedió a los datos es necesario que dichos datos sean devueltos o suprimidos por el cesionario.

Por otro lado, el RDLOPD indica que cuando se considere contratar con terceros la realización de una campaña publicitaria para la promoción de los productos o servicios de nuestra empresa y se le encomiende el tratamiento de determinados datos se aplicaran las siguientes normas:

- Cuando las variables utilizadas para identificar el público destinatario de una campaña o promoción comercial de productos o servicios, y los destinatarios de la campaña sean fijados por la entidad que contrate la campaña, ésta será responsable del tratamiento de los datos.
- Si estos son determinados sólo por la entidad o entidades contratadas, dichas entidades son las responsables del tratamiento.
- En caso que intervengan ambas empresas serán ambas responsables. Aquí la empresa que encargue la realización de la campaña publicitaria deberá adoptar las medidas necesarias para asegurarse de que la entidad contratada ha recabado los datos cumpliendo las exigencias de la LOPD.

7. LOS TIPOS DE FICHEROS: PÚBLICOS Y PRIVADOS

La LOPD dedica su Capítulo primero (artículos 20 al 24) a los ficheros de titularidad pública y el Capítulo segundo (artículos 25 al 32) a los ficheros de titularidad privada.

Por su parte, el Título V capítulo I del RDLOPD (artículos 52 a 64) se dedica a dichos ficheros.

Los ficheros de titularidad pública serán propios del ejercicio de una función pública, mientras que los privados pueden ser creados según las necesidades de la persona, empresa o entidad titular, para la realización de su actividad u objeto, siempre que sean legítimos.

Para ambos tipos de ficheros existe la obligación de notificación e inscripción en la Agencia Española de Protección de Datos.

TIPOS DE FICHEROS

FICHEROS DE TITULARIDAD PÚBLICA

FICHEROS DE TITULARIDAD PRIVADA

- a) Ficheros de titularidad pública: Los ficheros de titularidad pública son aquellos cuyo titular sea una Administración Pública. La Administración Pública tiene entre sus fines velar por el interés y los derechos de los ciudadanos, al igual que tiene que hacer cumplir las obligaciones de éstos y dispone de poder sancionatorio ante conductas indebidas, ilícitas o ilegales.

En este sentido para la gestión de las competencias encomendadas a las distintas Administraciones Públicas se les permite disponer de la información necesaria de los ciudadanos y se les exonera de tener que disponer de la necesidad de consentimiento.

La creación, modificación o supresión de los ficheros de las Administraciones Públicas, deberá hacerse mediante disposición general o acuerdo que se publicará en el Boletín Oficial del Estado o Diario Oficial correspondiente.

Dentro de los datos que necesariamente debe de comunicar a la Agencia Española de Protección de Datos las Administraciones para la creación o modificación de los ficheros están los siguientes:

- Finalidad del fichero y los usos previstos.
- Los colectivos sobre los que se pretenda obtener los datos.
- El procedimiento de recogida de los datos de carácter personal.
- La estructura básica del fichero y la descripción de los tipos de datos de carácter personal.
- Las cesiones de datos de carácter personal y las posibles transferencias de datos que se prevean a países terceros.
- Las Administraciones responsables del fichero.
- Los servicios ante los que pueden ejercitar los derechos ARCO.
- Las medidas de seguridad con indicación del nivel de seguridad exigible.
- Respecto a la supresión de los ficheros, habrá que indicarse el destino de los mismos y la forma de destrucción.

Las sanciones previstas en la normativa para los titulares de ficheros públicos no tienen carácter económico. En estos casos, el Director de la Agencia Española de Protección de Datos dicta una resolución con las medidas a adoptar para que cesen o se corrijan los efectos producidos por la infracción.

El formulario de solicitud está disponible en los siguientes enlaces:

<http://bit.ly/9baeYg>

<http://bitly.com/9baeYg.qrcode>

<http://bit.ly/fbTqSt>

<http://bitly.com/fbTqSt.qrcode>

- b) Ficheros de titularidad privada: Los ficheros de titularidad privada pueden ser creados cuando resulte necesario para la actividad u objeto legítimo de la persona, empresa o entidad.

Los ficheros de titularidad privada deben tener unas finalidades determinadas, acordes con los fines institucionales o con el objeto social de la persona, entidad o empresa.

Será necesaria su notificación ante la Agencia Española de Protección de Datos (Registro General de Protección de Datos) tanto la creación como la modificación o supresión del fichero. En esta notificación deberá comunicarse como contenido, según nos indica el artículo 26.2 de la LOPD: “el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar”.

Asimismo, deberá comunicarse cualquier cambio en la finalidad, el responsable o la dirección de ubicación del fichero.

Los ficheros de datos de carácter personal de titularidad privada serán notificados a la AEPD por la persona, empresa o entidad que pretenda crearlos con carácter previo a su creación.

Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia hubiera resuelto sobre la misma, se entenderá inscrito el fichero a todos los efectos. En este caso, se cuenta con silencio positivo de la AEPD.

El procedimiento para la inscripción de ficheros consiste en la presentación de los modelos o formularios, bien en soporte electrónico o en soporte papel, de notificación de creación, modificación o supresión de ficheros, de conformidad con lo establecido en los artículos 55 a 59 del RDLOPD.

Los pasos a seguir para la inscripción de los ficheros son los siguientes:

- **PASO 1**-Responder a las preguntas iniciales del asistente dependiendo del tipo de solicitud y forma de presentación elegido.

Inicialmente, y con el fin de preparar el formulario electrónico específicamente al tipo de solicitud y forma de envío que tiene previsto realizar, el asistente le formulará varias preguntas sobre:

- Tipo de solicitud de inscripción: Se debe señalar la casilla que corresponda, en función de si va a notificar una nueva inscripción, una modificación de un fichero que ya figura inscrito en el Registro General de Protección de Datos (RGPD) o una supresión de un fichero que, igualmente, ya figura inscrito en el RGPD. Tanto para notificar una modificación como una supresión, deberá conocer determinados datos de la inscripción del fichero (código de inscripción y CIF del responsable con el que el fichero figura inscrito en el RGPD).

- Modelo de declaración: Puedes optar por utilizar una de las notificaciones tipo precumplimentadas que aparecen en el formulario o bien por utilizar el formulario electrónico vacío para ser cumplimentado de forma completa por Vd.

- Forma de presentación: Por último, debes señalar la casilla correspondiente a la forma de envío que vas a utilizar:
 - ✓ A través de Internet con certificado digital de firma electrónica.
 - ✓ A través de Internet con presentación convencional de la Hoja de solicitud.
 - ✓ Mediante formulario en soporte papel con código de barras bidimensional PDF 417.

- **PASO 2**-Cumplimentar los apartados de la notificación. Se recomienda guardar la notificación antes de pasar a la siguiente

fase de cumplimentación, ya que una vez que se haya optado por cumplimentar la Hoja de solicitud no se podrán realizar nuevos cambios en la notificación.

Tanto si ha elegido utilizar una notificación tipo como un formulario vacío, deberá cumplimentar los apartados del formulario que describan el fichero que va a ser notificado.

El formulario electrónico de NOTificaciones Telemáticas a la AEPD (NOTA) de titularidad privada se compone de 2 páginas de detalle y la correspondiente Hoja de solicitud. En este formulario son de cumplimentación obligatoria distintos apartados.

En todos los apartados se encuentra disponible la ayuda contextual y una opción que nos permite verificar si el mismo ha sido cumplimentado correctamente.

Se recomienda guardar la notificación antes de pasar a la siguiente fase de cumplimentación, ya que una vez que se hayamos optado por cumplimentar la Hoja de solicitud no se podrán realizar nuevos cambios en la notificación.

Puede imprimir un borrador de la notificación teniendo en cuenta que esta impresión no podrá ser presentada para su inscripción en la Agencia. Tenemos que tener en cuenta que cualquier cambio que necesitemos hacer en la notificación deberá realizarse mediante el formulario electrónico, ya que en cualquiera de las formas de presentación la información consignada mediante dicho formulario electrónico prevalece sobre cualquier anotación realizada de forma manual.

- **PASO 3**-Cumplimentar la Hoja de solicitud. Una vez que se ha comprobado que los distintos apartados han sido cumplimentados correctamente, deberá cumplimentar la Hoja de solicitud. Para

ello debemos pulsar el botón «Cumplimentar hoja de solicitud» que se encuentra al final del formulario.

Debemos indicar los datos identificativos de la persona que firma la solicitud y el cargo o la condición del firmante de esta solicitud en relación con el responsable del fichero.

Señalamos también la dirección completa a efectos de notificaciones (esta dirección debe cumplimentarse en todos los casos).

Si optamos por presentar la notificación a través de Internet con certificado digital de firma y disponemos de una dirección electrónica a efectos de notificaciones del Servicio de Notificaciones Electrónicas (<http://notificaciones.060.es>) podemos indicar esto en el apartado de Dirección electrónica servicio de notificaciones, donde se notificará la inscripción del fichero. En cualquier otro caso, la notificación será realizada a la dirección que a estos efectos se haga constar en el apartado correspondiente de la Hoja de solicitud.

Antes de realizar el envío de la notificación debemos leer y aceptar la información relativa a la LOPD.

Por último, si hemos optado por presentar la notificación a través de Internet con certificado digital de firma debemos proceder a firmar la notificación mediante el certificado de firma.

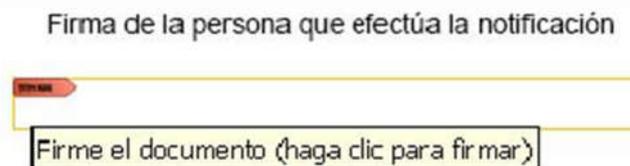
- **PASO 4**-Generar/Enviar la notificación: En el caso de presentación a través de Internet con certificado de firma electrónica, deberá antes «Finalizar y Firmar» la notificación con su certificado de firma electrónica reconocido. En el caso de presentación en formulario en papel, deberá pulsar el botón «Finalizar formulario» que se encuentra al final de la Hoja de solicitud generándose el código de barras bidimensional PDF 417

(nube de puntos), así como el correspondiente código de envío que establece la correspondencia entre el contenido que figura en cada una de las páginas que componen el modelo de notificación y la nube de puntos generada.

