Diputación Provincial de Burgos

Con la colaboración de:

Alcatraz®

csa

"La Protección de Datos en los Ayuntamientos"

Manual elaborado por la Sección de Modernización Administrativa y Nuevas Tecnologías de la Información y las Comunicaciones de la Diputación Provincial de Burgos en colaboración con ALCATRAZ SOLUTIONS y CSA

La razón de ser de las Diputaciones Provinciales, es, sin duda alguna, prestar servicios y asistencia a las Entidades Locales de su territorio, con el fin de facilitar la gestión diaria que deben ofrecer a sus vecinos ciudadanos en general.

En esta línea de dar cumplimiento a las competencias, que nos vienen marcadas en la propia Constitución Española de 1978, la Diputación de Burgos es consciente de que su papel de prestadora de servicios y asistencia es clave para lograr no solo el progreso de su Entidades Locales sino también para facilitar el cumplimiento de las obligaciones administrativas que nos vienen encomendadas.

La publicación de este manual "La Protección de Datos en los Ayuntamientos" se enmarca como un servicio más de la Diputación a las Entidades Locales de la Provincia. Creemos que el libro puede ser un instrumento muy útil para los alcaldes, concejales y personal de los Ayuntamientos, al recoger en sus páginas un completo y a la vez sencillo resumen de cuestiones relacionadas con el tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar, por parte de los Organismos Públicos y las Entidades Locales.

El Derecho a la Protección de Datos es un derecho personalísimo inherente a las personas físicas, cuyo objetivo primordial consiste en garantizar la autonomía y el control que a cada uno de nosotros nos corresponde sobre la información que nos concierne personalmente, sea íntima o no. Esto implica el derecho a conocer en todo momento, que tipo de datos están siendo objeto de tratamiento, por qué entidades, con qué finalidad, o incluso si están siendo objeto de cesión entre diferentes entidades.

Este manual se enmarca dentro del proyecto de implantación de un sistema de gestión de cumplimiento de la Ley Orgánica de Protección de Datos en los Ayuntamientos de la Provincia de Burgos, ya que la citada Ley afecta a todas las Administraciones Públicas que posean ficheros con datos de carácter personal.

Vicente Orden Vigara

Presidente de la Diputación Provincial de Burgos

Índice

1. Introducción

El presente Documento, que girará bajo el nombre de “La Protección de datos en los Ayuntamientos “, se trata de una guía informativa donde se exponen las exigencias establecidas por la normativa en materia de protección de datos y, especialmente, aquellas que afectan directamente a las Administraciones Públicas.

2. Objetivos

- Conocer los fundamentos y conceptos generales de la protección de datos personales.
- Obtener una visión general y una comprensión de la normativa vigente en materia de protección de datos (LOPD y RLOPD).
- Identificar los elementos y procesos necesarios para la implantación y gestión de la protección de datos en la organización.
- Conocer y aplicar los controles, procedimientos y medidas de seguridad exigidos para la correcta gestión de la protección de datos personales de la organización.
- Adquirir los conocimientos necesarios para la planificación y realización de auditorías de seguridad en materia de protección de datos.

3. Fundamentos de la Protección de Datos

3.1. Origen y evolución

El derecho a la protección de datos tiene su origen en nuestro texto constitucional, es decir, la Constitución Española, que en su artículo 18 regula el derecho al honor, la intimidad personal y familiar y la propia imagen.

Concretamente, el artículo 18 CE, localizado en el Título I relativo a los derechos y deberes fundamentales, establece que:

> *"1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*
>
> *2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.*
>
> *3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.*
>
> *4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".*

En relación con esta materia, España suscribió en 1984, el Convenio Nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

El párrafo 4 del artículo 18 de la CE fue objeto de desarrollo legislativo a través de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, comúnmente conocida como LORTAD. El desarrollo reglamentario de esta Ley Orgánica se realizó a través del Reglamento de Medidas de Seguridad, aprobado por Real Decreto 994/1999, de 11 de junio (en los sucesivo, RMS), a través del cual se desarrollaba la vertiente relativa a las medidas de índole técnica y organizativa que debían implementar las Organizaciones que en el desarrollo de sus funciones tratasen datos de carácter personal.

En el año 1995 se promulgó la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Como consecuencia de este hecho, en orden a transponer la Directiva mencionada al Ordenamiento jurídico español, se promulgó en el año 1999, la vigente Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (en adelante, **LOPD**), cuyos preceptos resultan aplicables tanto a los ficheros y/o tratamientos de datos de carácter automatizado, como no automatizado; a diferencia, de la LORTAD que únicamente regulaba el tratamiento automatizado de los datos.

La LOPD fue objeto de desarrollo en el año 2007 a través del Real Decreto 1720/2007, de 21 de diciembre, que aprobó su Reglamento de desarrollo (en lo sucesivo, **RLOPD**).

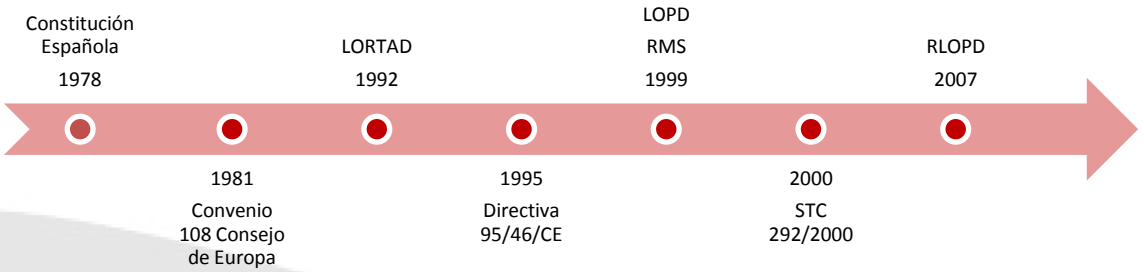


Ilustración 1 – Evolución de la normativa sobre protección de datos.

La normativa española vigente actualmente es:

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la ley Orgánica 15/1999 de la Ley Orgánica 15/1999 de 13 de diciembre, de protección de datos de carácter personal (RLOPD).

