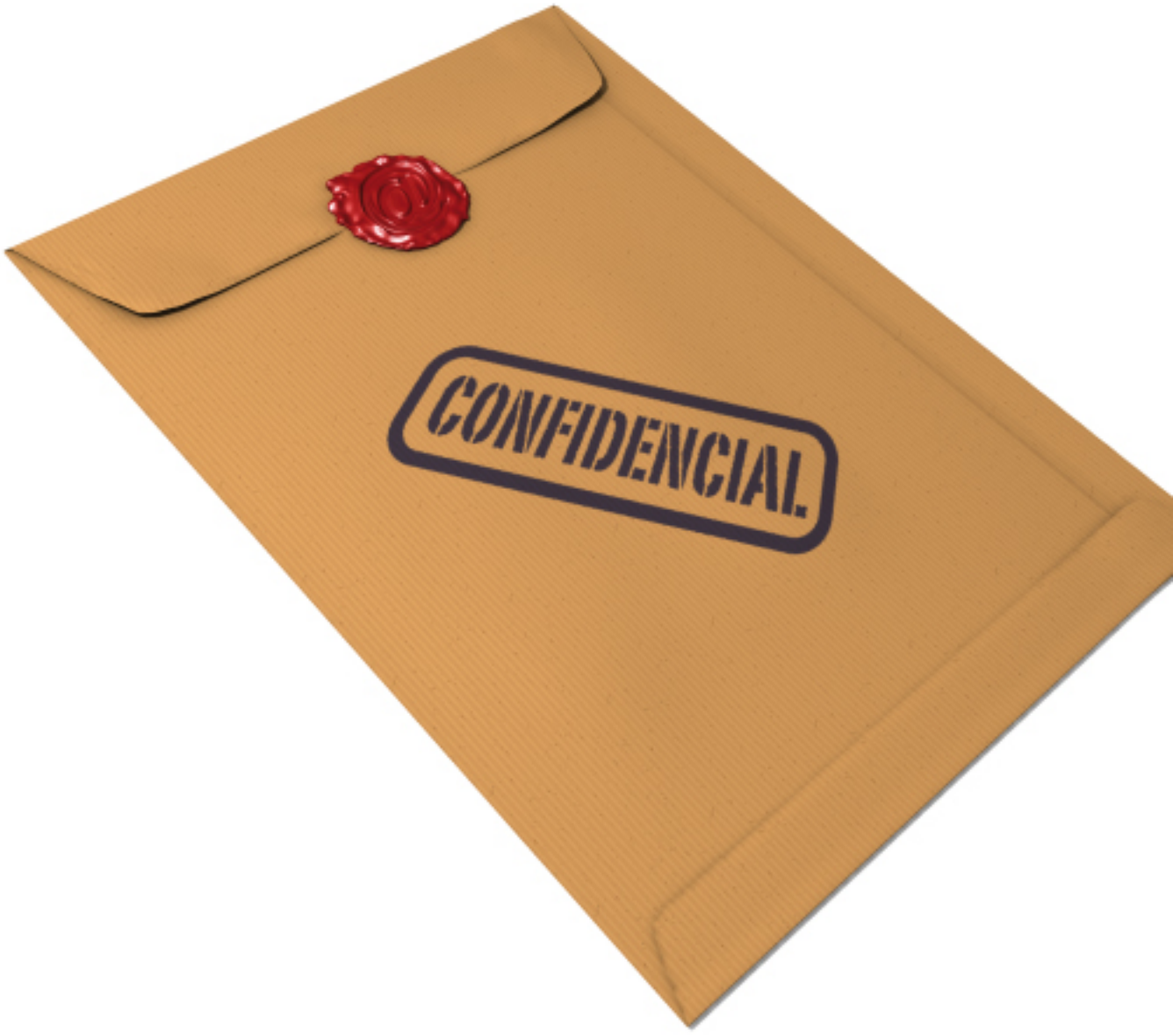
CUADERNOS PRÁCTICOS DE GESTIÓN

A qué me obliga la ley de protección de datos



XUNTA DE GALICIA

A qué me obliga la Ley de Protección de Datos

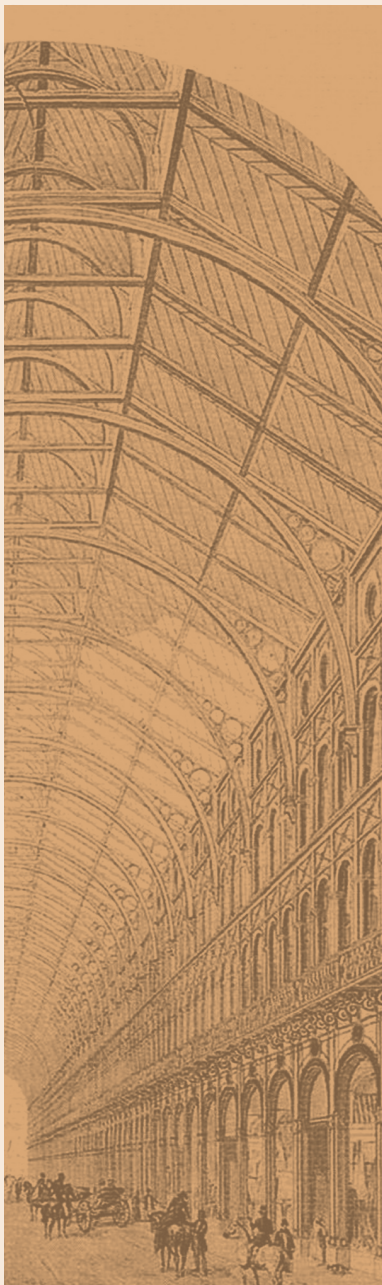
CUADERNOS PRÁCTICOS. GESTIÓN EMPRESARIAL

AUTOR	PROMOVE CONSULTORIA E FORMACIÓN SLNE
COORDINACIÓN	Roberto Vieites Rodríguez (CEEI Galicia, S.A)
EDITA	C.E.E.I GALICIA, S.A. (BIC GALICIA)
PORTADA	Producciones khartum SL
DISEÑO Y MAQUETACIÓN	gifestudio.com
(C) da edición	C.E.E.I GALICIA, S.A. (BIC GALICIA)
DEPÓSITO LEGAL	
IMPRIME	

Santiago de Compostela, CEEI GALICIA, S.A. 2012

ÍNDICE

1 Introducción



1 Introducción

Introducción

Esta publicación forma parte de la colección ***"Cuadernos prácticos de gestión empresarial",*** un nuevo recurso que Bic Galicia pone a disposición de emprendedores, empresarios y técnicos e apoyo a la creación de empresas.

La colección está integrada por una serie documentos en la que se abordan distintas áreas temáticas sobre actividades relacionadas con la gestión empresarial:

- Desarrollar la política comercial de la empresa y medir su efectividad.
- Diseñar la planificación estratégica de la empresa.
- Mejorar la implementación y seguimiento de la política de recursos humanos.
- Gestionar los recursos financieros.
- Implementar elementos 2.0 en la empresa.
- Etc.

En su elaboración se han utilizado las publicaciones de Bic Galicia, hibridando sus distintos contenidos para crear un nuevo producto que de respuesta a preguntas o temas concretos y específicos de la gestión empresarial.

Por ello, todos los cuadernos prácticos cuentan con un apartado específico en el que se indica qué herramientas de Bic Galicia permitirán ampliar información sobre el tema analizado.

Metodología

El proceso de elaboración de los cuadernos, desde el punto de vista metodológico, se ha basado en:

- La utilización de fuentes secundarias, especialmente aquellas herramientas, publicaciones y documentos desarrollados y diseñados por Bic Galicia y otras fuentes secundarias especializadas siempre que el contenido de las mismas aporte valor añadido al cuaderno.

- La utilización de información obtenida directamente a través de fuentes de información primaria, concretamente aportaciones, opiniones, consejos y sugerencias realizadas por expertos en la materia tratada en el cuaderno.

A través de esta nueva colección Bic Galicia pretende:

- Responder de forma concreta y específica a las demandas de información o dudas de las personas emprendedoras y empresarios facilitando el acceso a la información desagregada en diferentes publicaciones.

- Mejorar la difusión y el conocimiento a los recursos ya existentes de Bic Galicia, que serían las fuentes sobre las que ampliar información y profundizar en el tema a analizar.

- Facilitar la gestión empresarial y la implementación de medidas y acciones concretas necesarias en el ámbito empresarial.

- Optimizar el uso de sus recursos recuperando y reutilizando su base de publicaciones para desarrollar nuevos contenidos que respondan a nuevas necesidades de emprendedores, empresarios y técnicos de promoción económica.

Objetivos de este cuaderno

Este cuaderno recoge aspectos básicos de la gestión y aplicación de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, en las empresas. Se explican de forma sencilla los principales aspectos que regula la norma además de presentar modelos tipo para alguna de las acciones que se deben de realizar

- Conceptos básicos

- La gestión de ficheros y su seguridad

- Los derechos de los titulares de los datos

- Trasferencias internacionales de datos

- Sanciones

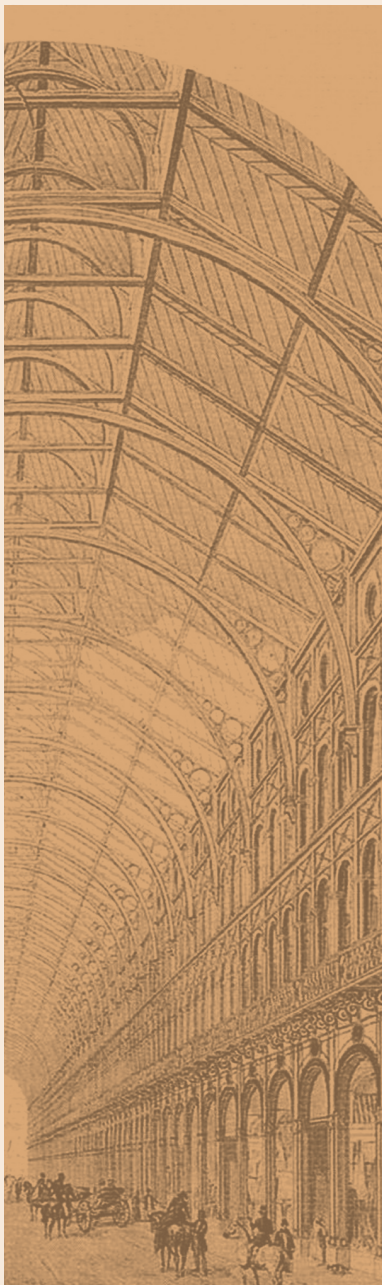
- .....

1.1 Para saber más

Para ampliar la información sobre la Ley Orgánica de Protección de Datos y sobre su gestión, obligaciones y sanciones para los empresarios se podrán consultar los siguientes recursos de Bic Galicia en su Portal www.bicgalicia.org

- Fichas informativas. Protección de datos
- Manual práctico de gestión: Conceptos jurídicos básicos

2 La protección de datos



2 La protección de datos

2.1 Agencia Española de Protección de Datos (AEPD)

Naturaleza y funciones:

La Agencia Española de Protección de Datos es, tal y como se recoge en el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos, un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con la plena independencia de las Administraciones Públicas en el ejercicio de sus funciones, relacionándose con el Gobierno a través del Ministerio de Justicia.

Su principal función es velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial que los ciudadanos puedan ejercer los derechos de información, acceso, rectificación, oposición y cancelación de sus datos de carácter personal y el control del cumplimiento por parte de los responsables de sus ficheros de sus obligaciones.

Entre sus funciones más importantes están la de inscribir los ficheros de datos de carácter personal en el Registro General de Protección de Datos, atender las peticiones y reclamaciones formuladas por las personas afectadas, requerir a los responsables y los encargados de los tratamientos para que adopten las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de la Ley Orgánica de Protección de Datos, realizar labores de inspección sobre los ficheros que tengan datos de carácter personal y ejercer la potestad sancionadora.