Dependiendo de la forma de presentación elegida, la notificación podrá ser presentada a través de los siguientes medios:

- ✓ **Presentación a través de Internet con certificado de firma reconocido**: Una vez cumplimentada la notificación y la Hoja de solicitud de forma correcta, será necesario indicar al formulario que no se van a realizar más cambios mediante el botón «Finalizar formulario» para proceder a la firma de la notificación.

En este momento aparecerá un icono en el lugar previsto para la firma de la persona que efectúa la notificación.



Pulsando el icono que aparece, se firmará la notificación con el certificado de firma reconocido correspondiente a la persona que, con representación suficiente del responsable del fichero, formula la notificación. Su sistema le informará de los certificados de firma de los que dispone y una vez firmada, se enviará la notificación al Registro Telemático de la AEPD.

Una vez recibida se emite un mensaje de confirmación de la solicitud, en el que constarán los datos proporcionados por el interesado, junto con la acreditación de la fecha y hora en que produjo la recepción y una clave de identificación de la transmisión. El mensaje de confirmación puede ser impreso o archivado informáticamente por el interesado y tendrá el valor de recibo de presentación a efectos de lo dispuesto en el artículo 6.3 del Real Decreto 772/1999.



**Fichero de titularidad privada
 SOLICITUD DE INSCRIPCIÓN**
 Confirmación de la recepción de la notificación en la AEPD

**NOTIFICACIONES
 ELEMÁTICAS A
 LA AEPD.**

Tipo de solicitud: Actuación sobre el fichero

Datos de registro de entrada (A consignar en la Agencia Española de Protección de Datos):
 Número de registro:
 Fecha: Hora:

Soporte de la solicitud y modo de presentación: Número del envío:

Persona física que actúa en representación del responsable del fichero ante la AEPD

Datos del responsable del fichero (del Apartado 1):
 Razón Social o Nombre y Apellidos: CIE/NIE:

Declarante:
 Nombre: Primer Apellido: Segundo Apellido:
 NIF: Cargo o condición del firmante en relación con el responsable de fichero:

Dirección a efectos de notificación:
 Apellidos y Nombre o razón Social:
 Dirección postal:
 Localidad: Código Postal: Provincia: País:
 Teléfono: Fax: Correo electrónico:
 Medio de notificación:

De conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, solicito la inscripción en el Registro General de Protección de Datos del fichero de datos de carácter personal al que hace referencia el presente formulario de notificación. Asimismo, bajo mi responsabilidad manifiesto que dispongo de representación suficiente para solicitar la inscripción de este fichero en nombre del responsable del fichero y que éste está informado del modo de obligaciones que se derivan de la LOPD. Igualmente, declaro que todos los datos consignados son ciertos y que el responsable del fichero ha sido informado de los supuestos legales que habilitan el tratamiento de datos especialmente protegidos, así como la cesión y la transferencia internacional de datos.

La Agencia Española de Protección de Datos podrá requerir que se acredite la representación de la persona que formula la presente notificación.
 En a de de

Conocimiento de los deberes del declarante

En cumplimiento del artículo 5 de la Ley 15/1999, por el que se regula el derecho de información en el registro de los datos, se advierte de los siguientes aspectos:
 Los datos de carácter personal, que pueden constar en esta notificación, se incluirán en el fichero de nombre "Registro General Protección de Datos", creado por Resolución del Director de la Agencia Española de Protección de Datos (AEPD) de fecha 26 de abril de 2006 (S.O.E/117) por la que se crea y modifica los ficheros de datos de carácter personal existentes en la AEPD. La finalidad del fichero es votar por la publicidad de los contenidos de los ficheros que contienen datos de carácter personal con el fin de hacer posible el ejercicio de los derechos de información, oposición, acceso, rectificación y cancelación de los datos. Los datos relativos a la persona física que presenta la notificación de fichero y solicita su inscripción en el Registro General de Protección de Datos se utilizarán en los términos previstos en los procedimientos administrativos que sean necesarios para la tramitación de la correspondiente solicitud y posteriores comunicaciones con la AEPD. También derecho a acceder a sus datos personales, rectificarlos o, en su caso, cancelarlos en la AEPD, órgano responsable del fichero.

En caso de que en la notificación deban incluirse datos de carácter personal, referentes a personas físicas distintas de la que efectúa la solicitud o del responsable del fichero, deberá, con carácter previo a su inclusión, informarse de los deberes contenidos en el Anexo anterior.

La no recepción del mensaje de confirmación, o en su caso, la recepción de un mensaje de indicación de error implica que no se ha producido la recepción del mismo, debiendo realizarse la presentación en otro momento o utilizando otros medios.

La presentación de solicitudes, escritos y comunicaciones al Registro Telemático podrá realizarse durante las 24 horas de todos los días del año.

- ✓ **A través de Internet sin certificado de firma electrónica reconocido:** Una vez cumplimentada la notificación y la Hoja de solicitud de forma correcta, hay que enviar la notificación mediante el formulario electrónico pulsando el botón «Enviar a través de Internet» que se encuentra en la Hoja de solicitud. El formulario indicará que se está conectando con el servidor de la

AEPD y, acto seguido, el sistema enviará la Hoja de solicitud (en formato PDF) que confirma que la notificación ha sido enviada correctamente. Dicha Hoja de solicitud, firmada por la persona que efectúa la notificación, es la que deberá remitir a la AEPD.



AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Fichero de titularidad privada SOLICITUD DE INSCRIPCIÓN
 Confirmación de la recepción de la notificación en la AEPD

NOTIFICACIONES ELEMÁTICAS-A LA AEPD

Tipo de solicitud: Actuación sobre el fichero

Datos de registro de entrada (A consignar en la Agencia Española de Protección de Datos):

Soporte de la solicitud y modo de presentación: Número del envío:

Persona física que actúa en representación del responsable del fichero ante la AEPD

Datos del responsable del fichero (del Actuario 1):
 Razón Social o Nombre y Apellidos: CIF / NIF:

Declarante:
 Nombre: Primer Apellido: Segundo Apellido:
 NIF: Cargo o condición del firmante en relación con el responsable del fichero:

Dirección a efectos de notificación:
 Apellidos y Nombre o razón Social:
 Dirección postal:
 Localidad: Código Postal: Provincia: País:
 Teléfono: Fax: Correo electrónico:
 Medio de notificación:

De conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, solicito la inscripción en el Registro General de Protección de Datos del fichero de datos de carácter personal al que hace referencia el presente formulario de notificación. Asimismo, bajo mi responsabilidad manifiesto que dispongo de representación suficiente para solicitar la inscripción de este fichero en nombre del responsable del fichero y que este está informado del resto de obligaciones que se derivan de la LOPD. Igualmente, declaro que todos los datos consignados son ciertos y que el responsable del fichero ha sido informado de los supuestos legales que habilitan el tratamiento de datos especialmente protegidos, así como de su opción y la transferencia internacional de datos.

La Agencia Española de Protección de Datos podrá requerir que se acredite la representación de la persona que formula la presente notificación.
 En a de de

Firma de la persona que efectúa la notificación: Conocimiento de los deberes del declarante

EJEMPLAR PARA PRESENTAR EN LA AEPD

En cumplimiento del artículo 5 de la Ley 15/1999, por el que se regula el derecho de información en la recogida de los datos, se advierte de los siguientes extremos: Los datos de carácter personal, que pudieran constar en esta notificación, se incluyen en el fichero de nombre "Registro General Protección de Datos", creado por Resolución del Director de la Agencia Española de Protección de Datos (AEPD) de fecha 26 de abril de 2000, (B.O.E. nº 117) por la que se crea y modifica los ficheros de datos de carácter personal sometidos en la AEPD. La finalidad del fichero es velar por la publicidad de la existencia de los ficheros que contienen datos de carácter personal con el fin de hacer posible el ejercicio de los derechos de información, oposición, rectificación y cancelación de los datos. Los datos relativos a la persona física que presenta la notificación se inscriben en el fichero una vez se produce la inscripción en los términos previstos en los procedimientos administrativos que sean necesarios para la tramitación de la correspondiente solicitud y posteriores comunicaciones con la AEPD. Tendrán derecho a acceder a sus datos personales, rectificarse o, en su caso, cancelarse en la AEPD, órgano responsable del fichero. En caso de que en la notificación deban incluirse datos de carácter personal, referentes a personas físicas distintas de la que efectúa la solicitud o del responsable del fichero, deberá, con carácter previo a su inclusión, informarse de los extremos contenidos en el párrafo anterior.

Cuando la notificación se envíe a través de Internet sin certificado de firma reconocida, no se considera recibida la notificación hasta la entrada en la Agencia Española de Protección de Datos de la hoja de solicitud firmada de forma manual. La dirección de la AEPD es:

Agencia Española de Protección de Datos
 c. Jorge Juan, 6

28001- Madrid

- ✓ **Presentación en papel con código de barras bidimensional PDF 417:** Una vez que hayamos cumplimentado la Hoja de solicitud, para obtener el modelo que puede ser presentado en la AEPD, debemos pulsar el botón «Finalizar formulario» que se encuentra al final de la Hoja de solicitud. En el caso de la presentación en papel, se genera el código de barras bidimensional PDF 417 (nube de puntos), así como el correspondiente código de envío que establece la correspondencia entre el contenido que figura en cada una de las páginas que componen el modelo de notificación y la nube de puntos generada. En el caso de que tengamos que realizar cambios en la notificación, debemos cumplimentar una nueva notificación y generar la correspondiente nube de puntos y código de envío. A continuación se muestra el aspecto que debe tener la Hoja de solicitud después de haber sido generada correctamente.



Una vez cumplimentada la notificación y la Hoja de solicitud de forma correcta, imprimimos la correspondiente notificación en la que figura el código de barras bidimensional PDF 417 (nube de puntos). Una vez firmada la Hoja de solicitud por la persona que, con representación suficiente del responsable del fichero, formula la notificación, se presentará en la AEPD o en alguno de los Registros y oficinas a los que se refiere el artículo 38.4 de la Ley 30/1992. La dirección de la AEPD es:

Agencia Española de Protección de Datos
c. Jorge Juan, 6
28001- Madrid

- **PASO 5**-*Recordatorio se ha indicado anteriormente.* En las presentaciones a través de Internet, deberá recibir el acuse de recibo de la AEPD del envío realizado. La no recepción del mensaje de confirmación, o en su caso, la recepción de un mensaje de indicación de error implica que no se ha producido la recepción del mismo, debiendo realizarse la presentación en otro momento o utilizando otros medios.
- **PASO 6**-*Recordatorio se ha indicado anteriormente.* Enviar la Hoja de solicitud firmada a la AEPD. En el caso de presentación a través de Internet con certificado de firma electrónica no será necesario remitir la Hoja de solicitud. En el caso de presentación en formulario en papel, se presentará la Hoja de solicitud con el código bidimensional correctamente impreso, así como las dos páginas con el contenido de la notificación en las que deberá figurar el código de envío generado por el formulario electrónico.