3.2. Derecho a la Protección de Datos de Carácter Personal

El "derecho a la protección de datos", recibe múltiples denominaciones: "libertad informática", "habeas data" o "autodeterminación informativa", y encuentra su fundamento –como ya se ha indicado en el punto anterior- en el artículo 18,4 de la Constitución Española, cuyo enunciado determina que "*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*".

Este precepto constitucional ha sido interpretado y desarrollado por nuestro Tribunal Constitucional en diversas sentencias, entre las que cabe citar la **STC 292/2000**, de 30 de noviembre, que determina que el derecho a la protección de datos tiene por objeto:

> *"Garantizar al titular de los datos (persona física) un poder de control y disposición sobre sus datos personales, es decir, sobre todos aquellos datos que le identifiquen o permitan su identificación. Por tanto, abarca cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, incluidos los datos personales públicos, accesibles al conocimiento de cualquiera".*

Asimismo, la sentencia antes citada acota el contenido del derecho a la protección de datos estableciendo que éste:

> *"Atribuye al titular de los datos un haz de facultades que consiste en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos (deberes jurídicos), es decir, otorga al titular el poder de disposición sobre sus datos personales, que se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.*

Este haz de facultades se haya limitado por la propia Ley y los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos. Por tanto, existe reserva de Ley, tanto para el desarrollo del derecho fundamental a la protección de datos (artículo 81.1 CE), como para regular su ejercicio o el haz de facultades que compone el contenido del derecho fundamental (artículo 53.1 CE).

3.3. Ámbito de aplicación

En este punto se analiza el ámbito de aplicación de la normativa sobre protección de datos, determinando a qué sujetos o supuestos es aplicable la misma. El ámbito de aplicación se clasifica en:

- Territorial
- Subjetivo
- Objetivo

- ***Ámbito Territorial***

La LOPD y su Reglamento de desarrollo se aplican a todo tratamiento de datos de carácter personal:

a) Efectuado en un establecimiento del responsable del tratamiento ubicado en territorio español.
b) Efectuado por un encargado del tratamiento ubicado en España. En este caso, le será de aplicación el Título VIII del RLOPD, relativo a las medidas de seguridad.
c) 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. En este supuesto, el responsable del tratamiento deberá designar un representante legal establecido en territorio español.
d) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española, según las normas de Derecho internacional público.

En este sentido, debe entenderse por "*establecimiento*", cualquier instalación estable que permita el ejercicio efectivo y real de una actividad.

Por otro lado, debe entenderse por "*medios*" en los términos descritos en la letra c) anterior, el conjunto de instrumentos o aparatos reunidos para tratar datos personales (como ejemplo de medios, cita los ordenadores, los terminales y los servidores) que están a disposición del responsable del tratamiento.

Por tanto, no es necesario que el responsable del tratamiento tenga un control total sobre los medios, basta con que determine qué datos se recogen, se almacenan, se transfieren, se modifican, etc., de qué forma y con qué objetivo. Esta facultad de disposición del responsable no debe confundirse con la propiedad o posesión de los medios, siendo este hecho indiferente.

- *Ámbito Subjetivo*

El ámbito subjetivo de aplicación de la normativa sobre protección de datos, es decir, qué sujetos o entidades resultan obligados o beneficiados por el régimen jurídico establecido en la LOPD, puede dividirse en:

a) **Ámbito obligacional**, sujetos obligados a acatar las prescripciones de la LOPD:

- **Responsable del fichero o del tratamiento**: Persona física o jurídica, o entidad sin personalidad jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.
- **Diferencias** entre Responsable del fichero y Responsable del tratamiento:

  Responsable del fichero: es quien decide la creación del fichero, su aplicación, su finalidad, contenido y uso.

  Responsable del tratamiento: es quien adopta decisiones sobre las concretas actividades de un determinado tratamiento de datos.

- Dentro de la Organización del responsable del fichero y/o tratamiento pueden identificarse los siguientes sujetos:

  Responsable de seguridad: persona encargada de controlar y coordinar las medidas de seguridad implantadas

  Usuario: sujeto autorizado para acceder o tratar datos de carácter personal

- **Encargado del tratamiento**: La persona física o jurídica, o entidad sin personalidad jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.
- **Diferencias** entre Responsable del fichero y Encargado del tratamiento:

  El **responsable del fichero o tratamiento** es quien decide sobre las características del fichero o tratamientos a realizar; mientras que, el **encargado del tratamiento** es quien ejecuta materialmente las decisiones del responsable del fichero o tratamiento en relación al fichero, es decir, no tiene capacidad o poder de decisión sobre el tratamiento que realiza.

- **Tercero**: la persona física o jurídica, o entidad sin personalidad jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de los usuarios.

  Destinatario o cesionario: la persona física o jurídica, o entes sin personalidad jurídica, pública o privada u órgano administrativo, al que se revelen los datos.

b) **Ámbito de protección**, sujetos protegidos por la normativa sobre protección de datos.

- **Afectado o interesado**: Persona física titular de los datos que sean objeto del tratamiento.

- ***Ámbito Objetivo***

La LOPD y su Reglamento de desarrollo se aplican a **los datos de carácter personal** registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

En atención a la definición anterior conviene, en primer lugar, determinar que se entiende por "*dato de carácter personal*" para, a continuación, definir los conceptos de "*tratamiento*" y "*fichero*":

- **Datos de carácter personal**

  Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables (artículo 5 del RLOPD).

  Se considera que una *persona es identificable*, cuando su identidad puede determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social, siempre y cuando no requiera plazos o actividades desproporcionados.

  Por tanto, si se recogen y tratan datos como el nombre, dirección postal, correo-e, teléfono, matrícula del coche, fotografía, huella digital, etc…, se están utilizando datos que identifican a una persona y, por tanto, deben cumplirse las prescripciones recogidas en la normativa sobre protección de datos.

En relación con la definición anterior, conviene matizar que, en determinados supuestos, los datos que, en principio, se considerarían datos de carácter personal no reciben tal clasificación y, por tanto, no les es de aplicación la normativa sobre protección de datos. En este sentido, el artículo 2 del RLOPD **excluye de su ámbito de aplicación** los tratamientos y/o tratamientos referidos a:

- *Personas jurídicas*
- *Datos de contacto profesionales (consistentes únicamente en el nombre y apellidos, funciones o puestos desempeñados, dirección postal o electrónica, teléfono y número de fax profesionales), cuando se utilicen con la finalidad de contactar con la entidad a la que pertenece el sujeto*
- *Empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros*
- *Personas fallecidas*

- **Tratamiento de datos**

  Cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias (artículo 5 del RLOPD).