Esa facultad de sancionar unida a que las infracciones pueden ser sancionadas con multas que van desde los 900 hasta los 600.000 euros, hacen que la obligación legal de protección de los datos de carácter personal adquiera una dimensión similar dentro de la empresa a las obligaciones fiscales o de la Seguridad Social.

Normativa reguladora:

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 1720/2007 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.
- Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.

2.2 La Ley Orgánica de Protección de Datos (LOPD)

Antecedentes

Esta ley tiene su precedente en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de los datos de carácter personal, la cual nacía para hacer frente a los riesgos que para los derechos de la personalidad puede suponer el acopio y tratamiento de datos por medios informáticos; el avance de la tecnología puso de manifiesto que en una sociedad cada vez más conectada y con mayor capacidad de almacenamiento de datos, era casi imposible conseguir borrar "nuestra historia"; por lo que se hacía imprescindible articular modos para proteger el honor y la intimidad de las personas. Sin embargo, aquella primera ley que tenía por objeto limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal, se vio pronto superada por el avance de las nuevas tecnologías y en especial por la expansión de internet.

La ley

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (en adelante, LOPD), entró en vigor el 14 de enero del año 2000, teniendo 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.

¿Cuándo se aplica la ley?

- Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento (la práctica totalidad de las empresas que operan en nuestro país).
- Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.
- Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

La ley NO se aplica a:

- A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
- A los ficheros sometidos a la normativa sobre protección de materias clasificadas.
- A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos.

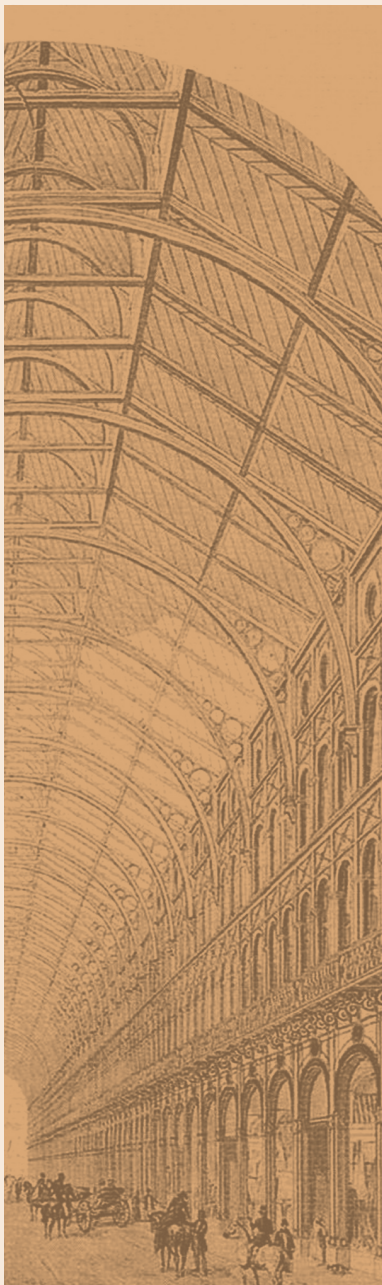
Desarrollo de la ley

La ley es desarrollada por el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de 13 de diciembre, de protección de datos de caracter personal.

2.3 ¿A qué me obliga la LOPD?

- A notificar a la Agencia Española de Protección de Datos (AEPD) la creación de ficheros de datos de carácter personal y a inscribir los ficheros en el Registro General de Protección de Datos.
- A informar previamente a las personas cuyos datos se solicitan.
- A recabar el consentimiento de dichas personas, tanto para el tratamiento de los datos personales como para proceder a cederlos a terceros.
- A establecer las medidas de seguridad necesarias para proteger los datos de carácter personal.
- A regular mediante un contrato la realización de tratamientos de los datos por cuenta de un tercero.
- A atender debidamente el ejercicio de los derechos de acceso, rectificación, cancelación y oposición por los interesados.
- A formar al responsable de seguridad y a los usuarios que tienen acceso a los datos de carácter personal.

3 Conceptos básicos sobre la protección de datos decarácter personal



3 Conceptos básicos sobre la protección de datos de carácter personal

3.1 Los ficheros de datos personales

Qué se considera datos de carácter personal:

Se considera datos de carácter personal a cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables:

- Datos de carácter identificativo: NIF/CIF, teléfono, dirección electrónica, etc.
- Datos de carácter personal: estado civil, fecha de nacimiento, edad, lugar de nacimiento, nacionalidad, sexo, etc.
- Datos de circunstancias sociales: servicio militar, propiedades, aficiones, estilo de vida, pertenencia a asociaciones, etc.
- Datos académicos o profesionales: formación, titulación, historial académico, experiencia profesional, etc.
- Datos profesionales: profesión, puesto de trabajo, vida laboral, etc.
- Datos de información comercial: actividades y negocios, licencias comerciales, suscripciones a publicaciones, etc.
- Económico- financieros: ingresos, rentas, inversiones, préstamos, avales, datos bancarios, etc.
- Especialmente protegidos: ideología, afiliación sindical, religión, creencias, salud, vida sexual, etc.

Qué es un fichero:

Es todo conjunto organizado de datos de carácter personal, sin importar el soporte en el que se encuentren o la forma en que dichos datos se organicen y almacenen; a modo de ejemplos, la agenda donde guardamos los teléfonos de nuestros clientes y proveedores, las bases de datos de proveedores y clientes, sus expedientes, los currículos que se utilizan en la selección y promoción del personal.

3.2 Quién es quién en la protección de datos

- El interesado es la persona titular de los datos, que sean objeto del tratamiento.
- El responsable del fichero o tratamiento es toda persona física o jurídica, pública o privada u órgano administrativo que, solo o conjuntamente con otros, decida sobre la finalidad, contenido y uso del tratamiento.
- El encargado del tratamiento es la persona física o jurídica, autoridad pública o cualquier otro organismo que trate los datos personales por cuenta del responsable del tratamiento.
- El responsable de seguridad es la persona encargada de que se adopten y cumplan todas las medidas de seguridad requeridas según el nivel de protección de los datos.
- El cesionario es la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos.
- El usuario es el personal al servicio del responsable del fichero o encargado del tratamiento, que tenga acceso a los datos de carácter personal como consecuencia de tener encomendadas tareas de utilización material de los datos almacenados o que se almacenarán en los ficheros.

La relación entre el responsable del archivo y el encargado del tratamiento se debe regular en un **contrato por escrito**, en el que se debe establecer que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones dadas por el responsable del tratamiento, que no los aplicará o utilizará para fines distintos a los que figuren en el contrato, ni los comunicará a otras personas. También se deben establecer las medias de seguridad a cumplir por el encargado del tratamiento.

3.3 Actuaciones sobre los datos de carácter personal

Las actuaciones pueden ser tratamiento de datos, cesión y comunicación de datos y cancelación de datos.

El tratamiento de datos

Son aquellas operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

La cesión o comunicación de datos

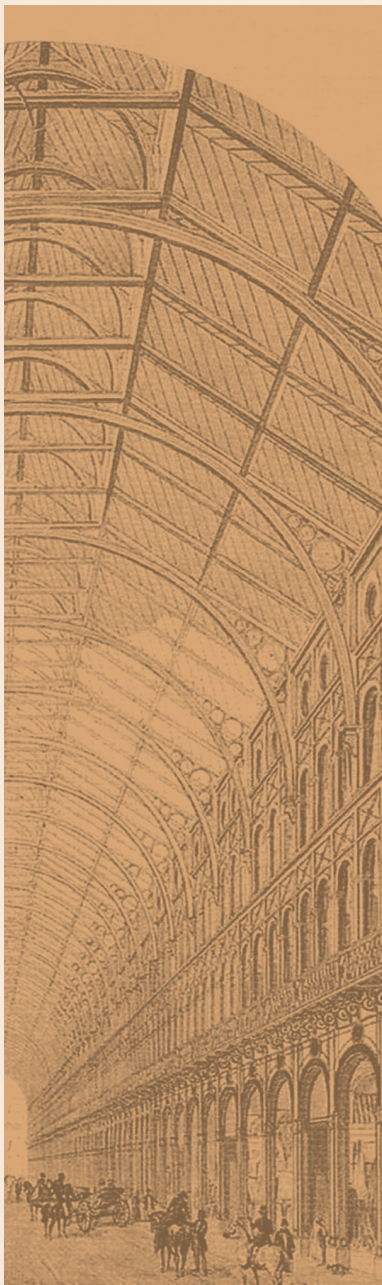
Es el tratamiento de datos que supone su revelación a una persona distinta del interesado.

La cancelación de los datos

Es el procedimiento por el cual el responsable del fichero cesa en el uso de los datos; implicará que se bloqueen los datos y su reserva 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.

Si la gestión de nóminas, contratación, tramitación de documentación a la seguridad social, etc. está subcontratada a una gestoría se considera a ésta como E**ncargado del tratamiento de los datos de carácter personal** mientras que tu empresa se considera **Responsable del tratamiento**. Deberás redactar un contrato.

4 Inscripción de los ficheros



4 Inscripción de los ficheros

4.1 Qué se debe de hacer antes de inscribir un fichero

4.1.1 Estándares de calidad

El responsable del fichero deberá asegurarse que los datos contenidos en dichos ficheros cumplen los siguientes estándares de calidad:

Los datos personales deben de ser:

- Adecuados.
- Pertinentes
- No excesivos
- No pueden usarse para finalidades diferentes de aquellas para las que fueron recogidos
- Exactos y puestos al día, de no ser exactos o estar incompletos deben ser eliminados o sustituidos por los correctos.
- Útiles, desde que dejen de ser útiles para la función para la que fueron recogidos deben eliminarse.

Principios relativos a la calidad de los datos; los datos de carácter personal:

- Deberán ser tratados de forma leal y lícita. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.
- Sólo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento.
- No podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

4.1.2 Información previa al interesado

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 los datos.
- 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 el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de tránsito, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

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.

El artículo 18 del Reglamento de desarrollo de la LOPD obligaba a que se conservase la acreditación del cumplimiento del deber de información mientras persistiera el tratamiento de los datos del interesado, dicho artículo fue anulado por la sentencia de la Sala 3ª del Tribunal Supremo del 15 de julio de 2010.

4.1.3 Consentimiento del interesado

Debe de recabarse el consentimiento del titular de los datos para poder proceder a su tratamiento.

Cuando se solicite el consentimiento debe de referirse a un tratamiento o tratamientos concretos y debe de quedar constancia de cuál es la finalidad para la que se recaban dichos datos.

Si no consta de forma inequívoca cual es la finalidad para la que se recaban esos datos el consentimiento se considerará nulo y por tanto no válido.

En caso de recogida de datos de menores de 14 años el consentimiento deberá de ser prestado por padres o tutores; si es mayor de 14 años podrá prestar directamente el consentimiento, salvo en los casos que la ley disponga otra cosa. En ningún caso se podrá obtener de un menor datos que permitan

obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo (información económica, actividad profesional de los padres) sin el consentimiento de éstos, con la excepción de los datos de identificación y dirección de la madre, padre o tutor, al objeto de conseguir su autorización.

Salvo que el consentimiento tenga que constar de forma expresa, se entenderá que el afectado consiente el tratamiento de los datos si después de informarle debidamente de la inclusión de sus datos en el fichero no muestra su negativa en un plazo de 30 días.

Hay que dar al afectado por el tratamiento de sus datos de carácter personal la posibilidad de revocar su consentimiento a través de un medio sencillo y gratuito:

- Se consideran que cumplen dichos requisitos un envío prefranqueado al responsable del tratamiento o la puesta a disposición de un número de teléfono gratuito.

- No lo cumplen cuando se exige el envío de cartas certificadas, utilización de servicios de telecomunicaciones o cualquier otro medio que implique un coste adicional al interesado.