Si en algún momento tenemos que realizar la **modificación** de un fichero previamente inscrito esta es la forma de proceder: Cumplimentar el modelo. Para ello debemos indicar el código de inscripción del fichero asignado por la AEPD y los datos identificativos del responsable del fichero, señalando aquellos apartados que se modifican respecto a la notificación anterior. Los apartados señalados que se pretendan modificar deben cumplimentarse por completo.

Cuando la modificación consiste en dejar sin contenido un apartado cuya cumplimentación no es obligatoria se debe señalar la casilla de supresión del apartado.

Hay que tener en cuenta que para modificar el NIF/CIF o la denominación social del responsable del fichero, debemos acompañar la modificación con la documentación que justifique el cambio.



AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

**Fichero de titularidad privada
CONTENIDO DE LA NOTIFICACIÓN**

**NOTIFICACIONES
ELECTRONICAS
A LA AEPD**

Tipo de solicitud de inscripción.

Indique qué operación va a realizar sobre el fichero. En caso de modificaciones y supresiones se deberá indicar el Código de Inscripción que se asignó al fichero en el momento de su alta en el RGPD así como el CIF/NIF con el que fue inscrito. En caso de modificación se solicitan los apartados que se desea modificar y el Nombre o Razón Social del responsable.

Alta Modificación Supresión

Modificación

Denominación social del responsable del fichero

CIF/NIF con el que figure inscrito el fichero

Códigos de Inscripción

Supr. Mod.

<input type="checkbox"/> Responsable del fichero o tratamiento	<input type="checkbox"/> Tipos de datos, estructura y organización del fichero
<input type="checkbox"/> Derechos de oposición, acceso, rectificación y cancelación	<input type="checkbox"/> Medidas de seguridad
<input type="checkbox"/> Encargado del tratamiento	<input type="checkbox"/> Cesión o comunicación de datos
<input type="checkbox"/> Identificación y finalidad del fichero	<input type="checkbox"/> Transferencias internacionales
<input type="checkbox"/> Origen y procedencia de los datos	

En caso de tener intención de **suprimir** un fichero previamente inscrito en el Registro General de Protección de Datos debemos indicar el código de inscripción del fichero asignado por la AEPD y los datos identificativos del responsable del fichero.

Además, se debe indicar el motivo de la supresión en el texto correspondiente, y el destino de la información en el siguiente campo. Si vamos a proceder a destruir el fichero, indicamos las previsiones adoptadas para ello.

Cuando se notificamos la supresión de un fichero por responsable distinto del que figura inscrito en el Registro General de Protección de

Datos debemos acompañar con documentación fehaciente que justifique el cambio del titular.

Tipo de solicitud de inscripción.

Indique qué operación va a realizar sobre el fichero. En caso de modificaciones y supresiones se deberá indicar el Código de Inscripción que se asignó al fichero en el momento de su alta en el RGPD así como el CIF/NIF con el que fue inscrito. En caso de modificación se solicitan los apartados que se desea modificar y el Nombre o Razón Social del responsable.

Alta Modificación Supresión

Supresión de la inscripción del fichero

Denominación social del responsable del fichero

CIF/NIF con el que figure inscrito el fichero

Códigos de Inscripción

Por último, está disponible un formulario tipo que de manera electrónica se puede notificar una serie de ficheros relacionados con la gestión de comunidades de propietarios, clientes, libro recetario de las oficinas de farmacia, pacientes, gestión escolar, nóminas y recursos humanos.

El formulario electrónico contiene una notificación precumplimentada en la que, además de añadir los datos específicos de la notificación, permite realizar algunos cambios. Una vez revisada la notificación, se debe firmar y enviar a la AEPD en cualquiera de las formas de presentación establecidas.



AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS

Fichero de titularidad privada CONTENIDO DE LA NOTIFICACIÓN



NOTIFICACIONES
ELECTRONICAS A
LA AEPD

Tipo de solicitud de inscripción.

Indique qué operación va a realizar sobre el fichero. En caso de modificaciones y supresiones se deberá indicar el Código de Inscripción que se asignó al fichero en el momento de su alta en el RGPD así como el CIF/NIF con el que fue inscrito. En caso de modificación se solicitan los apartados que se desea modificar y el Nombre o Razón Social del responsable.

Alta Modificación Supresión

Modelo de declaración

Si la notificación se refiere a un tratamiento de datos sobre miembros de comunidades de propietarios, clientes propios, libro de recetario, (clientes de farmacias), nóminas-recursos humanos (empleados) o pacientes, y la finalidad es la gestión propia de estos colectivos, puede marcar el cuadro TIPO y seleccionar el modelo que corresponda (se rellenan determinados apartados con valores apropiados) o bien seleccionar NORMAL para partir de un formulario totalmente vacío.

Normal Tipo

Tipos

<input type="checkbox"/> Comunidad de Propietarios	<input type="checkbox"/> Nóminas - Recursos Humanos	<input type="checkbox"/> Videovigilancia
<input type="checkbox"/> Clientes y/o proveedores	<input type="checkbox"/> Pacientes	
<input type="checkbox"/> Libro Recetario	<input type="checkbox"/> Gestión Escolar	

8. MEDIDAS DE SEGURIDAD

El artículo 9 de la LOPD nos indica que el Responsable del Fichero y en su caso, del Encargado del Tratamiento, deben adoptar las medidas de índole técnica y organizativa necesaria que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto.

Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal: infracciones administrativas o penales, solvencia patrimonial y de crédito, aquellos de los que sean responsables Administraciones



tributarias, aquéllos de los que sean responsables las entidades financieras, aquéllos de los que sean responsables las Entidades Gestoras de la Seguridad Social y aquéllos que contengan un conjunto de datos que ofrezcan una definición de la personalidad de los ciudadanos.

Las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal: Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual. Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas. Aquéllos que contengan datos derivados de actos de violencia de género.

El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad que será de obligado cumplimiento para el personal con acceso a los sistemas de información. Este documento podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. En todo caso, tendrá el carácter de documento interno de la organización y deberá contener, como mínimo, los siguientes aspectos: Ámbito de aplicación del documento, medidas para garantizar el nivel de seguridad exigido, funciones y obligaciones del personal, procedimiento de gestión de incidencias, los procedimientos de realización de copias y recuperación de datos y las medidas para la destrucción de los documentos y soportes.

En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, el documento de seguridad deberá contener además: La identificación del responsable o responsables de seguridad y los controles periódicos de verificación del cumplimiento de lo dispuesto en el documento.

Como se ha indicado las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto. Además, estos se clasifican dependiendo de si están automatizados o no automatizados.

MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS Y TRATAMIENTOS AUTOMATIZADOS

Medidas de seguridad de Nivel Básico

Medidas de seguridad de Nivel Medio

Medidas de seguridad de Nivel Alto

- **Medidas de Seguridad de Nivel Básico:** Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.

Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

- **Medidas de Seguridad de Nivel Medio:** En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. A partir del nivel medio los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento.

Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

- **Medidas de Seguridad de Nivel Alto:** Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. El período mínimo de conservación de los datos registrados será de dos años. El responsable de seguridad se encargará de revisar al

menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS Y TRATAMIENTOS NO AUTOMATIZADOS

Medidas de seguridad de Nivel Básico

Medidas de seguridad de Nivel Medio

Medidas de seguridad de Nivel Alto

- **Medidas de Seguridad de Nivel Básico:** Les es de aplicación lo establecido anteriormente para los ficheros automatizados respecto a las Funciones y obligaciones del personal, Registro de incidencias, Control de acceso y Gestión de soportes.

Además, deberá garantizarse la correcta conservación de los documentos.

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura.

La persona que se encuentre al cargo de la custodia de los documentos, deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

- **Medidas de Seguridad de Nivel Medio:** Se designará uno o varios responsables de seguridad. Los ficheros comprendidos en

la presente sección se someterán, al menos cada dos años, a una auditoría interna.

- **Medidas de Seguridad de Nivel Alto:** Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente.

La generación de copias o la reproducción de los documentos únicamente podrán ser realizadas bajo el control del personal autorizado. El acceso a la documentación se limitará exclusivamente al personal autorizado.

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

9. PREGUNTAS FRECUENTES Y RESOLUCIÓN DE DUDAS

La AEPD ha dado respuesta a una serie de preguntas que han sido realizadas en distintas ocasiones y que nos pueden orientar rápidamente:

- **¿La Ley de protección de datos ampara a los autónomos, a las empresas o a sus directivos?**

18-nov-2011

Con carácter general que el objeto de la Protección de Datos de Carácter Personal está regulado en los artículos 1 y 2 de la LOPD que expresamente establecen:

Artículo 1. Objeto

La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Artículo 2. Ámbito de aplicación

1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Asimismo, el artículo 2.2 del Real Decreto 1720/2007, de 21 de diciembre, reglamento que desarrolla la LOPD, señala que no será aplicable a los tratamientos de datos referidos a personas jurídicas ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquellas, consistentes en nombre y apellidos, las funciones o puestos desempeñados, la dirección postal o electrónica, teléfono y número de fax profesionales.

Igualmente, en su artículo 2.3 dispone que los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal.

Por ello, no es de aplicación la LOPD al caso planteado por Vd. relativo al tratamiento de datos de una empresa o persona jurídica o autónomo o a personal de contacto de la misma, entendiendo por tal, las personas que ostentan un cargo directivo que representa a la empresa (Director General, Administrador, Gerente, etc) y siempre que el dato se utilice en su condición de tal.

- **¿Es la dirección e-mail un dato de carácter personal?**

18-nov-2011

El concepto de dato personal, según la definición de la LOPD, de 13 de diciembre, de protección de datos de carácter personal, comprende cualquier información concerniente a persona física identificada o identificable, de donde se requiere la concurrencia de un doble elemento: por una parte la existencia de una información o dato y de otra, que dicho dato pueda vincularse a una persona física identificada o identificable.

En el supuesto de direcciones electrónicas la información está constituida por un conjunto de signos que cuando permiten la vinculación directa o indirecta con una persona física la convierte en un dato de carácter personal.