  Por tanto, la mera consulta de un fichero o el almacenamiento de información sin realizar una operación concreta con la misma, se consideran tratamientos a efectos de la LOPD.

- **Fichero**

  Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso (artículo 5 del RLOPD).

En relación con los dos conceptos anteriores, fichero y tratamiento, es necesario tener presente que el artículo 4 del RLOPD excluye de su ámbito de aplicación aquellos ficheros y/o tratamientos que tengan por objeto:

- Actividades exclusivamente personales o domésticas (que se inscriben en el marco de la vida privada o familiar de los particulares).
- Materias clasificadas.
- La investigación del terrorismo y de formas graves de delincuencia organizada.

3.4. Obligaciones del Responsable del Fichero

Las obligaciones de los organismos responsables del fichero pueden agruparse o clasificarse en tres bloques, denominados:

- Legalización
- Legitimación
- Protección

Cada uno de estos bloques está relacionado con un ámbito de actuación concreto. El primero, o legalización, está relacionado con los ficheros; el segundo, o legitimación, se asocia a los principios rectores de la normativa sobre protección de datos; y, el tercero, denominado "Protección", está vinculado a la seguridad de los datos.

- ***Legalización***

Implica que todos aquellos ficheros que contengan datos de carácter personal deben **inscribirse en el Registro General de Protección de Datos** (en lo sucesivo, RGPD) de la Agencia Española de Protección de Datos o en sus homónimos autonómicos (APDCAT, AVPD o APDCM).

En relación con la obligación de legalizar los ficheros ante las Autoridades de Control competentes, conviene saber que dicha declaración debe realizarse de conformidad con los siguientes criterios:

¿Quién?	*El Responsable del Fichero debe notificar la creación, modificación o supresión de los ficheros de los que es titular para su inscripción en el Registro correspondiente.*
¿Cuándo?	*Con anterioridad a la creación de los ficheros (Creación), cuando se produzcan cambios respecto a la inscripción inicial (Modificación), o cuando cese el uso del fichero (Supresión).*
¿Finalidad?	*Permite que los titulares de los datos puedan conocer quiénes son los responsables de los ficheros ante los que ejercitar directamente los derechos de acceso, rectificación, cancelación y oposición.*

- ***Legitimación***

El **Responsable del Fichero o Tratamiento** debe cumplir en las distintas fases del tratamiento de datos (recogida, tratamiento y cesión), y tener presentes, los **principios rectores de la protección de datos** establecidos por la normativa:

Principios de la LOPD	*Artículos*
Calidad	*4*
Deber de información	*5*
Consentimiento	*6*
Datos especialmente protegidos	*7*
Datos de salud	*8*
Confidencialidad	*9*
Seguridad	*10*
Cesión de datos	*11*
Acceso por terceros	*12*

- ***Protección***

El **responsable del fichero o tratamiento** y, en su caso, el **encargado del tratamiento** están obligados a adoptar las **medidas de índole técnica y organizativas** necesarias para garantizar la seguridad de los datos de carácter personal.

4. Legalización

4.1. Concepto de Fichero

Los organismos responsables de fichero[1] están obligados a declarar ante la Autoridad de Control competente aquellos ficheros de carácter personal, de los que sean titulares, que se traten en sus sistemas de información.

En este sentido, se entiende por "Fichero", *Todo* ***conjunto organizado de datos de carácter personal****, que permita el* ***acceso*** *a los datos* ***con arreglo a criterios determinados****, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso* (artículo 5.1.k) del RLOPD).

Por tanto, estaremos ante un fichero LOPD, cuando:

- Se trate de un **conjunto organizado** (ordenado) de datos
- Contenga **datos de carácter personal**[2]
- **Cualquiera que sea su modalidad de creación, almacenamiento, organización y acceso**; es decir, tanto si se tratan los datos en soporte papel como de forma automatizada.

La definición anterior debe matizarse en relación a ficheros cuyo sistema de tratamiento sea exclusivamente no automatizado, es decir, aquellos que se organizan de forma manual o en papel. En tales casos deberá tenerse presente para considerar que se trata de un Fichero LOPD, además de las características anteriores, las siguientes peculiaridades:

- Se halle **estructurado conforme a criterios específicos relativos a personas físicas**
- Permita **acceder sin esfuerzos desproporcionados** a los datos.

En atención a las características mencionadas, son ficheros LOPD, por ejemplo, aquellos en los que los datos personales se almacenen en bases de datos estructuradas o cuando nos hallemos ante expedientes físicos, como son las historias clínicas, en los que el criterio de ordenación se basa en la identidad del paciente.

En este mismo sentido, se pronuncia el Informe 0279/2009 emitido por la AEPD al entender que:

---

[1] *Cualquier persona física o jurídica, de naturaleza pública o privada, u órgano administrativo que sólo o conjuntamente decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.*

[2] *Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.*

"[…] la ordenación de los documentos por fecha no constituye un fichero, al no estar éste estructurado conforme a criterios relativos a las personas físicas, y siempre que impida acceder a los datos personales incorporados en los documentos exija esfuerzos desproporcionados a los datos personales. Si por el contrario, existe una correlación entre las fechas de los documentos y los sujetos a quienes se envían los mismo, lo que implica acceder sin esfuerzos desproporcionados a los datos personales, sí que la carpeta constituye un fichero no automatizado de datos de carácter personal.

[Por otra parte, se] plantea si los documentos incorporados a un soporte electrónico sin ningún orden lógico constituye un fichero. En este caso además de acudir a la definición de fichero antes señalada, es preciso destacar que el archivo de documentos en un sistema informático lleva implícita una organización, así todo sistema informático permite hacer búsquedas de documentos , lo que en definitiva convierte a la carpeta en la que se incorporen los documentos como fichero, dado que se cumple con los criterios de la definición, se permite el acceso a los documentos con independencia de la forma o modalidad de su creación, organización, almacenamiento y acceso."