Aunque la ley no exige recabar el consentimiento por escrito, es altamente recomendable, ya que la carga de probar la existencia de dicho consentimiento recae en el responsable del tratamiento de los datos.

4.2 Modelos de cláusulas tipo

4.2.1 Cláusula de información y consentimiento expresa

En cumplimiento con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, le informamos que sus datos personales serán tratados y quedarán incorporados en ficheros cuyo titular es (nombre de la empresa), registrados en la Agencia Española de Protección de Datos, cuya finalidad es (poner la finalidad para la que se crea el fichero).
Usted consiente expresamente la recogida y el tratamiento de los mismos para la citada finalidad.
En todo caso, puede ejercitar los derechos de acceso, rectificación, cancelación y oposición remitiendo un escrito junto a la fotocopia de su DNI a (dirección a la que pueden remitir los escritos).
Le rogamos que en el supuesto de producirse alguna modificación en sus datos de carácter personal, nos lo comunique con el fin de mantener actualizados los mismos.

4.2.2 Cláusula de información y consentimiento genérica

Los datos personales facilitados serán incorporados a un fichero titularidad de (nombre de la empresa) con la finalidad de (poner la finalidad perseguida con la creación del fichero). Asimismo, una finalidad es la de poder enviar, de manera periódica, información y publicidad sobre nuestros productos y servicios. Si en el plazo de 30 días, usted no nos manifiesta su negativa mediante (envío de la comunicación prefranqueada que se adjunta/llamada al número 900xxxxxxx), entenderemos que presta su consentimiento para el tratamiento de los datos facilitados.
De acuerdo con la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, puede ejercer los derechos de acceso, rectificación, cancelación y, en su caso, oposición, enviando una solicitud por escrito acompañada de la fotocopia de su DNI a la siguiente dirección (poner dirección).

4.2.3 Cláusula de consentimiento para correos electrónicos

Este mensaje y sus ficheros anexos son confidenciales. Los mismos contienen información reservada que no puede ser difundida y se amparan en la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico 34/2002 de 11 de julio (LSSICE). Si usted ha recibido este correo por error, reenvíelo al remitente y elimínelo de su sistema. No deberá copiar el mensaje ni divulgar su contenido.
Su dirección de correo electrónico junto a sus datos constan en un fichero inscrito en el Registro General de Protección de Datos, cuyo Responsable es XXXXXXX. La finalidad es mantener el contacto con Usted. Podrá ejercitar sus derechos de acceso, rectificación, cancelación u oposición dirigiéndose por escrito a XXXXX.

4.3 Cómo inscribir los ficheros

4.3.1 Notificar a la AEPD de la existencia de los ficheros

¿Quién debe de notificar?

Cualquier persona física o jurídica que vaya a proceder a la creación de un fichero que contenga datos de carácter personal debe de proceder a su notificación a la AEPD.

¿Qué se debe de notificar?

La creación de un fichero con datos de carácter personal que resulta necesario para el logro del objeto o finalidad de la empresa, junto a los datos referentes al responsable y encargado del tratamiento, dirección donde se pueden ejercer los derechos de la LOPD, nombre de los ficheros, su finalidad, el nivel de seguridad de los datos y categorías de los interesados.

¿Cuándo se debe de notificar?

La notificación del fichero debe de realizarse antes de proceder a su creación.

Descarga del formulario NOTA:
https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/Notificaciones_tele/obtencion_formulario/index-ides-idphp.php

¿Cómo se debe de notificar?

A través del sistema de notificaciones telemáticas de la AEPD (sistema NOTA) y de su formulario que permite tanto la presentación telemática de la notificación con certificado digital como su descarga para su presentación en papel.

¿Dónde se debe de notificar?

- Telemáticamente:
  - Con certificado digital a través de la página web de la AEPD: www.agpd.es.
  - Sin certificado digital remitiendo a la Agencia la Hoja de solicitud correspondiente al envío realizado debidamente firmada.

En formulario de papel ante la AEPD.

¿Por qué se debe de notificar?

Si no se notifica la existencia de un fichero podría incurrirse en falta leve o grave, quedando sujeto al régimen sancionador previsto en la LOPD, que prevé multas en estos supuestos de entre 900 a 300.000 euros.

4.3.2 Cómo cumplimentar el formulario NOTA

Datos necesarios para cumplimentar el formulario NOTA

La notificación deberá indicar la identificación del responsable del fichero, la identificación del fichero, sus finalidades y los usos previstos, el sistema de tratamiento empleado en su organización, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, la indicación del nivel de medidas de seguridad básico, medio o alto exigible, y en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales de datos.

¿Cómo cumplimentar el formulario NOTA?

- Identificación del responsable de los ficheros:

Nombre o denominación social de la persona responsable del fichero, recordar que es quien decide sobre la finalidad, contenido y uso que se va a dar a ese fichero, no pueden tener la consideración de responsables del fichero las personas vinculadas mediante una relación contractual de carácter laboral con el responsable del fichero.

Hay que indicar la actividad a la que se dedica la empresa y los demás datos identificativos (dirección, CIF/NIF y si se desea se puede aportar el teléfono, fax o correo electrónico del responsable de los ficheros).

- Dirección a la que se pueden dirigir los titulares de los datos para ejercer sus derechos de oposición, acceso, rectificación y cancelación:

Es el lugar (oficina, dirección postal o apartado de correos) donde pueden dirigirse los titulares de los datos para ejercer los derechos amparados por la LOPD, solo debe indicarse expresamente cuando sea distinto al domicilio del responsable del fichero.

- Identificación del encargado del tratamiento:

Cuando exista un tercero que realiza el tratamiento por cuenta del responsable, e implique una ubicación del fichero fuera del domicilio de este (como ejemplos la asesoría laboral, la empresa que se encargue del mantenimiento informático).

Recordar que ese tratamiento de los datos por cuenta de terceros debe de estar regulada contractualmente, recomendándose su constancia por escrito ya que es el medio más sencillo para acreditar su celebración.

Los trabajadores de la empresa no tienen la consideración de encargados del tratamiento a efectos de la LOPD.

- Identificación de los ficheros y su finalidad:

Debe indicarse un nombre que identifique el fichero (por ejemplo: agenda y contactos, clientes, proveedores, expedientes, currículos).

Hay que describir de modo detallado la finalidad del fichero y el uso que se va a hacer de él (a título de ejemplo descripción de la finalidad y el uso del fichero de agenda y contactos: contiene datos que permiten mantener el contacto por teléfono, fax, correo electrónico u ordinario con el personal, clientes, proveedores y otros contactos de terceros, en general necesarios para el mantenimiento de la relación con los mismos).

- Origen y procedencia de los datos y colectivos o categorías de interesados:

Deberá indicarse de donde proceden los datos contenidos (del propio interesado o su representante legal, registros públicos, otras personas físicas, fuentes accesibles al público, entidad privada o administraciones públicas).

Las fuentes accesibles al público son aquellos ficheros que pueden ser consultados por cualquier persona sin más limitación que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público: el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica, las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo, los diarios y boletines oficiales y los medios de comunicación.

Hay que especificar a qué colectivo o categoría pertenecen los titulares de los datos: trabajadores, clientes, proveedores, pacientes, etc…

- Tipos de datos, estructura y organización del fichero:

Hay que indicar ante qué tipo de datos nos encontramos:

  - Datos especialmente protegidos: ideología, afiliación sindical, religión y creencias. Importante recordar que este tipo de datos solo se pueden tratar cuando se ha conseguido el consentimiento expreso y por escrito del afectado.

  - Otros datos especialmente protegidos: origen racial o étnico, salud y vida sexual.

  - Datos de carácter identificativo: nombre y apellidos, dirección, teléfono, firma, DNI, tarjeta sanitaria, número de afiliación a la Seguridad Social, imagen/voz, marcas físicas o firma electrónica.

  - Otros datos: características personales, circunstancias sociales, académicos, profesionales, económicos, financieros, etc…

- Señalar cuál es el sistema de tratamiento de los datos (modo en que organiza la información o utiliza un sistema de información): automatizado, manual o mixto.

- Medidas de seguridad:

Hay que indicar el nivel de medidas de seguridad exigible al fichero. Existen tres niveles: básico, medio, alto.

- Cesión o comunicación de datos:

Cuando se prevea que se van a realizar cesiones o comunicaciones de datos, hay que indicar a que categoría pertenece el destinatario de la cesión (seguridad social, registros públicos, administración tributaria, notarios, bancos, etc…).

No se considera cesión de datos la prestación de un servicio por el encargado del tratamiento.

- Transferencias internacionales:

Cuando se realicen tratamientos de datos fuera del territorio del Espacio Económico Europeo, hay que indicar a qué países y los destinatarios de los datos.

4.3.3 Inscribir los ficheros en el Registro General de Protección de Datos.

Si la notificación realizada a través del formulario NOTA se ajusta a los requisitos exigibles el Registro General de Protección de Datos procederá sin más trámites a la inscripción del fichero. Lo habitual es que la inscripción se notifique por escrito, sin embargo, si transcurrido un mes desde la presentación de la solicitud de la inscripción la AEPD no hubiera resuelto sobre esta, se entenderá a todos los efectos inscrito el fichero.

Si no se cumplen los requisitos deberán pedirnos por escrito que se completen los datos o que se proceda a la subsanación de los defectos apreciados.

La inscripción en el Registro solo acredita que se ha cumplido con la obligación de notificación prevista en la LOPD, debiendo el responsable del tratamiento de los datos cumplir además con el resto de las obligaciones previstas en la Ley y en las disposiciones reglamentarias.

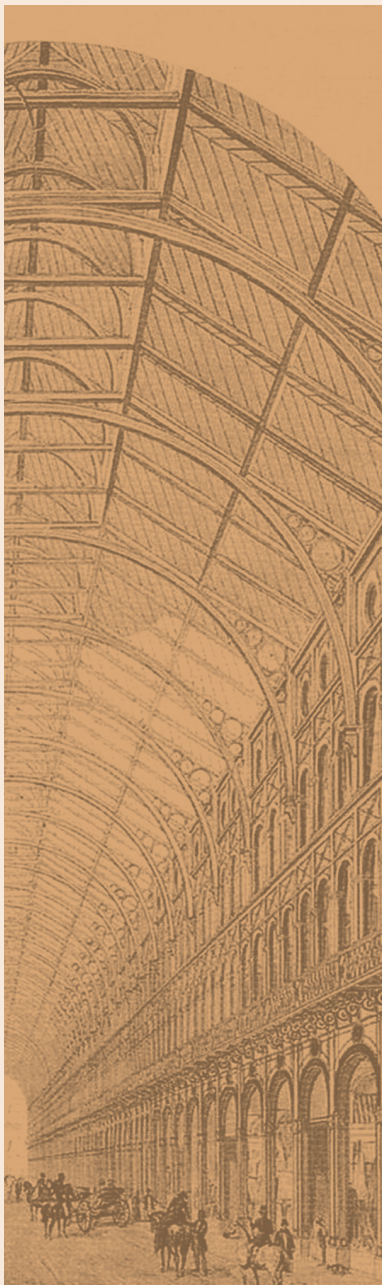
4.4 Modificación y supresión de ficheros

La inscripción del fichero deberá encontrarse actualizada en todo momento. Cualquier modificación de la inscripción de un fichero debe de ser notificada a la AEPD.

Cuando se proceda a suprimir un fichero también debe de ser notificado a la AEPD, la cual previa comprobación de que dicha notificación es correcta procederá a la cancelación de la inscripción correspondiente a dicho fichero.

Tanto la modificación como la supresión se notificarán a través del formulario NOTA, pudiendo utilizar los mismos medios de envío que para la inscripción.