El tratamiento de datos personales (en este caso, la dirección del e-mail) requiere el consentimiento de los titulares de los datos o bien la existencia de una Ley que lo ampare. En consecuencia, la utilización de e-mail sin consentimiento podría ser vulneración de la normativa sobre protección de datos y se podría denunciar ante la Agencia.

- **¿Cómo afecta la LOPD a la libreta de direcciones de correo electrónico (Microsoft Outlook) que guardan datos en cada PC?**

18-nov-2011

Se define un Fichero como “todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso”.

En consecuencia, la empresa será responsable de tantos ficheros como conjuntos estructurados de datos, adscritos a una determinada finalidad legítima utilice. Cada conjunto estructurado de datos aplicado a una finalidad concreta constituye un fichero, con independencia de los datos de carácter personal que se incluyen.

Partiendo de la definición anterior, la libreta de direcciones de Outlook es un fichero que contiene datos de carácter personal, pues el e-mail se puede identificarse a su titular.

En consecuencia, debe procederse a la inscripción de ficheros en el Registro General de Protección de Datos.

- **He ido a comprar a un gran almacén y me han intentado captar mi firma, pero no en un papel normal, sino en una tablilla electrónica, en la que queda grabada mi firma de manera digital ¿Es legal?**

18-nov-2011

El artículo 4 de la LOPD señala que:

1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

Igualmente, la entidad que recaba datos personales debe informar de lo dispuesto en el artículo 5 de la citada Ley Orgánica, según el cual:

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) 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.

- b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
- c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
- d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- e) De la identidad y dirección del responsable del tratamiento ”

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

En consecuencia, cuando se recaban datos personales (entre ellos la firma) debe informarse de lo expuesto anteriormente. Por lo tanto, teniendo en cuenta que la firma del contrato presupone su aceptación y si los datos se usan para el exclusivo cumplimiento del mismo, informándose debidamente al titular de los datos, se cumpliría la normativa de protección de datos. Si la firma digitalizada se usa para otros fines distintos, se podría estar infringiendo dicha normativa

- **¿La empresa que nos hace la revisión médica está obligada, antes de incluir nuestros datos en un fichero informático, a informarnos de cómo ejercer nuestros derechos?**

16-dic-2010

El derecho de información previo al tratamiento de los datos de carácter personal es uno de los derechos básicos y principales contenidos en la LOPD; por tanto, si se van a registrar y tratar datos de carácter personal, será necesario informar a través del medio que utilice para la recogida, del contenido del artículo 5 que regula el derecho de información previo a la recogida de los datos:

“1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

- a) 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.
- b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
- c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
- d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante ”

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

En consecuencia, cuando se recaban datos personales (como puede ser el caso expuesto por Vd.) debe informarse de lo expuesto anteriormente. Si se trata de menores de edad, hay que informar a sus padres o tutores. El responsable del fichero deberá conservar el soporte en el que conste el cumplimiento del deber de informar, pudiendo utilizar para ello medios informáticos o telemáticos, como el escaneo de la documentación en soporte papel, siempre que se garantice la autenticidad del documento.

El titular de los datos es quien decide si da sus datos personales o no, una vez que haya sido debidamente informado en los términos expuestos. Las consecuencias que se deriven de no dar los datos deben hacerse constar también. No obstante, este Organismo no puede entrar a conocer sobre esas consecuencias

- **¿Cuáles son las principales obligaciones de un responsable de ficheros de datos personales?**

16-dic-2010

Con carácter general, todo responsable de ficheros debe dar cumplimiento a los principios de la protección de datos recogidos en el Título II de la LOPD.

- ✓ Calidad de los datos: los datos sólo se podrán recoger y tratar, cuando sean adecuados, pertinentes y no excesivos, no pudiendo ser usados para finalidades incompatibles con aquellas para las que hubieran sido recabados. Asimismo, serán exactos y puestos al día, debiendo ser cancelados cuando hayan dejado de ser necesarios.
- ✓ Deber de información: Los interesados a los que se soliciten datos personales deberán ser previamente informados de la existencia de un fichero de datos personales, de su finalidad y de los destinatarios de la información. Igualmente, se les deberá informar de la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición, así como de la identidad y dirección del responsable.
- ✓ Consentimiento y comunicación de datos: El tratamiento de datos personales requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa. Asimismo, y con carácter general, los datos sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el consentimiento previo del interesado.
- ✓ Deber de secreto: el responsable del fichero y quienes intervengan en el tratamiento de los datos personales están obligados al secreto profesional respecto de los mismos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o responsable del fichero.
- ✓ Seguridad: el responsable del fichero y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativa que garanticen la seguridad de los datos de carácter

personal y eviten su alteración, pérdida, y su tratamiento o acceso no autorizado.

Los responsables de ficheros o tratamientos de datos personales están igualmente obligados a atender los derechos de acceso, rectificación, cancelación y oposición que la LOPD reconoce a los interesados.

Por otra parte, todo fichero de datos de carácter personal deberá ser notificado por su responsable a la Agencia Española de Protección de Datos para su inscripción en el Registro General de Protección de Datos.

- **¿En qué consiste la Inscripción de ficheros?**

02-nov-2011

Siempre que se proceda al tratamiento de datos personales, definidos en el art. 3,a) de la LOPD , como "cualquier información concerniente a personas físicas identificadas o identificables," que suponga la inclusión de dichos datos en un fichero, considerado por la propia norma (artículo 3.b).), como "conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso," el fichero se encontrará sometido a la Ley, siendo obligatoria su inscripción en el Registro General de Protección de Datos, conforme dispone el artículo 26:

"Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia Española de Protección de Datos.

Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos a países terceros.

Deberán comunicarse a la Agencia Española de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.

El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles. En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.

Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia Española de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado."

Tanto para inscribir, como para suprimir o modificar la inscripción de un fichero en el Registro General de Protección de Datos, se deberá cumplimentar el modelo establecido en la Resolución de 12 de julio de 2006, de la Agencia Española de Protección de Datos, (B.O.E. 181 de 31 de julio de 2006), por la que se aprueban los formularios electrónicos a través de los que deberán efectuarse las solicitudes de inscripción de ficheros en el Registro General de Protección de Datos, así como los formatos y requerimientos a los que deben ajustarse las notificaciones remitidas en soporte informático o telemático.

El formulario electrónico de NOTificaciones Telemáticas a la AEPD (NOTA) permite la presentación de notificaciones a través de Internet (con y sin certificado de firma electrónica reconocido) y en soporte papel.

Dicho formulario interactivo, en formato PDF, se encuentra disponible en la sede electrónica de la AEPD (<https://sedeagpd.gob.es>) y en la página web de la Agencia (www.agpd.es).

De lo indicado en el citado artículo 26 de la Ley Orgánica se desprende que la notificación de los ficheros habrá de ser previa a la creación de los mismos, por lo que la ausencia de dicha notificación sería una conducta constitutiva de infracción leve, con arreglo a lo dispuesto en el artículo 44.2.c) de la propia Ley.

- **¿En qué consiste el principio de seguridad de los datos?**

02-nov-2011

El principio de seguridad de datos establecido en el artículo 9 de la LOPD, impone al responsable del fichero adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

Estas medidas han sido desarrolladas en el Título VIII – De las medidas de seguridad en el tratamiento de datos de carácter personal, del Real Decreto 1720/2007, de 21 de diciembre (RDLOPD).

El artículo 80 del RDLOPD señala que las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto y, a continuación, el artículo 81 especifica la aplicación de los niveles de seguridad según el tipo de datos de carácter personal a tratar.

Con el objeto de facilitar a los responsables de los ficheros la adopción de las disposiciones del Reglamento de Seguridad, se ha elaborado un modelo de " documento de seguridad ", disponible en la página web de la Agencia, que puede servir de guía en el desarrollo de las previsiones del Real Decreto.

- **¿En qué consiste el deber de información?**

16-dic-2010

El deber de información al afectado, previo al tratamiento de sus datos de carácter personal, es uno de los principios fundamentales sobre los que se asienta la LOPD.

El artículo 5 señala lo siguiente: Derecho de información en la recogida de datos. Los interesados a los que se soliciten datos personales

deberán ser previamente informados de modo expreso, preciso e inequívoco:

- ✓ 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.

Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.

No será de aplicación lo dispuesto en el apartado anterior cuando expresamente una Ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia Española de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los

datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

Por tanto, cada persona de la que se pretenda recabar sus datos personales deberá ser informada previamente de todo el contenido del artículo 5.1 para que así conozca con qué finalidad se van a tratar, y por quién, pudiendo además en cualquier momento ejercitar sus derechos de acceso, rectificación, cancelación u oposición

Si la recogida de los datos se ha realizado sin el conocimiento del interesado se le deberá informar en el plazo de los tres meses siguientes al tratamiento.

El incumplimiento del deber de información que contiene el precepto transcrito se encuentra tipificado como falta leve en el artículo 44.2.d) de la LOPD.

- **¿En qué consiste el deber de guardar secreto?**

02-nov-2011

El artículo 10 de la LOPD , exige a quienes intervengan en cualquier fase del tratamiento de los datos, a guardar secreto profesional sobre los datos, subsistiendo la obligación aún después de finalizar su relación con el responsable del fichero: 'El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.'

El incumplimiento del deber de secreto puede ser constitutivo de una sanción leve, en los términos del artículo 44.2.e), o de infracción grave.

La vulneración del deber de guardar secreto sobre los datos de carácter personal especialmente protegidos a que hacen referencia los apartados 2 y 3 del artículo 7, así como de aquellos que hayan sido recabados para

finés policiales sin consentimiento de las personas afectadas, puede ser constitutivo de una sanción muy grave en los términos del artículo 44.4.g) de la LOPD.

- **¿Qué condiciones debe reunir el consentimiento del interesado para el tratamiento de datos?**

16-dic-2010

Como regla general, la inclusión de datos de carácter personal en un fichero supondrá un tratamiento de datos de carácter personal, que requerirá, en principio, el consentimiento del afectado. En particular, la LOPD establece en su artículo 6 lo siguiente: El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado.

No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación comercial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

CESIÓN DE DATOS

En cuanto a la cesión de datos, si la misma comporta identificación de concretas personas físicas constituye una comunicación de datos de carácter personal, definida en el artículo 3, i) de la LOPD, como "toda revelación de datos realizada a persona distinta del interesado".