- ***Ficheros excluidos***

No se consideran ficheros LOPD y, por tanto, no les es de aplicación el régimen de protección de datos regulado por la Ley Orgánica 15/1999, de 13 de diciembre, los siguientes ficheros y tratamientos:

a) Los realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas, es decir, actividades que se inscriben en el marco de la vida privada o familiar de los particulares.
b) Los sometidos a la normativa sobre protección de materias clasificadas.
c) Los establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.

4.2. Tipos de Ficheros

Existen múltiples clasificaciones de los ficheros relacionadas con la protección de datos:

a) En atención a la **titularidad del fichero**, serán ficheros públicos o privados

   La titularidad del fichero corresponde a la Entidad que declara su existencia y/o contenido ante las Autoridades de Control competentes. En otras palabras, el responsable del fichero es el titular del fichero.

- Fichero privado

Los ficheros de los que sean responsables:

- *las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos (artículo 5.1.l RLOPD),*
- *las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica (artículo 5.1.l RLOPD).*

- Fichero público

Los ficheros de los que sean responsables

- *los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, , así como las entidades u organismos vinculados o dependientes de las mismas (artículo 5.1.m RLOPD),*
- *las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público (artículo 5.1.m RLOPD).*

b) En atención al **sistema de tratamiento**

Por sistema de tratamiento, se entiende el modo en que se organiza o utiliza un sistema de información[3]. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados (artículo 5.2.n RLOPD)

- Fichero automatizado

Aquellos ficheros cuyo sistema de tratamiento es totalmente automatizado.

- Fichero no automatizado

Aquellos ficheros cuyo sistema de tratamiento es no automatizado o manual.

Todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica (artículo 5.1.n RLOPD).

- Fichero parcialmente automatizado (o mixto)

Ficheros cuyo tratamiento se realiza tanto de forma automatizada como no automatizada (papel).

[3] *Conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal (artículo 5.2.m RLOPD).*

- ***Declaración obligatoria***

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

En este sentido, El artículo 26 determina, en su apartado 1, que "*Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia Española de Protección de Datos*"

De lo indicado en el citado precepto de la LOPD se desprende que la notificación de los ficheros habrá de ser previa a la creación de los mismos, por lo que la ausencia de dicha notificación sería una conducta constitutiva de infracción leve, con arreglo a lo dispuesto en el artículo 44.2.c) de la propia Ley[4].

La inscripción de los ficheros en los Registros públicos de las Autoridades de Control tiene como finalidad garantizar el contenido del derecho a la protección de datos, es decir, que los interesados puedan ejercitar sus derechos de acceso, rectificación, cancelación y oposición (ARCO) ante los responsables del fichero, habiéndose habilitado al efecto el Registro General de Protección de Datos previsto por el artículo 14 de la LOPD, cuya consulta es pública y gratuita.

La obligación de declarar los ficheros se desarrolla en los artículos 20 y 25 de la LOPD, diferenciándose el procedimiento a seguir en función de la naturaleza pública o privada del fichero.

- ***Ficheros públicos y privados***

Tal y como se ha definido en el punto anterior, los ficheros pueden clasificarse en públicos y privados en atención a su titularidad, de forma que los ficheros de las Administraciones Públicas (Ayuntamientos, Diputaciones, Ministerios, etc.) deberán declararse como ficheros de naturaleza pública y los ficheros de las entidades de naturaleza privada (S.A., S.L., C.B., Comunidades de propietarios, etc.) como ficheros privados.

[4] *Véase Tema 9 del presente Curso.*

4.3. Inscripción de Ficheros: Procedimiento y Contenido

La creación, modificación o supresión de ficheros deberá ser notificada, en todo caso, a la Autoridad de Control competente para que proceda, en su caso, a la inscripción de los mismos en el Registro General de Protección de Datos.

En este sentido, el artículo 39.2 de la Ley Orgánica 15/1999 delimita claramente el contenido del Registro General de Protección de Datos, disponiendo que "serán objeto de inscripción en el Registro General de Protección de Datos:

a) Los ficheros de que sean titulares las Administraciones Públicas.
b) Los ficheros de titularidad privada.
c) Las autorizaciones a que se refiere la presente Ley.
d) Los códigos tipo a que se refiere el artículo 32 de la presente Ley.
e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

A continuación se analiza el procedimiento para solicitar la inscripción, el contenido de la misma y las particularidades asociadas a la inscripción de ficheros de titularidad pública, puesto que la presente guía está orientada a organismos públicos.

- ***Ficheros de titularidad pública***

El artículo 20 de la LOPD, desarrollado por el artículo 52 del RLOPD, dispone que "*la creación, modificación o supresión de los ficheros de titularidad pública sólo podrá hacerse por medio de* ***disposición general o acuerdo publicados en el «Boletín Oficial del Estado» o diario oficial correspondiente****. En todo caso, la disposición o acuerdo deberá dictarse y publicarse con carácter previo a la creación, modificación o supresión del fichero*."

En este sentido, todo fichero de datos de carácter personal de titularidad pública debe notificarse a la Agencia Española de Protección de Datos, o a la Autoridad de Control que corresponda, por el órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, en el **plazo de treinta días desde la publicación de su norma o acuerdo** de creación, modificación o supresión, **en el diario oficial correspondiente**.

La notificación de ficheros de titularidad pública debe practicarse adjuntando una copia de la norma o acuerdo de creación, modificación o supresión del fichero, salvo que el diario oficial en el que se encuentre publicada la norma o acuerdo sea accesible a través de internet, en cuyo caso será suficiente con indicar en la notificación la dirección electrónica que permita su concreta localización.

Fig.2 - Inscripción de ficheros de titularidad pública

- ***Contenido de la disposición o acuerdo***

Las disposiciones de carácter general o acuerdos que se adopten por el órgano responsable del fichero para la creación, modificación o supresión de ficheros de titularidad pública deben incluir los extremos regulados por el artículo 54 del RLOPD.