5 La seguridad de los datos de carácter personal



5 La seguridad de los datos de carácter personal

5.1 Los niveles de seguridad y a los datos a los que se aplica

Las medidas de seguridad exigibles se adaptan a tres niveles: alto, medio y básico

Nivel alto:

- Ficheros que contengan datos referentes a la ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
- Los recabados para fines policiales sin el consentimiento de la persona afectada.
- Los que contengan datos derivados de actos de violencia de género.

Nivel medio:

- Ficheros que contengan datos sobre la comisión de infracciones administrativas o penales.
- Los que posean quienes se dediquen a la prestación de servicios de información sobre solvencia patrimonial o crédito y siempre que los hayan obtenido de las administraciones públicas, de fuentes accesibles al público o que los datos se facilitasen por el interesado o con su consentimiento.
- Los de la Agencia Tributaria en tanto tengan relación con el ejercicio de sus potestades tributarias.
- Ficheros que posean las entidades financieras en relación con los servicios financieros que presten.
- Los que en ejercicio de sus competencias posean la Seguridad Social y las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.
- Ficheros que permitan evaluar la personalidad de los ciudadanos.

Nivel básico:

- Es aplicable a todos los ficheros o tratamientos de datos de carácter personal.

5.2 Documento de seguridad

El responsable del fichero tiene la obligación de elaborar un documento de seguridad, en él deberán de figurar las medidas de índole técnica y organizativa adaptadas a la normativa que el personal con acceso a los sistemas de información deberán cumplir obligatoriamente.

El documento de seguridad tendrá el carácter de documento interno de la empresa.

Puede tenerse un único documento de seguridad para todos los ficheros, uno para cada fichero, también pueden elaborarse documentos de seguridad agrupando ficheros según el sistema de tratamiento o atendiendo a criterios organizativos del responsable.

El documento de seguridad debe de mantenerse en todo momento actualizado y revisarse siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o como consecuencia de los controles periódicos realizados. Siempre se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

5.2.1 Contenido mínimo del documento de seguridad

➲ Ámbito de aplicación del documento detallando los recursos protegidos

Señalar quienes son las personas obligadas a cumplir las medidas de seguridad (personal con acceso a los datos, encargados de tratamiento…) y los ficheros a los que se aplican dichas medidas de seguridad. También deben de relacionarse los recursos que deben de hallarse protegidos, sea porque contienen físicamente los medios con los que se tratan los datos, los medios en sí o que sirven para acceder directa o indirectamente al fichero (como ejemplos, los locales donde se encuentren físicamente ubicados los ficheros, los ordenadores desde los que se puede tener acceso a los ficheros, el entorno de red, los servidores, las aplicaciones que permitan tener acceso a datos de carácter personal, etc…).

➲ Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar la seguridad

Deben de establecerse las medidas de seguridad concretas aplicables a los ficheros (control de accesos, tanto físicos como lógicos; registros de accesos; copias de seguridad; registro de incidencias; destrucción de ficheros físicos…); procedimientos de actuación (procedimiento de control de accesos, para la entrada o salida de datos de los ficheros, en caso de ejercicio de los derechos de acceso, rectificación, oposición o cancelación del titular de los datos, de copia de documentos, de archivo, etc…), reglas y es-

tándares (autorización previa para almacenar datos en dispositivos portátiles para realizar trabajo fuera de los locales pertenecientes al responsable del fichero, políticas de uso del correo electrónico, etc…).

- **Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en el fichero:**

Puede nombrarse uno o varios responsables de seguridad, si la estructura de la empresa es compleja (sea porque el desarrollo de las tareas afecta a varias áreas concretas o porque la empresa tenga diversos establecimientos) pueden delegarse funciones derivadas tanto de las obligaciones del responsable del tratamiento, como del responsable de seguridad.

- **Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan**:

Hay que identificar el fichero, describirlo, indicar su finalidad, los campos del fichero (qué tipo de datos incluye), el nivel de seguridad que le corresponde a ese fichero (básico, medio o alto), calidad de quien efectúa el tratamiento del fichero (responsable del fichero, responsable de seguridad, encargado de tratamiento…). Deben describirse los sistemas de información que los tratan (servidores y puestos de trabajo que alojan el fichero, aplicaciones informáticas vinculadas al tratamiento del fichero, …).

- **Procedimiento de notificación, gestión y respuesta ante las incidencias:**

Deberá elaborarse un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal; se creará un registro donde se hará constar que tipo de incidencia se ha producido (pérdida de un expediente, cesión no consentida de datos, acceso a un fichero por persona no autorizada, salida de datos sin autorización, etc…), momento en que se produce o detecta la incidencia, la persona que la notifica, los efectos derivados de esta y qué medidas se han tomado para paliar las posibles consecuencias producidas por la existencia de la incidencia.

- **Procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados:**

Debe de establecerse un procedimiento por el cual se realicen copias de seguridad al menos una vez por semana. También se establecerán procedimientos de recuperación de datos que permitan reconstruir los ficheros tal y como estaban antes del momento de su destrucción o pérdida.

- **Procedimientos para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos:**

En caso de que se proceda al traslado de documentación o soportes de un fichero deben de establecerse medidas que impidan que se acceda o modifique la información en él contenida.

Es muy importante que se establezca el procedimiento de destrucción de ficheros, si están contenidos en papel debe de preverse su destrucción mediante el uso de una destructora de papel y prohibir expresamente su reutilización cuando contengan datos de carácter personal. En caso de desechado y reutilización de soportes de ficheros automatizados deben de comprobarse su correcto borrado o su destrucción de modo que se impida el acceso a la información contenida en dichos soportes o su posible recuperación.

5.2.2 Otros contenidos en casos especiales:

➲ Ficheros a los que se les deben aplicar medidas de seguridad de nivel medio y alto:

Identificación del responsable o responsables de seguridad y establecer la realización de controles periódicos para verificar el cumplimiento de lo establecido en el documento de seguridad.

➲ Cuando exista un tratamiento de datos por cuenta de terceros:

El documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, identificación del responsable y período de vigencia del encargo.

5.3 Medidas de seguridad

Se distinguen las medidas de seguridad a adoptar según se trate de ficheros y tratamientos automatizados o no automatizados.

5.3.1 Ficheros y tratamientos automatizados

Las distintas medidas de seguridad que deben de adoptarse variarán en función de si los datos que protegen son de nivel básico, medio o alto.

5.3.1.1 Gestión de soportes

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

➲ Identificación, inventario y almacenamiento.

- Nivel alto: La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

- Nivel básico: Debe de realizarse un inventario de los soportes que contienen datos de carácter personal en el que conste la identificación de cada uno de ellos, la información que almacenan y realizar una relación del personal autorizado a acceder a dichos soportes.

Salidas de soportes.

- Nivel alto-Cifrado en la distribución de soportes y portátiles:
  La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

- Nivel básico-Autorización para la salida de soportes:
  La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.

- Nivel medio-Registro de salida de soportes:
  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.

- Dispositivos portátiles
  Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

Entrada de soportes.

- Nivel medio: Se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, 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 entrega que deberá estar debidamente autorizada.

Desechado y reutilización.

- Nivel básico: Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

5.3.1.2 Control de acceso

➲ **Control de acceso físico:**

- Nivel medio:
  Solo 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.

➲ **Control de acceso lógico:**

- Nivel básico:
  El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos –que serán a los recursos que precisen para el desarrollo de sus funciones- y establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.
  Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.
  En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

➲ **Identificación y autenticación:**

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

- Nivel básico:
  El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios, estableciendo 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.
  Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.

➲ **Registro de accesos:**

- Nivel alto:
  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.
  En el caso de que el acceso haya sido autorizado, será preciso guardar la información que

permita identificar el registro accedido.
Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.
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.
No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

- Que el responsable del fichero o del tratamiento sea una persona física.
- Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad.

5.3.1.3 Copias de seguridad y recuperación de datos.

- Nivel básico:
  Deberán realizarse copias de respaldo como mínimo una vez a la semana, salvo que no se hubiera producido ninguna actualización de los datos.
  Hay que establecer 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. Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.
  El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.
  Se deberá realizar una copia de seguridad antes de realizar pruebas con datos reales.

- 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, para dicha copia se dispondrán las mismas medidas de seguridad que para los datos y los equipos que los tratan.

5.3.1.4 Acceso a través de redes de telecomunicaciones.

- Nivel básico:
  Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

- Nivel alto:
  La transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

5.3.1.5 Gestión de incidencias.

- Nivel básico:
  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, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

- Nivel medio:
  En caso de datos de nivel medio y alto deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.
  Para la ejecución de los procedimientos de recuperación de los datos, será necesaria la autorización del responsable del fichero.

5.3.1.6 Pruebas con datos reales.

- Nivel básico:
  Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad. Previamente a las pruebas deberá haberse realizado una copia de seguridad.

5.3.1.7 Trabajo fuera de los locales.

- Nivel básico:
  Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, la cual tendrá que constar en el documento de seguridad, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.
  La autorización podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas.

5.3.1.8 Ficheros temporales o copias de trabajo de documentos.

- Nivel básico:
  Aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda y serán borrados o destruidos una vez que haya dejado de ser necesarios para los fines que se crearon.

5.4 Ficheros y tratamientos no automatizados

A los ficheros no automatizados se aplicarán las mismas previsiones que a los ficheros automatizados respecto a los niveles de seguridad de los datos, al encargado del tratamiento, las prestaciones de servicios sin acceso a datos personales, delegación de autorizaciones, régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento, copias de trabajo de documentos, registro de incidencias, control de acceso y gestión de soportes.

Y de forma particular se aplicarán las siguientes medidas de seguridad:

5.4.1 Almacenamiento de la documentación.

- Nivel básico:
  Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

- 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. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.
  Si esto no fuera posible debido a las características del local donde se encuentran, el responsable adoptará medidas alternativas que se incluirán en el documento de seguridad.

5.4.2 Custodia de los soportes.

- Nivel básico:
  Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

5.4.3 Copia o reproducción.

- Nivel alto:
  La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad. Una vez desechadas debe procederse a su destrucción de forma que se evite el acceso a la información contenida en las copias o su recuperación posterior.

5.4.4 Criterios de archivo.

- Nivel básico:
  El archivo que se efectúe de los soportes o documentos deberá garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

5.4.5 Control de accesos.

- Nivel alto:
  El acceso a la documentación se limitará exclusivamente al personal autorizado. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios. Si acceden al documento personas distintas a las autorizadas deberá quedar adecuadamente registrado.

5.4.6 Traslado de documentación.

- Nivel alto:
  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.

5.5 Funciones y obligaciones del personal

5.5.1 De los usuarios.

- **Usuario:** sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

- **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.

- **A título de ejemplo:** Cerrar o bloquear las sesiones al término de la jornada laboral o cuando se ausente de forma temporal de su puesto de trabajo, obtener autorización del responsable de seguridad para proceder a copiar ficheros con datos de carácter personal en algún soporte, guardar los documentos con datos de carácter personal en lugar seguro, solicitar autorización del responsable de seguridad para trasladar soportes o documentos con datos de carácter personal.

5.5.2 De los responsables.

➲ Del responsable del fichero o tratamiento

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

- Obligaciones del responsable del fichero: Notificar a la AEPD los ficheros que se creen, su modificación y su eliminación; recabar el consentimiento de los interesados para el tratamiento de datos, verificar que se cumple el deber de información, formar al personal respecto a las medidas de seguridad a adoptar, etc…

➲ Del responsable de seguridad

- Cuando existan datos a los que haya de aplicarse 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. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.

- Algunas de las funciones principales del responsable de seguridad:

  - Revisar que los datos que se traten sean adecuados, pertinentes y no excesivos en relación con las finalidades para las que se hayan obtenido, que no se usen finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos y que dichos datos sean exactos y estén al día.

  - Comprobar que se cumple con el deber de información y que se cuenta con el consentimiento del titular de los datos.

  - Implantar el procedimiento para atender el ejercicio de los derechos de acceso, rectificación, oposición y cancelación y atender las peticiones al respecto de los titulares de los datos.