El régimen de las cesiones de datos se contiene en el artículo 11 de la citada Ley Orgánica: Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

El consentimiento exigido en el apartado anterior no será preciso: Cuando la cesión está autorizada en una Ley, cuando se trate de datos recogidos de fuentes accesibles al público, cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros.

- **¿Puedo realizar envíos de propaganda electrónica a mis clientes?**

16-dic-2010

Desde el punto de vista de la normativa vigente, se deben identificar como Spam todas aquellas comunicaciones electrónicas del tipo que fueren (correo electrónico de Internet, mensajes cortos de telefonía móvil "SMS", etc) que el usuario recibe sin haber otorgado su consentimiento para ello, con las siguientes precisiones:

- ✓ Una comunicación electrónica no constituirá infracción en el caso de existir una relación contractual previa, y siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los emplee para el envío de comunicaciones comerciales referentes a productos o servicios de su propia

empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.

- ✓ Toda comunicación electrónica recibida sin consentimiento (y no existiendo una relación contractual previa), independientemente de su carácter comercial o no, es Spam. Sin embargo, la LSSICE (Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico) solo regula comunicaciones electrónicas comerciales. No obstante, cuando los destinatarios de las comunicaciones no comerciales son personas físicas, podría aplicarse la LOPD (tratamiento sin consentimiento).
- ✓ Queda, por tanto, una situación de Spam no recogida por la legislación española (tampoco por la directiva): cuando los destinatarios sean personas jurídicas y la comunicación electrónica no sea comercial. Existe numeroso Spam que no tiene carácter comercial, como aquel cuyo contenido son chistes, bromas, cadenas de favores y virus informáticos, por ejemplo, si bien en los casos constitutivos de delito existe la jurisdicción ordinaria.
- ✓ Se hace notar también que, en el caso en que los receptores de las comunicaciones comerciales sean personas jurídicas, la Agencia Española de Protección de Datos ostenta las competencias sancionadoras, ya que la LSSICE no hace distinción entre persona jurídica/física para los receptores de las comunicaciones electrónicas.

El envío de comunicaciones comerciales no deseadas por cualquier medio electrónico (e-mail, SMS, etc) es considerado Spam por la Ley de la Sociedad de los Servicios de Información (LSSI) y podría ser objeto de sanción.

- **¿Quiénes están obligados a notificar la creación, modificación o supresión de ficheros al Registro General de Protección de Datos?**

12-ene-2011

Están obligados a notificar la creación, modificación o supresión de ficheros para su inscripción en el RGPD, de acuerdo a lo dispuesto en la LOPD, aquellas personas físicas o jurídicas, de naturaleza pública o privada, u órgano administrativo, que procedan a la creación de ficheros que contengan datos de carácter personal.

Los ficheros de datos de carácter personal de titularidad privada serán notificados a la Agencia Española de Protección de Datos por la persona o entidad privada que pretenda crearlos, con carácter previo a su creación. El RGPD inscribirá el fichero si la notificación se ajusta a los requisitos exigibles. La inscripción del fichero en el RGPD es gratuita.

No se encuentran dentro del ámbito de aplicación de la LOPD, y por tanto no deben notificarse, los tratamientos referidos a personas jurídicas, ni a los ficheros que se limiten únicamente a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales. Tampoco deberán notificarse los ficheros con datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros.

La inscripción de un fichero deberá mantenerse actualizada en todo momento.

Cualquier modificación que afecte al contenido de la inscripción deberá ser previamente notificada a la AEPD o a las autoridades de control autonómicas competentes, a fin de proceder a su inscripción.

Cuando el responsable de un fichero decida su supresión, deberá notificarla a efectos de la cancelación de la inscripción.

- **¿Cuándo queda inscrito un fichero en el Registro General de Protección de Datos?**

03-nov-2011

El RGPD inscribe el fichero si la notificación se ajusta a los requisitos exigibles. En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.

Una vez inscrito el fichero en el RGPD, la Agencia notificará la resolución de inscripción del Director en la que se comunicará el código de inscripción asignado, a la dirección que a esos efectos se ha hecho constar en el apartado correspondiente de la Hoja de solicitud.

Igualmente, cuando los interesados así lo manifiesten expresamente en el formulario de notificación, podrán recibir por medios electrónicos la notificación de la resolución de inscripción, la comunicación de la necesidad de subsanar su solicitud, o cualquier otro escrito relacionado con la solicitud de inscripción de ficheros en el RGPD, para lo que deberán disponer de una dirección electrónica a efectos de notificaciones del Servicio de Notificaciones Electrónicas.

A través del Servicio de Notificaciones Electrónicas (https://notificaciones.060.es/PC_init.action), el Ministerio de Hacienda y Administraciones Públicas en colaboración con la Sociedad Estatal Correos y Telégrafos S.A. pone a disposición de cualquier persona física o jurídica que lo solicite la posibilidad de recibir de forma alternativa las notificaciones administrativas que por vía telemática pueda practicar las distintas Administraciones Públicas que actualmente reciben en papel. La suscripción a este servicio es voluntaria y tiene carácter gratuito.

En todo caso, la inscripción de un fichero en el RGPD, únicamente acredita que se ha cumplido con la obligación de notificación dispuesta en la LOPD, sin que de esta inscripción se pueda desprender el cumplimiento por parte del responsable del fichero del resto de las obligaciones previstas en la Ley y demás disposiciones reglamentarias.

- **¿El encargado de tratamiento debe constar inscrito en el RGPD?**

03-nov-2011

A efectos de inscripción, el Encargado del Tratamiento (art. 12 LOPD) no deberá figurar inscrito en el RGPD como entidad responsable de los ficheros o tratamientos. Únicamente el Responsable del Fichero deberá hacer constar los datos identificativos del Encargado del Tratamiento en el apartado 4 de la notificación.

Cuando la prestación de servicio implique que el fichero se encuentre ubicado en los locales del encargado del tratamiento, se podrá indicar este extremo cumplimentando el apartado de Encargado del tratamiento.

No obstante, si se desea que figuren inscritos más de un encargado en el apartado 4 se podrán notificar tantas inscripciones como encargados diferentes existan.

FUNCIONES Y OBLIGACIONES DEL PERSONAL

- **¿En qué consisten?**

13-ene-2011

El artículo 89 del Reglamento LOPD dispone:

Artículo 89.- Funciones y obligaciones del personal.

1.- Las funciones y obligaciones de cada una de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.

2.- El responsable del fichero adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

La descripción de las funciones del personal con acceso a datos de carácter personal tienen que estar incluidas en el documento de seguridad.

En todo caso, será necesario que el responsable del fichero y, en su caso, el encargado del tratamiento se aseguren que el personal con acceso a datos de carácter personal conoce las funciones y obligaciones que tiene con respecto al acceso a los datos de carácter personal, en particular, en lo relativo al deber de secreto y confidencialidad.

GESTION DE SOPORTES Y DOCUMENTOS

- **¿En qué consiste?**

04-nov-2011

El artículo 92 del Reglamento LOPD, determina como medida de seguridad de nivel básico la de identificar e inventariar los soportes y documentos que contengan datos de carácter personal, que sólo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.

La salida de soportes y documentos que contengan datos personales, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado.

En el caso de ficheros automatizados, la distribución de soportes (esto es, la salida de soportes físicos fuera de los locales de ubicación de los ficheros o sistemas de información) que contengan datos de carácter personal que requieran medidas de seguridad de nivel alto se realizará cifrando dichos datos evitando la manipulación durante su transporte.

En lo relativo a ficheros no automatizados, el artículo 114 del citado Reglamento LOPD señala que, siempre que se proceda al traslado físico de la documentación que recoja datos para los que resulten de

aplicación medidas de seguridad de nivel alto, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información.

COPIAS DE RESPALDO Y RECUPERACION DE DATOS

- **¿Qué son?**

04-nov-2011

El artículo 94 del Reglamento LOPD indica que el responsable de fichero se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos. Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho periodo no se hubiera producido ninguna actualización de los datos.

También se establecerán procedimientos para la recuperación de datos que deberán garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

El responsable del fichero debe proceder a verificar el correcto funcionamiento de estas copias al menos una vez cada seis meses.

Si se prevén hacer pruebas con datos reales, se hará previamente una copia de seguridad.

También es exigible para el caso de ficheros de imágenes de personas identificables.

NIVELES DE SEGURIDAD

- **¿Qué significa guardar las copias de respaldo en lugar físico diferente?**

04-nov-2011

Para los ficheros con datos de carácter personal sujetos a la obligación de implantar las medidas de nivel alto, el reglamento de desarrollo de la LOPD prevé la obligación de conservar una copia de respaldo de los

datos de estos ficheros y de los procedimientos de recuperación de los mismos en un lugar diferente del que se encuentran los equipos informáticos que los tratan (art. 102 Reglamento LOPD), con el fin de que no se encuentren sometidos a las mismas contingencias que pudiera sufrir el lugar habitual de almacenamiento en caso de un accidente o desastre, como por ejemplo, un incendio o una inundación.

En el caso de que no sea posible guardar una copia de los ficheros en un lugar distinto y no sujeto a los mismos riesgos, se deberán adoptar medidas complementarias para paliar el riesgo, tales como ubicar la copia en armarios ignífugos, de sistemas contraincendios, etc).

- **¿Qué nivel de seguridad tiene un fichero de curriculum vitae?**

04-nov-2011

El Artículo 81 del Reglamento que desarrolla la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre, dispone que los ficheros que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar aspectos de su personalidad o de su comportamiento y aquellos cuyo funcionamiento se rija por el artículo 29 de la LOPD (es decir, los relativos a solvencia patrimonial y crédito) deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio.

Teniendo en cuenta lo anterior, los ficheros que contengan curriculum vitae, que permiten fácilmente determinar las características laborales de los titulares de los datos, tiene que implementar el nivel de seguridad MEDIO.

- **¿Se deben ceder datos personales a la Inspección de Trabajo o de Hacienda?**

11-ene-2011

La comunicación de datos está; regulada en el artículo 11 de la LOPD y se prevé que los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

Las únicas excepciones a la norma general anterior vienen reguladas en el apartado 2 del propio artículo 11 y en el se prevé que no ser; necesario el consentimiento para la cesión:

- a) Cuando la cesión esté autorizada en una Ley.
 - b) Cuando sean datos recogidos de fuentes accesibles al público.
 - c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros.
 - d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas.
 - e) Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
 - f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos.
- **¿Debo entregar información de mis trabajadores a los representantes sindicales?**

11-ene-2011

La LOPD regula dentro de su artículo 11.1 la comunicación de datos, estableciendo con carácter general que los datos de carácter personal

objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

En el apartado 2 de dicho artículo 11 se prevén las excepciones (vistas en el apartado anterior).