En este sentido, se establece que la **disposición o acuerdo de creación del fichero** debe contener los siguientes extremos:

a) *La identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos.*
b) *El origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia.*
c) *La estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización.*
d) *Las comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios.*
e) *Las transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos.*
f) *Los órganos responsables del fichero.*
g) *Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición (en adelante, derechos ARCO).*

h) *El nivel básico, medio o alto de seguridad que resulte exigible, de acuerdo con lo establecido en el título VIII del presente reglamento.*

En relación a la **disposición o acuerdo de modificación** de ficheros se establece que debe indicar las modificaciones producidas en cualquiera de los apartados indicados anteriormente en relación a la disposición de creación.

Respecto de las **disposiciones o acuerdos que se dicten para la supresión** de ficheros se establece que deben indicar el destino que vaya a darse a los datos, y las previsiones que se adopten para la destrucción de los datos, en su caso.

5. Legitimación

5.1. Principio de Calidad

El principio de calidad se halla regulado en el artículo 4 de la LOPD en los términos siguientes:

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

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

3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16 de la LOPD.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

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

El desarrollo reglamentario de este principio se realiza por el artículo 8 del RLOPD, ampliándose el régimen aplicable a la rectificación de datos de oficio por el responsable del fichero y definiéndose el plazo de conservación de los datos bloqueados como consecuencia de la cancelación de los datos. En este sentido, se establece que:

> *"5. […] Si los datos de carácter personal sometidos a tratamiento resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados en el plazo de diez días desde que se tuviese conocimiento de la inexactitud, salvo que la legislación aplicable al fichero establezca un procedimiento o un plazo específico para ello.*
>
> *Cuando los datos hubieran sido comunicados previamente, el responsable del fichero o tratamiento deberá notificar al cesionario, en el plazo de diez días, la rectificación o cancelación efectuada, siempre que el cesionario sea conocido. En el plazo de diez días desde la recepción de la notificación el cesionario que mantuviera el tratamiento de los datos, deberá proceder a la rectificación y cancelación notificada.*
>
> *Esta actualización de los datos de carácter personal no requerirá comunicación alguna al interesado, […].*
>
> *6. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.*
>
> *No obstante, podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado.*
>
> *Una vez cumplido el período al que se refieren los párrafos anteriores, los datos sólo podrán ser conservados previa disociación de los mismos, sin perjuicio de la obligación de bloqueo prevista en la LOPD y el RLOPD."*

Del análisis de los artículos anteriores puede extraerse el contenido del principio de calidad que se sintetiza en:

- Pertinencia de los datos
- Veracidad o exactitud de los datos
- Cancelación de oficio

- ***Pertinencia***

Implica que los datos de carácter personal recabados y tratados deben ser adecuados, pertinentes y no excesivos en relación con las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

De forma que se prohíbe el uso de los datos con finalidades incompatibles, y la recogida de datos por medios fraudulentos, desleales o ilícitos.

En otras palabras el responsable del fichero debe analizar la documentación que utiliza para recabar datos de carácter personal para determinar la pertinencia de los datos obtenidos a través de los mismos. Asimismo deberá analizar sus ficheros para establecer si los datos contenidos en los mismos son adecuados, pertinentes y no excesivos en relación a las finalidades de los mismos (recaudación, padrón, gestión de recursos humanos, etc.).

Un dato será impertinente si no es necesario para dar cumplimiento a la finalidad prevista para el tratamiento y fichero de que se trate. Así, por ejemplo, conocer el DNI del suscriptor de un boletín electrónico gratuito de carácter mensual, cuyos datos se incluyen en el fichero de "Suscriptores" que tiene como finalidad la gestión del boletín, es un dato impertinente para la finalidad indicada ya que es innecesario conocer este dato por parte del responsable del fichero para remitir dicho boletín.

- ***Exactitud***

El responsable del fichero o tratamiento debe preocuparse de mantener los datos exactos y actualizados de forma que respondan con veracidad a la situación actual del afectado. Esta obligación de rectificación de los datos opera de oficio en el sentido de que desde el momento en que el responsable del fichero o tratamiento tenga constancia, por cualquier medio, de la inexactitud de los datos debe proceder a rectificarlos y sustituirlos, sin la previa solicitud del interesado, en el plazo de 10 DÍAS y comunicarlo a aquellos Terceros a los que hubiese comunicado dichos datos para que procedan, en el mismo plazo, a la rectificación de los mismos.

- ***Cancelación***

El responsable del fichero o tratamiento debe cancelar los datos del interesado cuando éstos hayan dejado de ser necesarios o pertinentes en relación a la finalidad para la que fueron recabados.

La cancelación de los datos implica que el responsable del fichero o tratamiento procede al **bloqueo** de los mismos, adoptando las medidas necesarias para garantizar que no se realiza ningún tratamiento accidental de los datos. Dicho bloqueo implica que los datos se **conserven durante el tiempo en que pueda exigirse algún tipo de responsabilidad** para el responsable del fichero o tratamiento derivada de una relación u obligación jurídica o de la ejecución de un contrato. Transcurrido el plazo asociado a estas responsabilidades deberá procederse a la **supresión/eliminación** de los datos de los ficheros del responsable del fichero o tratamiento; salvo que los mismos se sometan a un **procedimiento de disociación** por el que los datos afectados no permitan la identificación del interesado.

Dicho de otro modo y aplicando un ejemplo, cuando un trabajador deje de formar parte de la Organización, por jubilación o por cualquier otra causa, el responsable del fichero o tratamiento deberá proceder al bloqueo de sus datos por cuanto la finalidad que legitimó la obtención de los datos fue la relación de carácter laboral que unía al interesado con la organización, finalizada dicha relación los datos devienen impertinentes y, en consecuencia, el responsable del fichero debe proceder a bloquearlos hasta que prescriban las responsabilidades asociadas a este tipo de relación, es decir, cinco años, teniendo en cuenta las obligaciones asociadas al régimen de la seguridad social.

5.2. Principio de Información

El principio de información se halla regulado, esencialmente, en el artículo 5 de la LOPD. A través de este principio se materializa el contenido del derecho a la protección de datos, en su vertiente informativa, en cuanto permite al interesado conocer "*en todo momento quién dispone de [sus] datos personales y a qué uso los está sometiendo" (STC 292/2000)*.