  - Implantar controles periódicos para verificar el cumplimiento de lo dispuesto en el documento de seguridad y revisar dichos controles.

  - Definir y documentar las obligaciones del personal.

- Establecer mecanismos que permitan identificar a los usuarios que acceden al sistema, que limiten la posibilidad de intentos reiterados de acceso no autorizados y que los usuarios solo puedan acceder a los datos necesarios para sus funciones.

- Autorizar las recuperaciones de datos y la salida de soportes fuera de los locales.

- Realizar copias de respaldo, al menos semanalmente y verificar cada seis meses el procedimiento para su realización.

- Establecer un procedimiento de notificación y gestión de las incidencias.

5.6 Controles: Auditoría y controles periódicos

Auditoría

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 del presente título.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas.

El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.

Controles periódicos

Los ficheros a los que sean de aplicación las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto deben de ser sometidos a controles periódicos para verificar que se cumple lo establecido en el documento de seguridad.

5.7 Modelos de formulario

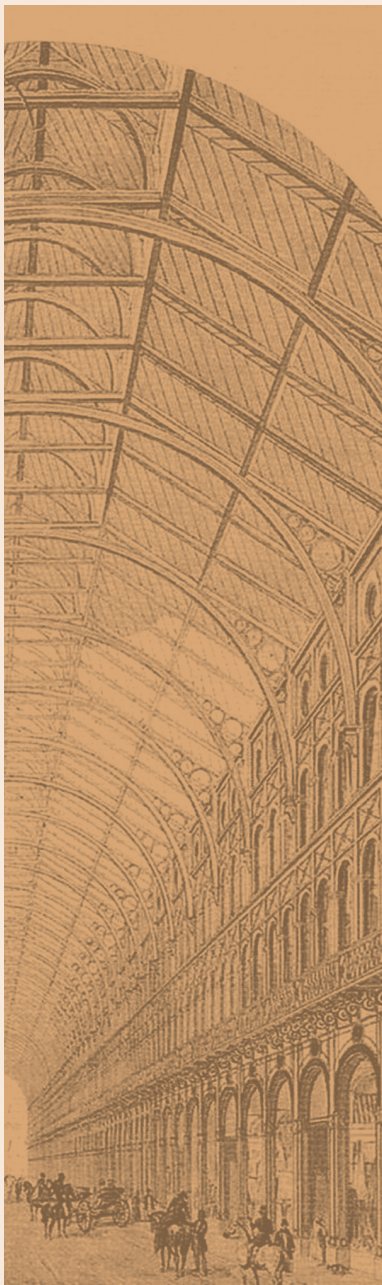
5.7.1 Formulario de registro de entrada y salida de soportes

REGISTRO DE ENTRADA Y SALIDA DE SOPORTES						
REGISTRO DE ENTRADA						
Tipo de documento o soporte	Fecha Hora	Emisor	Núm. documentos o soportes enviados	Tipo de información	Forma de envío	Responsable recepción
REGISTRO DE SALIDA						
Tipo de documento o soporte	Fecha Hora	Emisor	Núm. documentos o soportes enviados	Tipo de información	Forma de envío	Responsable recepción

5.7.2 Formulario de registro de incidencias

REGISTRO DE INDICENCIAS		
Núm. Incidencia:	Fecha/hora:	Persona que notifica:
Dirigido a:		
Tipo de incidencia: Observaciones: Efectos derivados:		
Medidas correctoras aplicadas:		
SOLO PARA DATOS DE NIVEL MEDIO:		
Procedimiento de recuperación de datos: SI NO Persona que ejecutó el proceso de recuperación de datos: Datos que ha sido necesario grabar manualmente:		

6 Derechos de los titulares de los datos (A.R.C.O.)



6 Derechos de los titulares de los datos (A.R.C.O.)

6.1 Disposiciones comunes

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, recoge una serie de derechos fundamentales de los ciudadanos, que le proporcionan al titular de la información personal la posibilidad de efectuar un control material de sus datos.

6.1.1 Condiciones para el ejercicio de los derechos

Los derechos de acceso, rectificación, cancelación y oposición son personalísimos y serán ejercidos por el afectado, acreditando su identidad.

Como excepciones a esta indicación se consideran los siguientes casos:

- Cuando el afectado se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de estos derechos, podrán ejercitarse por su representante legal, en cuyo caso será necesario que acredite tal condición.

- Los derechos también podrán ejercitarse a través de representante voluntario, expresamente designado para el ejercicio del derecho. En ese caso, deberá constar claramente acreditada la identidad del representado, mediante la aportación de copia de su Documento Nacional de Identidad o documento equivalente, y la representación conferida por aquél.

Los derechos serán denegados cuando la solicitud sea formulada por persona distinta del afectado y no se acreditase que la misma actúa en representación de aquél.

6.1.2 Condiciones generales para el ejercicio de los derechos

- Los derechos de acceso, rectificación, cancelación y oposición son derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

- Deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos, no pudiendo suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.

- No se consideran conformes con la normativa de protección de datos que se establezca como medio para el ejercicio de derechos: el envío de cartas certificadas o semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional o cualquier otro que implique un coste excesivo para el interesado.

- Si la empresa dispone de servicios para la atención al público o para el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, pueden utilizarse para que los interesados ejerciten sus derechos. En tal caso, la identidad del interesado se considerará acreditada por los medios establecidos para la identificación de los clientes del responsable en la prestación de sus servicios o contratación de sus productos.

- Deberá atenderse la solicitud de acceso, rectificación, cancelación u oposición ejercida por un afectado aún cuando el mismo no hubiese utilizado el procedimiento establecido específicamente al efecto por aquél, siempre que el interesado haya utilizado un medio que permita acreditar el envío y la recepción de la solicitud.

6.1.3 Solicitud y contestación

Solicitud

El ejercicio de los derechos deberá llevarse a cabo mediante comunicación dirigida al responsable del fichero, que contendrá:

- 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.

- Petición en que se concreta la solicitud.

- Dirección a efectos de notificaciones, fecha y firma del solicitante.

- Documentos acreditativos de la petición que formula, en su caso.

Contestación

- El responsable del tratamiento deberá contestar la solicitud que se le dirija en todo caso, con independencia de que figuren o no datos personales del afectado en sus ficheros.

- En el caso de que la solicitud no reúna los requisitos especificados deberá solicitarse la subsanación de los mismos.

- Corresponderá al responsable del tratamiento la prueba del cumplimiento del deber de respuesta, debiendo conservar la acreditación del cumplimiento del mencionado deber.

- El responsable del fichero deberá adoptar las medidas oportunas para garantizar que las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

6.1.4 Derechos ante el encargado del tratamiento

Cuando los afectados ejercitasen sus derechos ante un encargado del tratamiento y solicitasen el ejercicio de su derecho ante el mismo, el encargado deberá dar traslado de la solicitud al responsable, a fin de que por el mismo se resuelva, a menos que en la relación existente con el responsable del tratamiento se prevea precisamente que el encargado atenderá, por cuenta del responsable, las solicitudes de ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación u oposición.

6.2 Derecho de acceso

6.2.1 Concepto y ejercicio

Concepto del derecho de acceso

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

En virtud del derecho de acceso el afectado podrá obtener del responsable del tratamiento información relativa a datos concretos, a datos incluidos en un determinado fichero, o a la totalidad de sus datos sometidos a tratamiento.

No obstante, cuando razones de especial complejidad lo justifiquen, el responsable del fichero podrá solicitar del afectado la especificación de los ficheros respecto de los cuales quiera ejercitar el derecho de acceso, a cuyo efecto deberá facilitarle una relación de todos ellos.

El derecho de acceso es independiente del que otorgan a los afectados las leyes especiales y en particular la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Ejercicio del derecho de acceso

Al ejercitar el derecho de acceso, el afectado podrá optar por recibir la información a través de uno o varios de los siguientes sistemas de consulta del fichero:

- Visualización en pantalla.
- Escrito, copia o fotocopia remitida por correo, certificado o no.
- Telecopia.
- Correo electrónico u otros sistemas de comunicaciones electrónicas.
- Cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable.

Los sistemas de consulta del fichero podrán restringirse en función de la configuración o implantación material del fichero o de la naturaleza del tratamiento, siempre que el que se ofrezca al afectado sea gratuito y asegure la comunicación escrita si éste así lo exige.

Si se ofrece un determinado sistema para hacer efectivo el derecho de acceso y el afectado lo rechazase, el responsable del tratamiento no responderá por los posibles riesgos que para la seguridad de la información pudieran derivarse de la elección.

Si se ofrece un procedimiento para hacer efectivo el derecho de acceso y el afectado exigiese que el mismo se materializase a través de un procedimiento que implique un coste desproporcionado, surtiendo el mismo efecto y garantizando la misma seguridad el procedimiento ofrecido por el responsable, serán de cuenta del afectado los gastos derivados de su elección.

6.2.2 Contestación: Otorgamiento y denegación del acceso

Otorgamiento del acceso

Debe resolverse sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud. Si en ese plazo no se responde de forma expresa a la petición, el interesado podrá interponer una reclamación ante la AEPD.

Si no se tienen datos de carácter personal de quien realiza la solicitud debe de comunicárselo en el mismo plazo de un mes.

Si la solicitud se estima pero no se acompaña a la comunicación la información, el acceso se hará efectivo durante los diez días siguientes a dicha comunicación.

La información que se proporcione, cualquiera que sea el soporte en que fuere facilitada, se dará en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

Dicha información comprenderá todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático, así como la información disponible sobre el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.

Denegación de acceso

Se podrá denegar el acceso a los datos de carácter personal cuando el derecho ya se haya ejercitado en los doce meses anteriores a la solicitud, salvo que se acredite un interés legítimo al efecto.

También podrá denegarse el acceso en los supuestos en que así lo prevea una Ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.

En todo caso, se informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos.

6.3 Derechos de rectificación y cancelación

6.3.1 Concepto y ejercicio

El **derecho de rectificación** es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.

El **derecho de cancelación** es el que dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo de dichos datos.

Ejercicio de los derechos de rectificación y cancelación

La solicitud de rectificación deberá indicar a qué datos se refiere y la corrección que haya de realizarse y deberá ir acompañada de la documentación justificativa de lo solicitado.

En la solicitud de cancelación, el interesado deberá indicar a qué datos se refiere, aportando al efecto la documentación que lo justifique, en su caso.

Contestación a la solicitud

El responsable del fichero resolverá sobre la solicitud de rectificación o cancelación en el plazo máximo de diez días a contar desde la recepción de la solicitud. Si en ese plazo no se responde de forma expresa a la petición, el interesado podrá interponer una reclamación ante la AEPD.

Si no se tienen datos de carácter personal de quien realiza la solicitud debe de comunicárselo en el mismo plazo de diez días.

6.3.2 Comunicación al cesionario

Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá comunicar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que éste, también en el plazo de diez días contados desde la recepción de dicha comunicación, proceda, asimismo, a rectificar o cancelar los datos.

La rectificación o cancelación efectuada por el cesionario no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la LOPD.

6.3.3 Denegación de los derechos de rectificación y cancelación.

La cancelación no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos.

Podrá también denegarse los derechos de rectificación o cancelación en los supuestos en que así lo prevea una ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.

En todo caso, se informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos.

6.4 Derecho de oposición

6.4.1 Concepto y ejercicio

Concepto del derecho de oposición

Es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos:

- Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario.
- Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, cualquiera que sea la empresa responsable de su creación.
- Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal.

Ejercicio del derecho de oposición

El derecho de oposición se ejercitará mediante solicitud dirigida al responsable del tratamiento.

Cuando la oposición se realice con base a que no ha sido necesario su consentimiento para el tratamiento deberán hacerse constar los motivos fundados y legítimos, relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho.

6.4.2 Contestación

El responsable del fichero resolverá sobre la solicitud de oposición en el plazo máximo de diez días a contar desde la recepción de la solicitud. Si en ese plazo no se responde de forma expresa a la petición, el interesado podrá interponer una reclamación ante la AEPD.