En la materia que nos ocupa, la única cesión prevista de los datos referentes a los trabajadores sería la derivada de las facultades atribuidas a los representantes de los trabajadores (Comité de Empresa, Delegados de Personal o Junta de personal, según proceda).

En cuanto a la posibilidad de cesión de datos de los trabajadores a los representantes sindicales, y como consecuencia de la excepción de prestación del consentimiento en los supuestos en que una Ley así lo permita (artículo 11.2.a), debe ponderarse con el legítimo ejercicio de las funciones de control que se atribuyen por la Ley a los órganos de representación colectiva de los trabajadores en la empresa, conforme a las cuales el Estatuto de los Trabajadores dispone que dichos órganos tendrán derecho a acceder a cierta documentación de la empresa.

En el caso de cesión de los datos de los trabajadores, la misma únicamente podría entenderse amparada en caso de que se produjera en el ámbito de las funciones desarrolladas por los Delegados de Personal o el Comité de Empresa (según sea uno u otro al órgano de representación de los trabajadores), al encontrarse reconocido por el Estatuto de los Trabajadores el derecho de los representantes de los trabajadores (Delegados de Personal o Comité de Empresa) a acceder a determinados datos de los trabajadores en el ámbito de sus competencias, en caso contrario será necesario el consentimiento del interesado para proceder a la comunicación de sus datos.

- **La Mutua de accidentes solicita a la empresa copia de los TC2 de los trabajadores ¿Se le pueden entregar?**

11-ene-2011

En primer lugar, las Mutuas de Accidentes de Trabajo y Enfermedades Profesionales de la Seguridad Social son, según resulta del artículo 68 de la Ley General de la Seguridad Social, aprobada por Real Decreto Legislativo 1/1994, de 20 de junio, asociaciones debidamente autorizadas por el Ministerio de Trabajo y Asuntos Sociales, cuyo objeto principal es colaborar en la gestión de la Seguridad Social.

Los empresarios que formalicen la protección del personal a su servicio frente a las contingencias de accidente de trabajo y enfermedad profesional, pueden optar entre hacerlo en la entidad gestora correspondiente de la Seguridad Social o asociándose a una Mutua de Accidentes de Trabajo y Enfermedades de la Seguridad Social.

Por otro lado, la mencionada Ley General de la Seguridad Social regula la obligatoria afiliación a la misma de los “Trabajadores por cuenta ajena que presten sus servicios en las condiciones establecidas en el artículo 1.1 del Estatuto de los Trabajadores en las distintas ramas de actividad económica o asimilados a ellos, bien sean eventuales, de temporada o fijos, aun de trabajadores a domicilio.

De dichos preceptos legales deriva la obligación legal de comunicar por parte de los empresarios los datos de sus trabajadores a las indicadas Mutua de Accidentes de Trabajo y Enfermedades Profesionales de la Seguridad Social, cuando se haya optado por estas como medio de protección de tales contingencias.

- **Hemos creado una Base de Datos común para diversas empresas del mismo grupo ¿podemos utilizar todas las empresas del grupo la misma Base de Datos sin problemas?**

11-ene-2011

La comunicación de datos está regulada en el artículo 11 de la LOPD que prevé dentro de su apartado primero que los datos de carácter

personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

Las únicas excepciones a la norma general anterior vienen reguladas en el apartado 2 del propio artículo 11 (visto con anterioridad).

Fuera de estos supuestos, es preciso el consentimiento de los afectados.

En el caso planteado (creación de una base de datos común entre dos empresas), cuando una empresa accede a la base de datos de otra con personalidad jurídica propia se está produciendo una cesión de datos.

Cada empresa debe inscribir su propio fichero con datos personales y debe obtener el consentimiento de los titulares de los datos para que se produzca la cesión entre ambas.

- **Debo colocar cartel de aviso de videocámaras? ¿Dónde puedo conseguirlo?**

12-ene-2011

Lo importante y obligatorio es colocar el cartel de información de los derechos en materia de video vigilancia sin ser relevante su apariencia. Por lo tanto, sería conforme a la normativa si incluye la cámara e informa de los derechos que asisten a los ciudadanos y de la dirección del responsable del fichero para ejercitar esos derechos. (Artículo 3 de la Instrucción 1/2006 de video vigilancia).

- **¿La empresa instaladora tiene que ser una empresa de seguridad homologada al igual que en lo que respecta a las cámaras de seguridad o puedo optar por otro proveedor?**

12-ene-2011

Este Organismo únicamente tiene competencia para analizar si la recogida de imágenes a través de videocámaras puede ser contraria a la LOPD. Para dicho fin se ha dictado la INSTRUCCIÓN 1/2006, de 8 de noviembre, 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.

Hasta la entrada en vigor de Ley 25/2009, el 27 de diciembre (conocida como ley ómnibus), sólo era conforme a la legislación de protección de datos personales la utilización de dispositivos de video vigilancia si se había contratado con empresas de seguridad privada, debidamente autorizadas por el Ministerio del Interior.

La Ley citada reforma la Ley de Seguridad Privada, liberalizando esta actividad determinando que la venta, entrega, instalación o mantenimiento de estos sistemas podrá llevarse a cabo por particulares y empresas distintas de las de seguridad privada siempre que la instalación no implique una conexión con centrales de alarma.

- **¿Cuál es el tiempo mínimo/máximo para guardar las imágenes?**

12-ene-2011

De conformidad con el artículo 4 de la LOPD, las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras.

Sólo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal.

Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible

para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. Los datos serán cancelados en el plazo máximo de un mes desde su captación.

El responsable deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos y eviten su alteración, pérdida, tratamiento o acceso no autorizado. Asimismo cualquier persona que por razón del ejercicio de sus funciones tenga acceso a los datos deberá de observar la debida reserva, confidencialidad y sigilo en relación con las mismas.

DENUNCIAS/RECLAMACIONES

- **¿Cómo puedo poner una denuncia ante la Agencia?**

16-dic-2010

Se entiende por denuncia el acto por el que cualquier persona pone en conocimiento de un Órgano administrativo la existencia de un determinado hecho que pudiera constituir infracción administrativa (artículo 11.1.d) del Real Decreto 1398/1993, de 4 de agosto, por el que se regula el ejercicio de la potestad sancionadora).

Si Vd. dispone de pruebas o indicios que acrediten el incumplimiento de la Ley, puede ponerlo en conocimiento de esta Agencia. Para ello deberá presentar un escrito de denuncia - en los términos que se prevén en el artículo 70 de la Ley 30/1992 de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común - y enviarlo por correo (incluido el electrónico) o por fax al número 914455699.

Dicho escrito deberá contener:

- a) Nombre y apellidos del interesado y, en su caso, de la persona que lo represente, así como la identificación del medio preferente o del lugar que se señale a efectos de notificaciones.



- b) Hechos, razones y petición en que se concrete, con toda claridad, la solicitud.
- c) Lugar y fecha.
- d) Firma del solicitante o acreditación de la autenticidad de su voluntad expresada por cualquier medio.
- e) Órgano, centro o unidad administrativa a la que se dirige. (En su caso sería la Subdirección General de Inspección de Datos de esta Agencia, calle Jorge Juan, 6-28001-Madrid).

Igualmente, las denuncias deberán expresar la identificación de los presuntos responsables y acompañar los documentos o cualquier otro tipo de prueba o indicio que permita corroborar los hechos denunciados.

- **¿Tengo que presentar mi DNI para pedir que me cancelen o rectifiquen mis datos?**

16-dic-2010

En este caso, deberá dirigirse directamente al responsable del fichero en donde se encuentren sus datos personales, utilizando cualquier medio que permita acreditar el envío y la recogida de su solicitud (fax, burofax, correo ordinario, certificado o no, e-mail...), para el ejercicio de sus derechos, acompañando copia de su D.N.I. e indicando el fichero o ficheros a consultar. Puede sustituirse la presentación del documento de identidad por el uso de la firma electrónica identificativa.

- **¿Cómo puedo ejercitar mis derechos de acceso, rectificación, cancelación u oposición?**

16-dic-2010

Para presentar una reclamación - en los términos que se prevén en la Ley 30/1992 de Régimen Jurídico de las Administraciones Públicas y del



Procedimiento Administrativo Común - debe rellenar un escrito y enviarlo por correo (incluido el electrónico) o por fax al número 914455699.

Dicho escrito deberá contener:

- a) Nombre y apellidos del interesado y, en su caso, de la persona que lo represente, así como la identificación del medio preferente o del lugar que se señale a efectos de notificaciones.
- b) Hechos, razones y petición en que se concrete, con toda claridad, la solicitud.
- c) Lugar y fecha.
- d) Firma del solicitante o acreditación de la autenticidad de su voluntad expresada por cualquier medio.
- e) Órgano, centro o unidad administrativa a la que se dirige. (En su caso sería la Subdirección General de Inspección de Datos de esta Agencia, calle Jorge Juan, 6-28001-Madrid).

Igualmente, las reclamaciones deberán expresar la identificación de los presuntos responsables y acompañar los documentos o cualquier otro tipo de prueba o indicio que permita comprobar que Vd se ha dirigido previamente a los responsables de los ficheros solicitándole el ejercicio de un derecho

- **¿Qué es el Cloud Computing?**

10-jul-2012

El llamado Cloud Computing (o computación en nube) es un modelo de prestación de servicios tecnológicos que permite el acceso bajo demanda y a través de la red a un conjunto de recursos compartidos y configurables (como redes, servidores, capacidad de almacenamiento, aplicaciones y servicios) que pueden ser rápidamente asignados y liberados con una mínima gestión por parte del proveedor de servicios.