Este principio impone al responsable del fichero o tratamiento la obligación de informar a los interesados sobre el tratamiento de sus datos y los derechos que les asisten. En este sentido, en función del origen de los datos, es decir, si proceden del interesado o de un tercero distinto del interesado, el contenido de la información proporcionada al interesado y la modalidad de cumplimiento del deber de información difieren:

- ***Datos facilitados por el interesado***

El apartado 1 del artículo 5 de la LOPD dispone que "*los interesados a los que se soliciten datos personales deberán ser previamente* ***informados de modo expreso, preciso e inequívoco*** *[sobre]:*

a) La existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) El carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) Las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) La posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) *La identidad y dirección del responsable del tratamiento o, en su caso, de su representante.*

En relación con este contenido mínimo debe tenerse en cuenta que la información a que se refieren las letras b), c) y d), no es necesaria siempre y cuando ésta se deduzca claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

Por ejemplo, si se solicita la dirección postal para la entrega de un paquete es obvio que si no se facilita dicho dato no podrá realizarse el servicio contratado, de forma que la información referida a las letras b) y c) no sería necesaria.

La LOPD establece la obligación, para el responsable del fichero o tratamiento, de incluir en todos aquellos **cuestionarios o impresos** (en formato papel o electrónico) que utilice en la recogida de datos, de forma claramente legible, el contenido mínimo al se acaba de hacer referencia (artículo 5.1).

- ***Datos facilitados por un tercero diferente del interesado***

Cuando los datos de carácter personal no hayan sido recabados del interesado, el responsable del fichero o tratamiento debe informarle de forma expresa, precisa e inequívoca, dentro de los 3 MESES siguientes al momento del registro de los datos, sobre:

- *Contenido del tratamiento,*
- *La procedencia u origen de los datos,*
- *La existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.*
- *La posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.*
- *La identidad y dirección del responsable del tratamiento o, en su caso, de su representante.*

En relación con este contenido mínimo también es aplicable la excepción descrita en relación al punto anterior sobre la inclusión de la información a que se refieren las letras b), c) y d) del artículo 5.1 de la LOPD.

La información descrita en los apartados anteriores no deberá llevarse a cabo en aquellos casos en que:

- El interesado ya hubiera sido informado con anterioridad sobre el tratamiento de sus datos por el responsable del fichero o tratamiento. *Por ejemplo, en aquellos casos en que los datos los proporciona otra Entidad que informó al interesado de la cesión de sus datos a nuestra Organización y de la finalidad de dicha cesión no será necesario informar, de nuevo, al interesado*;
- Una Ley expresamente así lo prevea;
- El tratamiento tenga fines históricos, estadísticos o científicos;
- La información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Autoridad de Control competente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias;
- Los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial.

5.3. Principio de Consentimiento

El principio de consentimiento se halla regulado por múltiples artículos de la LOPD y su Reglamento de desarrollo (artículos 6 y 11 de la LOPD; y, artículos 10 y siguientes del RLOPD). A través de este principio se materializa la vertiente dispositiva del contenido del derecho a la protección de datos, por cuanto implica "*la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular [por parte del interesado]*" (STC 292/2000).

Este principio implica que el responsable del fichero o tratamiento debe **obtener el consentimiento, previo e informado, del interesado** para el tratamiento de sus datos (recogida, tratamiento y/o cesión), salvo en aquellos supuestos en que el mismo no sea exigible debido a la concurrencia de alguna de las excepciones previstas en la LOPD.

Se considerará que el consentimiento es informado cuando incluya los requisitos establecidos por el artículo 5.1 de la LOPD, relativo al deber de información, y los extremos que en su caso se requieran en función del tipo de tratamiento respecto del que se solicite el consentimiento.

En este sentido, en función del tipo de tratamiento respecto del que se solicita el consentimiento, el contenido de la información proporcionada al interesado es diferente. En este sentido, pueden mencionarse los siguientes **tipos de consentimiento en función del tratamiento**:

- Consentimiento para el tratamiento de los datos
- Consentimiento para la cesión de los datos
- Consentimiento para tratamientos accesorios
- Consentimiento para el tratamiento de datos de menores de edad

Si el consentimiento obtenido no cumple los requisitos necesarios, en relación al tratamiento de que se trate, el consentimiento será nulo y, en consecuencia, será sancionable.

En este sentido corresponde al responsable del fichero o tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho.

- ***Consentimiento para el tratamiento de los datos***

La solicitud de consentimiento debe referirse a un tratamiento o serie de tratamientos concretos, con respecto a una finalidad o finalidades determinadas, así como las restantes condiciones que concurran en el tratamiento o serie de tratamientos.

No obstante lo anterior, los datos de carácter personal pueden **tratarse sin necesidad del consentimiento** del interesado cuando:

a) *Lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los supuestos siguientes:*
   - *El tratamiento tenga por objeto la satisfacción de un interés legítimo del responsable del tratamiento amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados.*
   - *El tratamiento sea necesario para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas.*

b) *Los datos objeto de tratamiento figuren en fuentes accesibles al público y el responsable del fichero tenga un interés legítimo para su tratamiento o conocimiento, siempre que no se vulneren los derechos y libertades fundamentales del interesado.*

   No obstante, las Administraciones públicas sólo podrán comunicar datos recogidos de fuentes accesibles al público a responsables de ficheros de titularidad privada cuando se encuentren autorizadas para ello por una norma con rango de ley.

c) *Se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de las competencias que les atribuya una norma con rango de ley o una norma de derecho comunitario.*

d) *Se recaben por el responsable del tratamiento con ocasión de la celebración de un contrato o precontrato o de la existencia de una relación negocial, laboral o administrativa de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento.*

e) *El tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del apartado 6 del artículo 7 de la LOPD.*

En estos casos, en los que no es necesario el consentimiento del afectado para el tratamiento de sus datos, el interesado puede **oponerse al tratamiento** de sus datos cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero debe excluir del tratamiento los datos relativos al afectado. Esta potestad de oponerse al tratamiento no opera cuando una Ley disponga lo contrario.

- ***Consentimiento para la cesión de los datos***

Cuando el responsable del fichero o tratamiento solicite el consentimiento del interesado para la cesión de sus datos, debe informarle de forma que conozca inequívocamente **la finalidad a la que se destinarán los datos** respecto de cuya comunicación se solicita el consentimiento y el **tipo de actividad desarrollada por el cesionario**.