En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.

6.4.3 Exclusión o denegación

El responsable del fichero o tratamiento deberá excluir del tratamiento los datos relativos al afectado que ejercite su derecho de oposición o denegar motivadamente la solicitud del interesado en el plazo de diez días.

6.4.4 Derecho de oposición a las decisiones basadas únicamente en un tratamiento automatizado de datos.

Concepto

Los interesados tienen derecho a no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta.

Excepciones

- Que se haya adoptado en el marco de la celebración o ejecución de un contrato a petición del interesado, siempre que se le otorgue la posibilidad de alegar lo que estimara pertinente, a fin de defender su derecho o interés. En todo caso, el responsable del fichero deberá de informar previamente al afectado, de forma clara y precisa, de que se adoptarán decisiones en las que se evaluarán aspectos de su personalidad y cancelará los datos en caso de que no llegue a celebrarse finalmente el contrato.

- Que la decisión basada en el tratamiento automatizado esté autorizada por una norma con rango de Ley que establezca medidas que garanticen el interés legítimo del interesado.

6.5 Tutela de los derechos e indemnización

Tutela de los derechos

Cuando a un interesado se le deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la AEPD, que deberá asegurarse de la procedencia o improcedencia de la denegación y dictar resolución expresa de tutela de derechos en seis meses.

Derecho a indemnización

Los interesados que sufran daño o lesión en sus bienes o derechos, a causa de un incumplimiento de lo establecido en la LOPD 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.

6.6 Modelo de formulario para el ejercicio de derechos ARCO

Formulario para el ejercicio de Derechos de Acceso, Rectificación, Cancelación u Oposición (A.R.C.O):
D/Dña._____, DNI_____,
Domicilio_____; CP_____,
Localidad_____, Provincia _____, Teléfono _____ .
Solicita (señalar el que proceda):
Ejercitar el Derecho de Acceso sobre sus datos de carácter personal, solicitando se le remita información por correo a la dirección anteriormente indicada.
Ejercitar el Derecho de Rectificación de los siguientes datos de carácter personal, en el sentido que se indica a continuación:

_____

_____

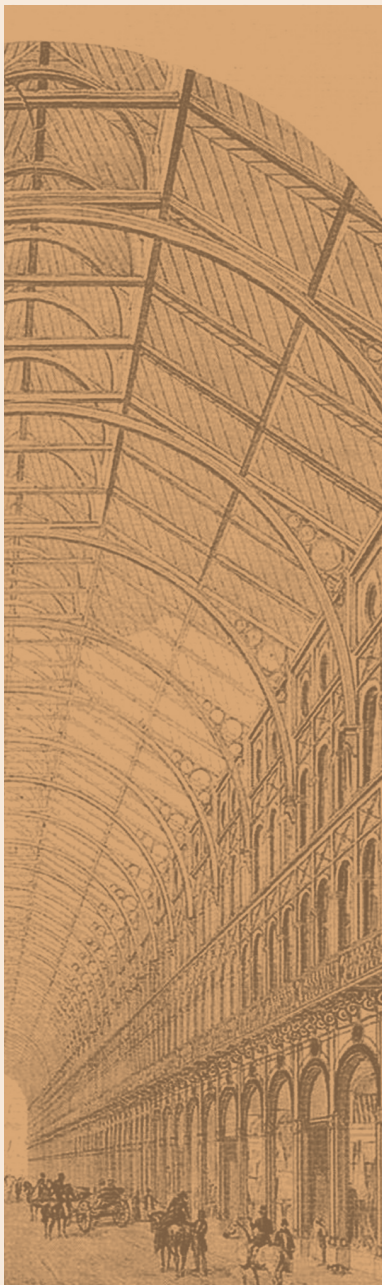
Ejercitar el Derecho de Cancelación de los datos de todos los archivos/ficheros de _____ (datos del responsable del fichero)
Ejercitar el Derecho de Oposición al tratamiento sus datos para las siguientes finalidades:

_____

_____

Se deberá entregar el formulario debidamente cumplimentado y adjuntando una fotocopia de DNI o documento equivalente que acredite la identidad del solicitante. Si actúa en representación de un tercero deberá aportarse DNI del representante y documento acreditativo de la representación del interesado.
El siguiente formulario deberá remitirse por correo a _____(nombre del responsable del fichero y dirección donde se puede remitir la solicitud).
Con el envío del presente formulario, Usted presta su consentimiento y se da por informado de que los datos que voluntariamente facilite a través del mismo serán incorporados en el fichero no automatizado denominado "Solicitudes de Ejercicios ARCO", cuyo responsable es _____ (nombre responsable del fichero), y con domicilio en _____(dirección del responsable del fichero). La recogida y tratamiento de sus datos tendrá como finalidad exclusiva la gestión adecuada del ejercicio de los derechos de acceso, rectificación, cancelación y oposición en relación con sus datos tal y como se indica en el presente formulario.

7 Acceso a datos por cuenta de terceros y prestación de servicios sin acceso a datos



7 Acceso a datos por cuenta de terceros y prestación de servicios sin acceso a datos

7.1 Acceso a datos por cuenta de terceros

Acceso en locales del responsable de tratamiento o acceso remoto

Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

Cuando dicho acceso sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

Acceso en locales del encargado

Si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

El acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad establecidas en la normativa de protección de datos de carácter personal.

Identificación de accesos por terceros

Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.

Delegación total del tratamiento en el encargado

En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios.

Este hecho se indicará de modo expreso en el contrato celebrado entre el responsable del fichero y el encargado del tratamiento, con especificación de los ficheros o tratamientos afectados.

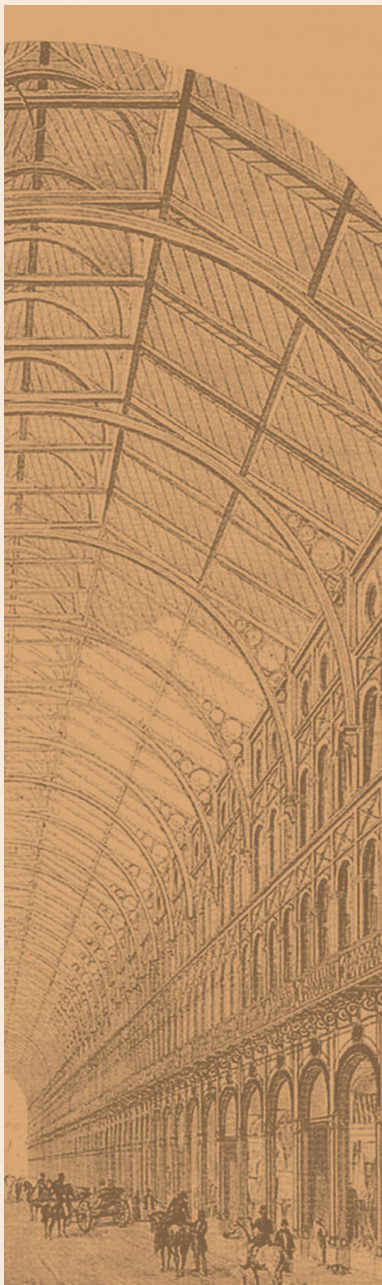
En estos casos, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por la normativa sobre protección de datos de carácter personal.

7.2 Prestaciones de servicios sin acceso a datos personales

El responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

8 Particularidades de determinados tipos de ficheros



8 Particularidades de determinados tipos de ficheros

8.1 Ficheros de información sobre solvencia patrimonial o crédito

Procedencia de los datos

Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

Ejercicio de los derechos de acceso, rectificación, cancelación y oposición

Se rige por lo dispuesto de modo general para el resto de los ficheros con los siguientes criterios:

- Cuando la petición de ejercicio de los derechos se dirigiera al responsable del fichero, éste estará obligado a satisfacer, en cualquier caso, dichos derechos.

- Si la petición se dirigiera a las personas y entidades a las que se presta el servicio, éstas únicamente deberán comunicar al afectado aquellos datos relativos al mismo que les hayan sido comunicados y a facilitar la identidad del responsable para que, en su caso, puedan ejercitar sus derechos ante el mismo.

8.2 Tratamiento de datos relativos a las obligaciones dinerarias

El Tratamiento de datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés, implica:

Requisitos para la inclusión de los datos

- Existencia previa de una deuda cierta, vencida, exigible, que haya resultado impagada.

- Que no hayan transcurrido seis años desde la fecha en que hubo de procederse al pago de la deuda o del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico.

- Requerimiento previo de pago a quien corresponda el cumplimiento de la obligación.

Información previa a la inclusión de los datos en el fichero

- El acreedor deberá informar al deudor, en el momento en que se celebre el contrato y, en todo caso, al tiempo de efectuar el requerimiento, que en caso de no producirse el pago en el término previsto para ello y cumplirse los requisitos previstos, los datos relativos al impago podrán ser comunicados a ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias.

- El acreedor o quien actúe por su cuenta o interés estará obligado a conservar a disposición del responsable del fichero común y de la Agencia Española de Protección de Datos documentación suficiente que acredite el cumplimiento de los requisitos establecidos para la inclusión de los datos y del requerimiento previo.

Notificación de la inclusión

- El responsable del fichero común deberá notificar a los interesados respecto de los que hayan registrado datos de carácter personal, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos, informándole asimismo de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, en los términos establecidos por la LOPD.

- Se efectuará una notificación por cada deuda concreta y determinada con independencia de que ésta se tenga con el mismo o con distintos acreedores.

- La notificación deberá efectuarse a través de un medio fiable, auditable e independiente de la entidad notificante, que la permita acreditar la efectiva realización de los envíos.

- En todo caso, será necesario que el responsable del fichero pueda conocer si la notificación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado. No se entenderán suficientes para que no se pueda proceder al tratamiento de los datos referidos a un interesado las devoluciones en las que el destinatario haya rehusado recibir el envío.

- Si la notificación de inclusión fuera devuelta, el responsable del fichero común comprobará con la entidad acreedora que la dirección utilizada para efectuar esta notificación se corresponde con la contractualmente pactada con el cliente a efectos de comunicaciones y no procederá al tratamiento de los datos si la mencionada entidad no confirma la exactitud de este dato.

Conservación de los datos

- Sólo podrán ser objeto de tratamiento los datos que respondan con veracidad a la situación de la deuda en cada momento concreto. El pago o cumplimiento de la deuda determinará la cancelación inmediata de todo dato relativo a la misma.

- En los restantes supuestos, los datos deberán ser cancelados cuando se hubieran cumplido seis años contados a partir del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico.

Acceso a la información contenida en el fichero

Los datos contenidos en el fichero común sólo podrán ser consultados por terceros cuando precisen enjuiciar la solvencia económica del afectado. En particular, se considerará que concurre dicha circunstancia en los siguientes supuestos:

- Que el afectado mantenga con el tercero algún tipo de relación contractual que aún no se encuentre vencida.

- Que el afectado pretenda celebrar con el tercero un contrato que implique el pago aplazado del precio.

- Que el afectado pretenda contratar con el tercero la prestación de un servicio de facturación periódica.

Ejercicio de los derechos de acceso, rectificación, cancelación y oposición

Además de cumplir lo prevenido para la generalidad de ficheros para el ejercicio de los derechos, se tendrán en cuenta las siguientes reglas:

- Si la solicitud se dirigiera al titular del fichero común, éste deberá comunicar al afectado todos los datos relativos al mismo que obren en el fichero.

- En este caso, el titular del fichero común deberá, además de dar cumplimiento a lo establecido en el presente reglamento, facilitar las evaluaciones y apreciaciones que sobre el afectado se hayan comunicado en los últimos seis meses y el nombre y dirección de los cesionarios.