- **Características del Cloud Computing**

10-jul-2012

El modelo de Cloud Computing tiene las siguientes cinco características esenciales:

1. Autoservicio bajo demanda. El usuario puede acceder a capacidades de computación “en la nube” de forma automática conforme las necesita sin necesidad de una interacción humana con su proveedor o sus proveedores de servicios Cloud.
2. Múltiples formas de acceder a la red. Los recursos son accesibles a través de la red y por medio de mecanismos estándar que son utilizados por una amplia variedad de dispositivos de usuario.
3. Compartición de recursos. Los recursos de los proveedores son compartidos por múltiples usuarios, a los que se van asignando capacidades de forma dinámica según sus peticiones
4. Elasticidad. Los recursos se asignan y liberan rápidamente, muchas veces de forma automática, lo que da al usuario la impresión de que los recursos a su alcance son ilimitados y están siempre disponibles.
5. Servicio medido. El proveedor es capaz de medir, a determinado nivel, el servicio efectivamente entregado a cada usuario, de forma que tanto proveedor como usuario tienen acceso transparente al consumo real de los recursos.

- **Aplicación de la normativa sobre protección de datos**

10-jul-2012

Con carácter previo es necesario resaltar que el cumplimiento de la legislación de protección de datos es un aspecto esencial a la hora de contratar servicios Cloud por parte de un responsable del tratamiento.

Debe considerarse que las modalidades de computación y las modalidades de servicios condicionan la aplicación de los preceptos correspondientes de la LOPD y de su Reglamento.

En cualquier caso, a los responsables del tratamiento que contraten servicios de Cloud Computing (art. 3.d) de la LOPD y art. 5.1.q) del RLOPD), les corresponde la decisión sobre la finalidad, el contenido y el uso del tratamiento, así como la decisión sobre optar por la computación en la nube y sobre su modalidad. Por su parte, el prestador de servicios de Cloud Computing tendrá la naturaleza de encargado del tratamiento (art. 3.g) de la LOPD y (art. 5.1.i) del RLOPD, pues en definitiva trata datos personales por cuenta del responsable.

- **Aspectos esenciales técnico-jurídicos del contrato de servicios**

10-jul-2012

La LOPD establece en su art. 12.2 que la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito. Por tanto, el contrato de prestación de servicios entre el responsable del tratamiento y su proveedor de servicios Cloud ha de incorporar las previsiones citadas.

En este sentido, el encargado está obligado a seguir las instrucciones del responsable del fichero en el tratamiento de los datos. Una forma de que el cliente indique estas instrucciones puede ser la de adoptar decisiones sobre el tipo de nube con la que se le prestarán los servicios y sobre las modalidades de servicios que contrata.

Para ello, deberá haber solicitado y obtenido previamente información suficiente sobre ambos aspectos.

Es importante destacar que el responsable del tratamiento es responsable de seleccionar como encargado del tratamiento a alguien que cumpla los requisitos legalmente establecidos. Esta responsabilidad se extiende a la subcontratación de servicios. Así, cuando el encargado

del tratamiento subcontrate alguna actividad propia del tratamiento de los ficheros, dicha subcontratación habrá de recogerse en el contrato de prestación de servicios entre el responsable y el encargado, siendo necesaria una autorización del primero en los casos de subcontratación sobrevenida no prevista en el contrato (art. 21 RLOPD).

Una fórmula que puede utilizarse a tal efecto es que el cliente autorice los servicios susceptibles de subcontratación (p.ej. servicios de “hosting”) y tenga permanentemente a su disposición una relación actualizada de las entidades subcontratadas y de los países donde operan, (por ejemplo en una página web a la que tenga acceso o a través de otras alternativas que le permitan estar informado).

En definitiva, para garantizar la seguridad jurídica del servicio Cloud contratado, el contrato de prestación de servicios suscrito entre el despacho y el proveedor ha de recoger, un conjunto mínimo de cláusulas, entre las que cabe destacar las siguientes:

- ✓ Régimen de los datos. Es esencial que el contrato especifique que el proveedor no puede disponer de los datos personales ni hacer uso de los mismos para ningún fin que no esté expresamente autorizado por el responsable del tratamiento.
- ✓ Cumplimiento de legislación de protección de datos de carácter personal. El proveedor ha de asumir expresamente el papel de encargado del tratamiento de los ficheros de datos de carácter personal que el despacho decida trasladar “a la nube”, con todas las obligaciones propias de tal figura tal y como se recogen en la legislación española y europea.
- ✓ Seguridad en el acceso. El proveedor ha de garantizar que la información solo será accesible al responsable del tratamiento que contrata sus servicios, y a quienes éste determine con los perfiles de acceso correspondientes.
- ✓ Integridad y conservación. El proveedor ha de disponer de los mecanismos de recuperación ante desastres, continuidad en el

servicio y copia de seguridad necesarios para garantizar la integridad y conservación de la información.

- ✓ Disponibilidad. El proveedor ha de garantizar una elevada disponibilidad del servicio, así como comprometerse a organizar las paradas programadas para mantenimiento con la suficiente antelación y dando aviso de las mismas al despacho.
- ✓ Portabilidad. El proveedor ha de obligarse, a la terminación del servicio, a entregar toda la información al despacho en el formato que se acuerde, para que éste pueda almacenarla en sus propios sistemas o bien trasladarla a los de un nuevo proveedor, en el plazo más breve posible y con total garantía de la integridad de la información.

10. ENLACES DE ORGANISMOS DE PROTECCIÓN DE DATOS

NACIONALES:

- Autoridad Catalana de Protección de Datos: www.apdcat.net
- Agencia de Protección de Datos de la Comunidad de Madrid: www.madrid.org/apdcm
- Agencia Vasca de Protección de Datos: www.avpd.euskadi.net/s04-4319/es/
- Congreso: www.congreso.es
- Ministerio de Justicia: www.mju.es
- Poder Judicial: www.poderjudicial.es
- Portal del Ciudadano: www.administracion.es
- Senado: www.senado.es
- Tribunal Constitucional: www.tribunalconstitucional.es

INTERNACIONALES:

- **Instituciones europeas**
 - ✓ Autoridad Común de Control de Europol: <http://europoljsb.ue.eu.int/default.asp?lang=ES>

- ✓ Autoridad Común de Control de Shengen: www.schengen-isa.dataprotection.org
- ✓ Comisión Europea: <http://europa.eu.int>
- ✓ Consejo de Europa: www.coe.int
- ✓ Consejo UE: <http://ue.eu.int>
- ✓ Grupo del artículo 29 : http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm
- ✓ Parlamento Europeo: www.europarl.eu.int
- ✓ Supervisor Europeo de Protección de Datos: <http://www.edps.eu.int>
- ✓ Tribunal de Justicia UE: <http://curia.europa.eu/es/>

- **Autoridades de Protección de Datos en Europa**

- ✓ Alemania : www.datenschutz.de www.bfd.bund.de
- ✓ Andorra : <https://www.apda.ad/>
- ✓ Austria: www.dsk.gv.at
- ✓ Bélgica: www.privacycommission.be
- ✓ Bulgaria: www.cpdp.bg
- ✓ Chipre: www.dataprotection.gov.cy
- ✓ Dinamarca: www.datatilsynet.dk
- ✓ Eslovaquia: www.dataproyection.gov.sk
- ✓ Eslovenia: www.varuh-rs.si
- ✓ Estonia: www.dp.gov.ee
- ✓ Finlandia: www.tietosuoja.fi
- ✓ Francia - versión española: www.cnil.fr/index.php?id=5
- ✓ Francia: www.cnil.fr
- ✓ Grecia : www.dpa.gr
- ✓ Guernsey: www.dataprotection.gov.gg
- ✓ Holanda: www.cbpweb.nl
- ✓ Hungría: abiweb.obh.hu/abi
- ✓ Irlanda: www.dataprivacy.ie



- ✓ Islandia: www.personuvernd.is
- ✓ Italia: www.garanteprivacy.it
- ✓ Jersey: www.dataprotection.gov.je
- ✓ Letonia: www.dvi.gov.lv
- ✓ Liechtenstein: www.sds.llv.li
- ✓ Lituania: www.ada.lt
- ✓ Luxemburgo: www.cnpd.lu
- ✓ Malta: www.dataprotection.gov.mt
- ✓ Noruega : www.datatilsynet.no
- ✓ Polonia: www.giodo.gov.pl
- ✓ Portugal: www.cnpd.pt
- ✓ Reino Unido: www.dataprotection.gov.uk
- ✓ República Checa: www.uoou.cz
- ✓ Rumania: www.avp.ro
- ✓ Suecia: www.datainspektionen.se
- ✓ Suiza: www.edsb.ch

- **Iberoamérica**

- ✓ Argentina: <http://www.jus.gov.ar/dnppd>
- ✓ Chile - Servicio de Registro Civil e Identificación:
<http://www.registrocivil.cl> <http://www.modernizacion.cl>
- ✓ Colombia: <http://www.defensoria.org.co>
- ✓ México: <http://www.ifai.org.mx>
- ✓ Nicaragua: <http://www.conicyt.gob.ni>

- **Agencias, organizaciones e Instituciones de protección de datos en otros países**

- ✓ Australia: www.privacy.gov.au
- ✓ Canadá: www.privcom.gc.ca
- ✓ EEUU (FTC, en español):
www.ftc.gov/ftc/spanishinfo/consumer.htm
- ✓ EEUU (Departamento de Seguridad Interior): www.dhs.gov



- ✓ Hong Kong: www.pco.org.hk
- ✓ Naciones Unidas: www.unhchr.ch/hchr_un.htm
- ✓ Nueva Zelanda : www.privacy.org.nz
- ✓ OCDE: www.oecd.org/sti/security-privacy

11. FORMULARIOS

Los principales formularios son los siguientes:

- **Acceso:**

A. DERECHO DE ACCESO.

A.1. EJERCICIO DEL DERECHO DE ACCESO (1).

DATOS DEL RESPONSABLE DEL FICHERO(2).

Nombre / razón social..... Dirección de la Oficina /
Servicio ante el que se ejercita el derecho de acceso:
C/Plaza..... nº..... C.Postal.....
Localidad..... Provincia..... Comunidad
Autónoma..... C.I.F. /D.N.I.....

DATOS DEL INTERESADO O REPRESENTANTE LEGAL(3).

D. / D^a., mayor de
edad, con domicilio en la
C/Plaza..... nº.....,
Localidad..... Provincia..... C.P.....
Comunidad Autónoma..... con D.N.I....., del que
acompaña copia, por medio del presente escrito ejerce el derecho de acceso, de
conformidad con lo previsto en el artículo 15 de la Ley Orgánica 15/1999, de 13 de
diciembre, de Protección de Datos de Carácter Personal y en los artículos 27 y 28 del



Real Decreto 1720/2007, de 21 de diciembre, por el que se desarrolla la misma, y en consecuencia,

SOLICITA,

Que se le facilite gratuitamente el derecho de acceso a sus ficheros en el plazo máximo de un mes a contar desde la recepción de esta solicitud, y que se remita por correo la información a la dirección arriba indicada en el plazo de diez días a contar desde la resolución estimatoria de la solicitud de acceso.