No obstante lo anterior, es posible la **cesión de los datos de carácter personal sin necesidad del consentimiento** del interesado cuando:

a) *Lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los supuestos siguientes:*
   - *La cesión tengan por objeto la satisfacción de un interés legítimo del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados.*
   - *La cesión de los datos sea necesario para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas.*

b) *Los datos objeto de cesión figuren en fuentes accesibles al público y el tercero a quien se comuniquen los datos tenga un interés legítimo para su tratamiento o conocimiento, siempre que no se vulneren los derechos y libertades fundamentales del interesado.*

   No obstante, las Administraciones públicas sólo podrán comunicar datos recogidos de fuentes accesibles al público a responsables de ficheros de titularidad privada cuando se encuentren autorizadas para ello por una norma con rango de ley.

c) *La cesión responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control comporte la comunicación de los datos. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.*

d) *La comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas o a las instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas y se realice en el ámbito de las funciones que la ley les atribuya expresamente.*

e) *La cesión entre Administraciones públicas cuando concurra uno de los siguientes supuestos:*
   - *Tenga por objeto el tratamiento de los datos con fines históricos, estadísticos o científicos.*
   - *Los datos de carácter personal hayan sido recogidos o elaborados por una Administración pública con destino a otra.*
   - *La comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias.*

- ***Consentimiento para tratamientos accesorios***

Cuando el responsable del fichero o tratamiento solicite el consentimiento del afectado, durante la formación de un contrato, para **finalidades que no guarden relación directa con el mantenimiento,**

desarrollo o control de la relación contractual, debe permitirle manifestar expresamente su negativa al tratamiento o cesión de sus datos.

En particular, se entiende cumplida la obligación anterior si se permite al afectado la marcación de una **casilla claramente visible y que no se encuentre ya marcada** en el documento que se le entregue para la celebración del contrato, o bien si el responsable del fichero o tratamiento establece un **procedimiento equivalente** que permita al interesado manifestar su negativa al tratamiento cuyo consentimiento se solicita.

Por ejemplo, si el responsable del fichero o tratamiento quisiera solicitar el consentimiento del interesado para la remisión de un boletín mensual debería cumplir con los requisitos establecidos en este apartado, es decir, incluir una casilla no premarcada en la que se facilitase al interesado la posibilidad de negarse a dicho tratamiento.

- ***Consentimiento para el tratamiento de datos de menores de edad***

El tratamiento de datos de carácter personal de interesados menores de edad (18 años) tiene un **régimen específico** según el cual el tratamiento de datos de:

- **Mayores de catorce años**, puede consentirse por el propio interesado o menor, salvo en aquellos casos en los que la Ley exija la asistencia de los titulares de la patria potestad o tutela.
- **Menores de catorce años**, requiere en todo caso el consentimiento de los padres o tutores.

Este consentimiento debe ir referido, en todo caso, a los datos de los que sea titular el interesado o menor, de forma que en ningún caso podrán recabarse datos que permitan obtener información sobre los demás **miembros del grupo familiar**, o sobre las características del mismo, sin el consentimiento de los titulares de tales datos (*por ejemplo, datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros*). No obstante, si pueden recabarse los datos de identidad y dirección del padre, madre o tutor, siempre y cuando se utilicen con la única finalidad de recabar la autorización indicada anteriormente.

La información dirigida a los interesados menores debe expresarse en un lenguaje que sea **fácilmente comprensible** para éstos.

Por otro lado, el responsable del fichero o tratamiento tiene la obligación de articular los **procedimientos necesarios** para garantizar que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales.

- *Forma de recabar el consentimiento*

El responsable del tratamiento puede recabar el consentimiento del interesado de forma expresa o tácita:

- El **consentimiento expreso** implica que el interesado realiza un acción positiva autorizando el tratamiento (por escrito, verbal, etc.).

- El **consentimiento tácito**, regulado expresamente en el artículo 14 del RLOPD, implica que el responsable se dirige al interesado, informándole en los términos previstos en los artículos 5 de la LOPD, y le concede un plazo de 30 DÍAS para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos.

  El responsable del fichero debe utilizar medios de comunicación que le permitan conocer si la comunicación ha sido objeto de **devolución por cualquier causa**, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

  En este sentido, el responsable del fichero o tratamiento debe facilitar al interesado un **medio sencillo y gratuito** para manifestar su negativa al tratamiento de sus datos.

  Este tipo de consentimiento **no es admisible** para el tratamiento de datos especialmente protegidos.

  Se posibilita que el responsable del fichero o tratamiento, que preste al interesado un servicio que genere **información periódica o reiterada, o facturación periódica**, pueda obtener el consentimiento tácito mediante la incorporación del mismo a la información periódica o a la facturación del servicio prestado. Esta información deberá ser claramente legible.

En ningún caso se admite el consentimiento presunto. Este consentimiento implica que se desarrolla el tratamiento materialmente, sin haber informado al interesado sobre el mismo, mientras el interesado no manifieste su negativa al mismo.

- *Revocación del consentimiento*

El consentimiento prestado por el interesado a través de cualquier de los procedimientos descritos en el punto anterior puede ser revocado **en cualquier momento** por el interesado, cuando exista causa justificada y sin efectos retroactivos.

Con este fin, debe proporcionarse al interesado un **medio sencillo, gratuito y que no implique ingreso alguno para el responsable** del fichero o tratamiento, para revocar el consentimiento prestado.

En particular, se considera **conforme al RLOPD** el envío prefranqueado al responsable del tratamiento o la llamada a un número telefónico gratuito o a los servicios de atención al público establecidos por el responsable. Por el contrario**, no se consideran conformes**, el envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste adicional al interesado.

El responsable debe cesar en el tratamiento de los datos del interesado que revoca su consentimiento en el plazo máximo de 10 DÍAS a contar desde la recepción de la revocación del consentimiento, sin perjuicio de su obligación de bloquear los datos conforme a lo dispuesto en el artículo 16.3 de la LOPD (cancelación de datos).

En caso de que el interesado solicite la confirmación del cese en el tratamiento de sus datos por parte del responsable del fichero o tratamiento, éste deberá responder expresamente a la solicitud.