- Si la solicitud se dirigiera a cualquier otra entidad participante en el sistema, deberá comunicar al afectado todos los datos relativos al mismo a los que ella pueda acceder, así como la identidad y dirección del titular del fichero común para que pueda completar el ejercicio de su derecho de acceso.

8.3 Tratamiento para actividades de publicidad y prospección comercial

Deben de cumplir con los requisitos que se expondrán a continuación las siguientes empresas:

- Las que se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas.

- Las que realicen estas actividades con el fin de comercializar sus propios productos o servicios o los de terceros

8.3.1 Datos susceptibles de tratamiento

Sólo podrán utilizar nombres y direcciones u otros datos de carácter personal cuando los mismos se encuentren en uno de los siguientes casos:

- Figuren en una fuente accesible al público y el interesado no haya manifestado su negativa u oposición a que sus datos sean objeto de tratamiento para las actividades descritas en este apartado.

- Hayan sido facilitados por los propios interesados u obtenidos con su consentimiento para finalidades determinadas, explícitas y legítimas relacionadas con la actividad de publicidad o prospección comercial, habiéndose informado a los interesados sobre los sectores específicos y concretos de actividad respecto de los que podrá recibir información o publicidad.

¿Cuáles se consideran por la LOPD fuentes accesibles al público?

- El censo promocional.

- Las guías de servicios de comunicaciones electrónicas.

- 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. 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.

- Los diarios y boletines oficiales.

- Los medios de comunicación social.

8.3.2 Deber de información al interesado

Cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, deberá informarse al interesado en cada comunicación que se le dirija del origen de los datos (que han sido obtenidos de fuentes accesibles al público y de la entidad de la que hubieran sido obtenidos) y de la identidad del responsable del tratamiento así como de los derechos que le asisten, con indicación de ante quién podrán ejercitarse.

8.3.3 Campañas de publicidad entre los clientes

Cuando una empresa quiera realizar una campaña de publicidad de sus productos o servicios entre sus clientes podrá:

- Realizar por sí misma una actividad publicitaria de sus productos o servicios entre sus clientes, para lo cual deberá contar con el consentimiento inequívoco del cliente para que sus datos sean utilizados para tal fin.

- Contratar a terceros para la realización de la campaña publicitaria de sus productos o servicios, encomendándole el tratamiento de determinados datos, en ese caso se aplicarán las siguientes normas:

  - Cuando los parámetros identificativos de los destinatarios de la campaña sean fijados por la entidad que contrate la campaña, ésta será responsable del tratamiento de los datos.

  - Cuando los parámetros fueran determinados únicamente por la entidad o entidades contratadas, dichas entidades serán las responsable del tratamiento.

  - Cuando en la determinación de los parámetros intervengan ambas entidades, serán ambas responsables del tratamiento.

¿Qué se consideran parámetros identificativos?

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

Al encargar la campaña a un tercero se deberán adoptar las medidas necesarias para asegurarse de que la entidad contratada ha recabado los datos cumpliendo las exigencias de la normativa de protección de datos.

8.3.4 Ficheros de exclusión del envío de comunicaciones comerciales

Cuando un afectado haya manifestado su negativa a recibir publicidad se podrán conservar los mínimos datos imprescindibles para identificarlo y adoptar las medidas necesarias que eviten el envío de publicidad.

Es posible la creación de ficheros comunes, de carácter general o sectorial, en los que sean objeto de tratamiento los datos de carácter personal que resulten necesarios para evitar el envío de comunicaciones comerciales a los interesados que manifiesten su negativa u oposición a recibir publicidad. Los citados ficheros podrán contener los mínimos datos imprescindibles para identificar al afectado.

8.3.5 Ejercicio de los derechos de acceso, rectificación, cancelación y oposición

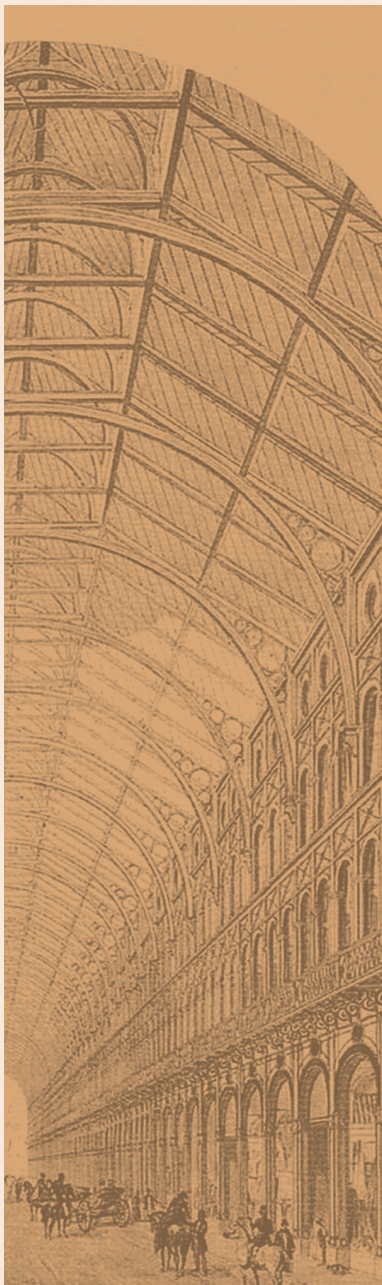
En el caso de ejercicio de los derechos de acceso, rectificación y cancelación, además de cumplir lo prevenido para la generalidad de ficheros para el ejercicio de los derechos se deberá:

- Si el derecho se ejercitase ante una entidad que hubiese encargado a un tercero la realización de una campaña publicitaria, aquélla estará obligada, en el plazo de diez días, desde la recepción de la comunicación de la solicitud de ejercicio de derechos del afectado, a comunicar la solicitud al responsable del fichero a fin de que el mismo otorgue al afectado su derecho en el plazo de diez días desde la recepción de la comunicación, dando cuenta de ello al afectado.

- En el caso de ejercicio del derecho de oposición, además de los requisitos previstos para dicho ejercicios en la normativa deberá tenerse en cuenta que:

  - Si el derecho de oposición se ejercitase ante una entidad que hubiera encomendado a un tercero la realización de una campaña publicitaria, aquélla estará obligada, en el plazo de diez días, desde la recepción de la comunicación de la solicitud de ejercicio de derechos del afectado, a comunicar la solicitud al responsable del fichero a fin de que el mismo atienda el derecho del afectado en el plazo de diez días desde la recepción de la comunicación, dando cuenta de ello al afectado.

9 Transferencias internacionales de datos



9 Transferencias internacionales de datos

9.1 Autorización y notificación

Para que la transferencia internacional de datos pueda considerarse conforme a la normativa de protección de datos será necesaria la autorización del Director de la Agencia Española de Protección de Datos.

La autorización no será necesaria:

- Cuando el Estado en el que se encontrase el importador ofrezca un nivel adecuado de protección.
- Cuando la transferencia se encuentre en uno de los siguientes supuestos:
  - Resulte de la aplicación de tratados o convenios en los que sea parte España.
  - Se haga a efectos de prestar o solicitar auxilio judicial internacional.
  - Sea necesaria para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico o la gestión de servicios sanitarios.
  - Se refiera a transferencias dinerarias conforme a su legislación específica.
  - El afectado haya dado su consentimiento inequívoco a la transferencia prevista.
  - Sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.
  - Sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.
  - Sea necesaria o legalmente exigida para la salvaguarda de un interés público.
  - Sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

- Se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.

- Tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

En todo caso, la transferencia internacional de datos deberá ser notificada a fin de proceder a su inscripción en el Registro General de Protección de Datos.

Transferencias a estados que proporcionen un nivel adecuado de protección

Se consideran países con un nivel adecuado de protección:

- Suiza.
- Las entidades estadounidenses adheridas a los principios de "Puerto Seguro".
- Canadá respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos.
- Argentina.
- Guernsey.
- Isla de Man.
- Jersey.
- Islas Feroe.
- Andorra.
- Israel.

9.2 Transferencias a estados que no proporcionen un nivel adecuado de protección

Cuando la transferencia tenga por destino un Estado respecto del que no se haya declarado por la Comisión Europea o no se haya considerado por el Director de la Agencia Española de Protección de Datos que existe un nivel adecuado de protección, será necesario recabar la autorización del Director de la Agencia Española de Protección de Datos.

La autorización podrá ser otorgada en caso de que el responsable del fichero o tratamiento aporte un contrato escrito, celebrado entre el exportador y el importador, en el que consten las necesarias

garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos.

El Director de la Agencia Española de Protección de Datos podrá denegar o, suspender temporalmente, previa audiencia del exportador, la transferencia, cuando concurra alguna de las circunstancias siguientes:

- Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos que el contrato garantiza.
- Que la entidad destinataria haya incumplido previamente las garantías establecidas en cláusulas contractuales de este tipo.
- Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el importador.
- Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos.
- Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una situación de riesgo de daño efectivo a los afectados.

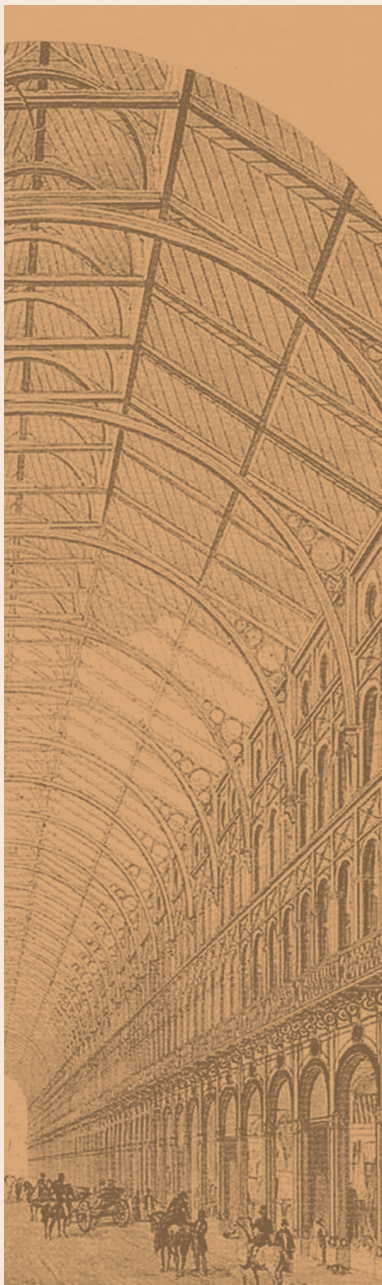
9.3 Procedimiento de autorización transferencias internacionales de datos

El procedimiento para la obtención de la autorización para las transferencias internacionales de datos a países terceros se iniciará siempre a solicitud del exportador que pretenda llevar a cabo la transferencia.

En su solicitud, además de los requisitos legalmente exigidos, el exportador deberá consignar, en todo caso:

- La identificación del fichero o ficheros a cuyos datos se refiera la transferencia internacional, con indicación de su denominación y código de inscripción del fichero en el Registro General de Protección de Datos.
- La transferencia o transferencias respecto de las que se solicita la autorización, con indicación de la finalidad que la justifica.
- La documentación que incorpore las garantías exigibles para la obtención de la autorización así como el cumplimiento de los requisitos legales necesarios para la realización de la transferencia, en su caso.
- Cuando la autorización se fundamente en la existencia de un contrato entre el exportador y el importador de los datos, deberá aportarse copia del mismo, acreditándose asimismo la concurrencia de poder suficiente en sus otorgantes.

10 Infracciones y sanciones



10 Infracciones y sanciones

Cuando el Director de la Agencia Española de Protección de Datos resuelva autorizar la transferencia internacional de datos, se dará traslado de la resolución de autorización al Registro General de Protección de Datos, a fin de proceder a su inscripción.

El plazo máximo para dictar y notificar resolución será de tres meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, se entenderá autorizada la transferencia internacional de datos.

Los responsables del tratamiento de datos de carácter personal y los encargados de su tratamiento están sometidos al régimen sancionador de la Ley Orgánica de Protección de Datos (LOPD).