Asimismo, se solicita que dicha información comprenda, de modo legible e inteligible, los datos de base que sobre mi persona están incluidos en sus ficheros, los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los mismos, los cesionarios y la especificación de los concretos usos y finalidades para los que se almacenaron.

En.....a.....de.....de 20.....

Firmado

1 Se trata de la petición de información sobre los datos personales incluidos en un fichero. Este derecho se ejerce ante el responsable del fichero (Organismo Público o entidad privada) que es quien dispone de los datos. La Agencia Española de Protección de Datos no dispone de sus datos personales sino solamente de la ubicación del citado responsable si el fichero está inscrito en el Registro General de Protección de Datos.

2 Si Vd. desconoce la dirección del responsable del fichero puede dirigirse a la Agencia Española de Protección de Datos para solicitar esta información en el teléfono 901 100 099.

3 También podrá ejercerse a través de representación legal, en cuyo caso, además del DNI del interesado, habrá de aportarse DNI y documento acreditativo auténtico de la representación del tercero.

RECTIFICACIÓN



B. DERECHO DE RECTIFICACIÓN.

B.1. EJERCICIO DEL DERECHO DE RECTIFICACIÓN (1)

DATOS DEL RESPONSABLE DEL FICHERO (2).

Nombre / razón social..... Dirección
de la Oficina / Servicio ante el que se ejercita el derecho de rectificación:
C/Plaza..... nº.....
C.Postal..... Localidad..... Provincia.....
Comunidad Autónoma..... C.I.F./D.N.I.

DATOS DEL AFECTADO O REPRESENTANTE LEGAL(3).

D. / D^a....., mayor de edad, con
domicilio en la C/Plaza..... nº ,
Localidad..... Provincia..... C.P.....
Comunidad Autónoma..... con D.N.I....., del que
acompaña copia, por medio del presente escrito ejerce el derecho de rectificación sobre los
datos anexos, aportando los correspondientes justificantes, de conformidad con lo previsto en
el artículo 16 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de
Carácter Personal y en los artículos 31 y 32 del Real Decreto 1720/2007, de 21 de diciembre,
por el que se desarrolla la misma y en consecuencia,

SOLICITA,

Que se proceda a acordar la rectificación de los datos personales sobre los cuales se ejercita el
derecho, que se realice en el plazo de diez días a contar desde la recogida de esta solicitud, y
que se me notifique de forma escrita el resultado de la rectificación practicada.

Que en caso de que se acuerde, dentro del plazo de diez días hábiles, que no procede acceder
a practicar total o parcialmente las rectificaciones propuestas, se me comunique
motivadamente a fin de, en su caso, solicitar la tutela de la Agencia Española de Protección de
Datos, al amparo del artículo 18 de la citada Ley Orgánica 15/1999.

Que si los datos rectificadas hubieran sido comunicados previamente se notifique al
responsable del fichero la rectificación practicada, con el fin de que también éste proceda a
hacer las correcciones oportunas para que se respete el deber de calidad de los datos a que se
refiere el artículo 4 de la mencionada Ley Orgánica 15/1999.

En.....a.....de.....de 20.....



Firmado:

1. Consiste en la petición dirigida al responsable del fichero con el fin de que los datos personales respondan con veracidad a la situación actual del afectado.
2. Si Vd. desconoce la dirección del responsable del fichero puede dirigirse a la Agencia Española de Protección de Datos para solicitar esta información en el teléfono 901 100 099.
3. También podrá ejercerse a través de representación legal, en cuyo caso, además del DNI del interesado, habrá de aportarse DNI y documento acreditativo auténtico de la representación del tercero.

CANCELACIÓN

C. DERECHO DE CANCELACIÓN.

C.1. EJERCICIO DEL DERECHO DE CANCELACIÓN (1)

DATOS DEL RESPONSABLE DEL FICHERO (2)

Nombre / razón social..... Dirección de la Oficina
/ Servicio ante el que se ejercita el derecho de cancelación:
C/Plaza..... nº..... C.Postal.....
Localidad..... Provincia..... Comunidad
Autónoma..... C.I.F./D.N.I.

DATOS DEL AFECTADO O REPRESENTANTE LEGAL(3)

D. / D^a, mayor de edad, con
domicilio en la C/Plaza..... nº.....,
Localidad..... Provincia..... C.P.....
Comunidad Autónoma..... con D.N.I....., del que
acompaña copia, por medio del presente escrito ejerce el derecho de cancelación, de
conformidad con lo previsto en el artículo 16 de la Ley Orgánica 15/1999, de 13 de diciembre,
de Protección de Datos de Carácter Personal y en los artículos 31 y 32 del Real Decreto
1720/2007, de 21 de diciembre, por el que se desarrolla la misma y en consecuencia,

SOLICITA,



Que se proceda a acordar la cancelación de los datos personales sobre los cuales se ejercita el derecho, que se realice en el plazo de diez días a contar desde la recogida de esta solicitud, y que se me notifique de forma escrita el resultado de la cancelación practicada.

Que en caso de que se acuerde dentro del plazo de diez días hábiles que no procede acceder a practicar total o parcialmente las cancelaciones propuestas, se me comunique motivadamente a fin de, en su caso, solicitar la tutela de la Agencia Española de Protección de Datos, al amparo del artículo 18 de la citada Ley Orgánica 15/1999.

Que si los datos cancelados hubieran sido comunicados previamente se notifique al responsable del fichero la cancelación practicada con el fin de que también éste proceda a hacer las correcciones oportunas para que se respete el deber de calidad de los datos a que se refiere el artículo 4 de la mencionada Ley Orgánica 15/1999.

En.....a.....de.....de 20.....

Firmado:

(1) Consiste en la petición de cancelación de un dato que resulte innecesario o no pertinente para la finalidad con la que fue recabado. El dato será bloqueado, es decir, será identificado y reservado con el fin de impedir su tratamiento.

(2) Si Vd. desconoce la dirección del responsable del fichero puede dirigirse a la Agencia Española de Protección de Datos para solicitar esta información en el teléfono 901 100 099.

(3) También podrá ejercerse a través de representación legal, en cuyo caso, además del DNI del interesado, habrá de aportarse DNI y documento acreditativo auténtico de la representación del tercero.

OPOSICIÓN

DERECHO DE OPOSICION

E.1. EJERCICIO DEL DERECHO DE OPOSICIÓN (1)

DATOS DEL RESPONSABLE DEL FICHERO (2)

Nombre / razón social:

Dirección de la Oficina / Servicio ante el que se ejercita el derecho de oposición:

Calle/Plaza..... nº..... C.Postal.....

Localidad..... Provincia.....

Comunidad Autónoma..... C.I.F. /D.N.I.....

DATOS DEL INTERESADO O REPRESENTANTE LEGAL (3)



D. / D^a....., mayor de edad, con domicilio en la Calle/Plaza..... nº..... Localidad..... Provincia..... C.P..... Comunidad Autónoma..... con D.N.I....., del que acompaño copia, por medio del presente escrito ejerzo el derecho de oposición, de conformidad con lo previsto en los artículos 6.4, 17 y 30.4 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal y en los artículos 34 y 35 del Real Decreto 1720/2007, de 21 de diciembre, que la desarrolla y en consecuencia,

EXPONGO,

(Describir la situación en la que se produce el tratamiento de sus datos personales y enumerar los motivos por los que se opone al mismo)

Para acreditar la situación descrita, acompaño una copia de los siguientes documentos:
(Enumerar los documentos que adjunta con esta solicitud para acreditar la situación que ha descrito)

SOLICITO,

Que sea atendido mi ejercicio del derecho de oposición en los términos anteriormente expuestos.

En.....a.....de.....de 20.....

Firmado:

(1) Se trata de la solicitud de oposición al tratamiento de los datos personales incluidos en un fichero. Este derecho se ejerce ante el responsable del fichero (Organismo Público o entidad privada) que es quien dispone de los datos. La Agencia Española de Protección de Datos no dispone de sus datos personales sino solamente de la ubicación del citado responsable si el fichero está inscrito en el Registro General de Protección de Datos.

(2) Si Vd. desconoce la dirección del responsable del fichero puede dirigirse a la Agencia Española de Protección de Datos para solicitar esta información en el teléfono 901 100 099.

(3) También podrá ejercerse a través de representación legal, en cuyo caso, además del DNI del interesado, habrá de aportarse DNI y documento acreditativo auténtico de la representación del tercero.



MODELO DE DENUNCIA

DATOS DEL AFECTADO (1)

D. / D^a., mayor de edad, con domicilio en..... nº.....,
Localidad..... Provincia..... C.P.....
Comunidad Autónoma....., con D.N.I./Pasaporte nº.....

DATOS DEL PRESUNTO RESPONSABLE

Nombre / Razón social:
Oficina / Servicio (en su caso):
Domicilio: nº..... ,
Localidad..... Provincia.....
C.P.....
Comunidad Autónoma..... C.I.F. /D.N.I.....

De acuerdo con lo previsto en la normativa vigente, pone en conocimiento del Director de la Agencia Española de Protección de Datos los siguientes HECHOS:

.....
.....

Que justifica con la DOCUMENTACIÓN ANEXA que se relaciona a continuación:

Documento nº 1.....
Documento nº 2.....
Documento nº 3.....
.....

En virtud de lo expuesto, SOLICITA que se dicte acuerdo de inicio de procedimiento sancionador o de infracción de las Administraciones Públicas o se incoen actuaciones con objeto de determinar si concurren circunstancias que justifiquen tal iniciación y que, en cualquier caso, se me notifique el acuerdo que se adopte, de conformidad con lo previsto en el Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado mediante Real Decreto 1720/2007, de 21 de diciembre.

En.....a.....de..... de 20.....

Firmado:

SR. DIRECTOR DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
C/ Jorge Juan, 6.- 28001 MADRID

(1) La denuncia puede presentarse por el propio afectado, en cuyo caso acompañará copia del DNI, o cualquier otro documento que acredite la identidad y sea considerado válido en derecho.

También puede concederse la representación legal a un tercero, en cuyo caso, además, se deberá aportar DNI y documento acreditativo de la representación de éste.

LOGO VIDEOVIGILANCIA