10.1 Infracciones en materia de protección de datos de carácter personal

La LOPD califica las infracciones en leves, graves y muy graves.

10.1.1 Infracciones muy graves

- La recogida de datos en forma engañosa o fraudulenta.
- Tratar o ceder los datos de carácter personal relativos a la ideología, afiliación sindical, religión, creencias, origen racial, salud, vida sexual y relativos a la comisión de infracciones penales o administrativas, si no se está en uno de los supuestos en que la ley lo autoriza o violentar la prohibición de crear ficheros con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.
- No cesar en el tratamiento ilícito de datos de carácter personal cuando existiese un previo requerimiento del Director de la Agencia Española de Protección de Datos para ello.
- La transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia Española de Protección de Datos salvo en los supuestos en los que conforme a esta Ley

y sus disposiciones de desarrollo dicha autorización no resulta necesaria.

10.1.2 Infracciones graves

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

- Tratar datos de carácter personal sin recabar el consentimiento de las personas afectadas, cuando el mismo sea necesario conforme a la normativa de protección de datos.

- Tratar datos de carácter personal o usarlos posteriormente, cuando dichos datos no sean adecuados, pertinentes, exactos, ni estén puestos al día o se usan para finalidades incompatibles con aquellas para la que los datos fueron recogidos.

- La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal.

- El impedimento o la obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

- El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos no hayan sido recabados del propio interesado.

- El incumplimiento de los restantes deberes de notificación o requerimiento al afectado impuestos por la normativa de protección de datos de carácter personal.

- Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad.

- No atender los requerimientos o apercibimientos de la Agencia Española de Protección de Datos o no proporcionar a aquélla cuantos documentos e informaciones sean solicitados por la misma.

- La obstrucción al ejercicio de la función inspectora.

- La comunicación o cesión de los datos de carácter personal sin contar con legitimación para ello.

10.1.3 Infracciones leves

- No remitir a la AEPD las notificaciones previstas en la normativa de protección de datos.

- No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos.

- El incumplimiento del deber de información al afectado acerca del tratamiento de sus da-

tos de carácter personal cuando los datos sean recabados del propio interesado.

- La transmisión de los datos a un encargado del tratamiento sin firmar un contrato donde se regule la realización de tratamientos por cuenta del tercero y las medidas de seguridad que este debe adoptar.

10.2 Sanciones en materia de protección de datos de carácter personal

La AEPD tiene la potestad de imponer sanciones de conformidad con la gravedad de la infracción.

10.2.1 Sanciones

- Las infracciones leves serán sancionadas con multa de 900 a 40.000 euros.
- Las infracciones graves serán sancionadas con multa de 40.001 a 300.000 euros.
- Las infracciones muy graves serán sancionadas con multa de 300.001 a 600.000 euros.

10.2.2 Graduación de las sanciones

Las horquillas que establecen para las sanciones son tan amplias que se establecen una serie de criterios que la AEPD debe de tener en cuenta para graduar la sanción:

- El carácter continuado de la infracción.
- El volumen de los tratamientos efectuados.
- La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.
- El volumen de negocio o actividad del infractor.
- Los beneficios obtenidos como consecuencia de la comisión de la infracción.
- El grado de intencionalidad.
- La reincidencia por comisión de infracciones de la misma naturaleza.
- La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.
- La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una ano-

malía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.

- Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

10.2.3 Atenuantes

En caso de que se aprecie la existencia de alguna de las siguientes circunstancias se aplicará la cuantía de la sanción que se establezca para la infracción anterior en gravedad en la escala (así una infracción muy grave se sancionará como leve si se aprecia la existencia de una de esas circunstancias):

- Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios expuestos para graduar la sanción, siempre que estos se aprecien en sentido positivo (que no se haya obtenido beneficio de la infracción, que no haya existido intencionalidad, que el infractor haya puesto todos los medios a su alcance para paliar los efectos de la infracción, …)

- Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.

- Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.

- Cuando el infractor haya reconocido espontáneamente su culpabilidad.

- Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente.

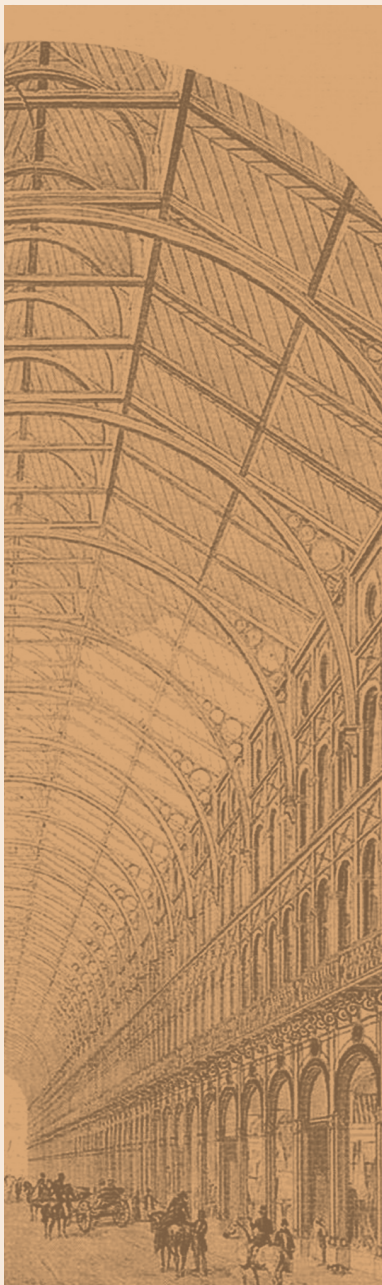
10.2.4 Apercibimiento

La AEPD podrá no abrir expediente sancionador y limitarse a apercibir al infractor para que tome las medidas correctoras necesarias, cuando concurran los siguientes presupuestos:

- Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.

- Que el infractor no hubiese sido sancionado o apercibido con anterioridad.

11 La página web de la AEPD



11 La página web de la AEPD

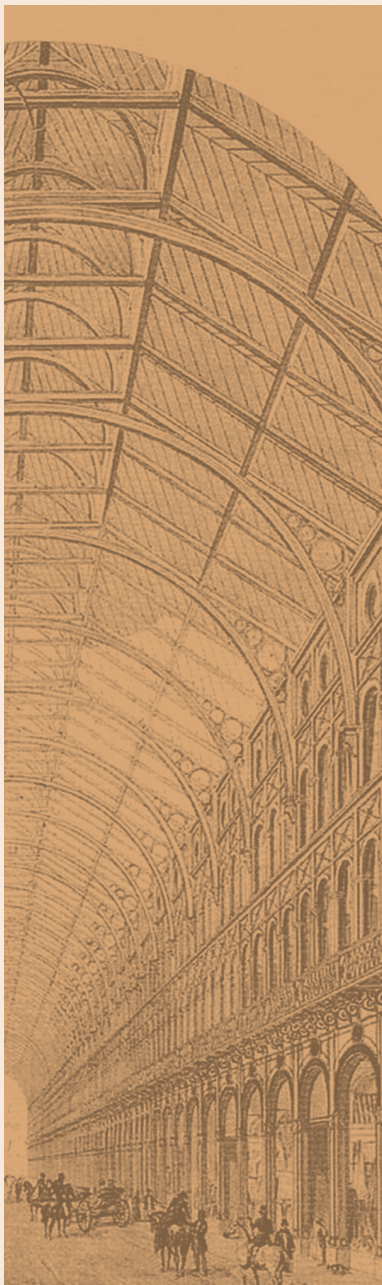
A través de la página web de la AEPD, www.agpd.es, podemos proceder a los siguientes trámites:

- Dar de alta los ficheros de datos de carácter personal de los que seamos responsables, así mismo, podemos notificar cualquier modificación de dichos ficheros o proceder a dar de baja un fichero, todo ello se hace a través del formulario NOTA.

- Efectuar consultas tanto sobre el estado de tramitación de las solicitudes que hayamos realizados a través del formulario NOTA, como del contenido de las inscripciones que hayamos realizado en el Registro General de Protección de Datos.

Además de para realizar dichos trámites la página web de la AEPD puede ser una herramienta de apoyo muy útil para adaptar nuestra empresa a la normativa existente en protección de datos; a través de las resoluciones e informes que en materia de Protección de datos emite la Agencia.

12 Consejos y recomendaciones



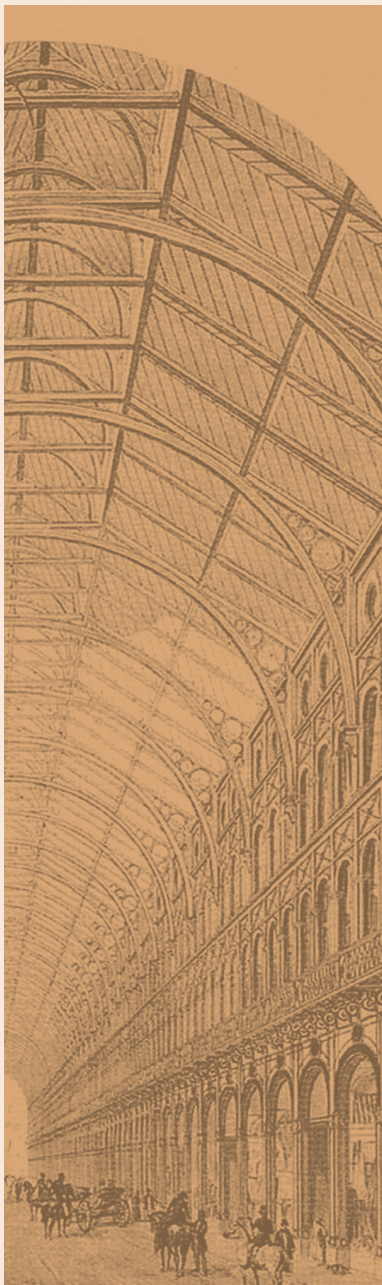
12 Consejos y recomendaciones

Cumplir con la normativa de protección de datos es de vital importancia para nuestra empresa ya que tal y como hemos visto en esta guía las sanciones pueden llegar a ser de muy elevada cuantía; además, cada vez de forma más generalizada los clientes y usuarios son conocedores de los derechos que les asisten y de la opción que tienen de denunciar ante la Agencia de Protección de Datos cuando dichos derechos no son respetados.

Algunas recomendaciones básicas en materia de protección de datos que pueden evitar que se produzcan denuncias contra nuestra empresa ante la AEPD o que en caso de producirse, se atenúen las posibles sanciones:

- Tener cláusulas tipo que han de incorporarse a toda la documentación que produzca la empresa y que puede tener implicación en el ámbito de la protección de datos (facturas, correos electrónicos, faxes, etc…).
- Que todos aquellos terceros que tengan acceso a los ficheros con datos de carácter personal firmen un contrato donde se responsabilicen del cumplimiento de todas las obligaciones relativas a la protección de datos.
- Formación de los trabajadores de la empresa en materia de protección de datos.
- En caso de que exista alguna incidencia y la seguridad de los datos se haya visto comprometida, es fundamental reaccionar con la mayor celeridad posible y tratar de minimizar los efectos de dicha incidencia.
- Registrar debidamente todo lo referente a los ficheros en los que consten datos de carácter personal (entradas y salidas de ficheros y soportes, incidencias, acceso de terceros, etc…)
- Realizar auditorías periódicas para verificar cumplimiento de las obligaciones establecidas por la normativa de protección de datos.

13 Bibliografía



13 Bibliografía

- *Manuales prácticos de gestión: Conceptos jurídicos básicos*. CEEI Galicia S.A. (2010)
- Fichas informativas. Protección de datos. CEEI Galicia S.A.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE nº 298 del 14 de diciembre de 1999.

UNIÓN EUROPEA
FONDO SOCIAL EUROPEO
"O FSE inviste no teu futuro"

XUNTA DE GALICIA