Por otro lado, si los datos hubieran sido cedidos a un tercero, el responsable del tratamiento deberá comunicarlo a los cesionarios, en el plazo de 10 DÍAS desde la revocación del consentimiento, para que éstos, cesen en el tratamiento de los datos en caso de que aún los mantuvieran.

5.4. Datos especialmente protegidos

Se consideran *datos especialmente protegidos*, los relativos a **ideología, afiliación sindical, religión, creencias, origen racial o étnico, vida sexual y salud**. El régimen jurídico de este principio se regula por los artículos 7 y 8 de la LOPD.

En relación con este tipo de datos se establece:

- 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 de los interesados.
- La necesidad de obtener el **consentimiento expreso** para el tratamiento de los relativos al origen racial o étnico, vida sexual y salud; y el **consentimiento expreso y por escrito** para el tratamiento de datos relativos a la ideología, afiliación sindical, religión o creencias.

  El consentimiento indicado anteriormente **no es necesario** para ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.
- La obligatoriedad de advertir al interesado de la posibilidad de no prestar su consentimiento en relación al tratamiento de datos relativos a su ideología, religión o creencias.

No obstante lo anterior podrán tratarse datos especialmente protegidos sin el consentimiento del interesado, cuando:

- Lo autorice una ley por razones de interés general
- El tratamiento resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, por parte de un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.
- El tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.
- Los destinatarios de los datos personales sobre la salud de los interesados sean organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas.

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

5.5. Confidencialidad

El principio de confidencialidad o deber de secreto se regula por el artículo 10 de la LOPD, cuyo contenido determina que:

> *"El Responsable del Fichero, así como quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal, están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo"*.

Por tanto, este principio determina que por el mero hecho de tratar o acceder a datos de carácter personal existe la **obligación legal de guardar secreto** sobre los mismos. Esta obligación atañe a **quienes intervengan en cualquier fase del tratamiento**, por tanto:

- Responsable del fichero o tratamiento
- Usuarios de la Organización
- Encargados del tratamiento
- Terceros

La duración de esta obligación es **indefinida**, es decir, subsiste aún después de finalizar la relación con el responsable del fichero que justifica el acceso o tratamiento de los datos.

5.6. Principio de Cesión

El principio de cesión se regula con carácter general por el artículo 11 de la LOPD e implica que el responsable del fichero o tratamiento debe obtener el **consentimiento previo e informado** del interesado para comunicar sus datos a un tercero, salvo que concurra alguna de las excepciones legalmente previstas.

En este sentido, existe cesión de datos desde el momento en que se revelan datos de carácter personal a persona distinta del interesado (tercero).

P.ej.: la simple consulta que un tercero realice a los datos aunque sea a distancia y sin creación de un fichero o tratamiento nuevo se considera cesión.

El consentimiento para la cesión de los datos requiere que se **informe** al interesado sobre la finalidad a que destinarán los datos cuya comunicación se autoriza y el tipo de actividad de aquel a quien se pretenden comunicar; y es **revocable** en todo momento.

Los terceros destinatarios de los datos, también conocidos como **Cesionarios**, están obligados a la observancia de la LOPD y su Reglamento de desarrollo por el solo hecho de la comunicación (artículo 11.5 de la LOPD).

En relación con esta figura si bien la LOPD no exige la formalización del contrato conviene que el responsable del fichero o tratamiento, **cedente** de los datos, suscriba un **contrato** con los cesionarios en el que se regule el régimen de cesión de los datos en el que se refleje el origen de los datos y, en su caso, la obtención del consentimiento, así como todas aquellas cuestiones que puedan afectar a la confidencialidad y legitimación de la cesión de los datos.

Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

5.7. Principio de Acceso a Datos

El artículo 12 de la LOPD regula este principio como excepción al principio de cesión. Es decir, en su apartado 1, determina que:

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

En otras palabras, se considera el acceso a datos por parte de un tercero cuando se cumplen los siguientes **requisitos**:

- el acceso a datos de carácter personal es necesario para la prestación de un servicio
- beneficiario del servicio es el responsable del fichero o tratamiento

No obstante, se considerará que existe cesión de datos cuando el acceso tenga por objeto el establecimiento de un **nuevo vínculo** entre quien accede a los datos y el afectado.

En otras palabras, no se considerará cesión de datos, el acceso de un tercero a los datos, cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento, salvo que el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado. En el primer caso, el tercero prestador de servicios tendrá la condición de **encargado del tratamiento**, y en el segundo caso, tendrá la condición de **cesionario**.

El responsable del fichero o tratamiento está obligado a formalizar un **contrato** con los **encargados del tratamiento** cuyo **contenido mínimo** es:

- Compromiso del encargado del tratamiento de
  - Tratar los datos únicamente conforme a las instrucciones del responsable del tratamiento
  - No aplicar o utilizar los datos con fin distinto al que figure en el contrato
  - No comunica los datos, ni siquiera para su conservación, a otras personas.
- Las medidas de seguridad a que se refiere el artículo 9 de la LOPD que el encargado del tratamiento está obligado a implementar.

Este contrato, comúnmente conocido como **contrato de acceso a datos**, debe ser previo a la efectiva prestación del servicio y constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido.

En el caso de que el **encargado del tratamiento** destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, **respondiendo de las infracciones en que hubiera incurrido personalmente**.

No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo.

En relación con la contratación de este tipo de proveedores, encargados del tratamiento, conviene tener presente que el artículo 20.2 del RLOPD determina que "*cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento*". Por tanto se exige **diligencia en la elección del encargado y deber de vigilancia** en relación al cumplimiento de las garantías exigidas por el RLOPD.

- ***Posibilidad de subcontratación de los servicios***

El encargado del tratamiento **no puede subcontratar con un tercero** la realización de ningún tratamiento encomendado por el responsable del tratamiento, **salvo** que haya obtenido de éste **autorización** para ello. En este caso, la contratación se efectuará en nombre y por cuenta del responsable del tratamiento.

No obstante lo anterior, es **posible la subcontratación** sin necesidad de la autorización mencionada siempre y cuando se cumplan los siguientes **requisitos**:

a) Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar.

   Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, el encargado del tratamiento deberá comunicar al responsable los datos que la identifiquen antes de proceder a la subcontratación.

b) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.
c) Que el encargado del tratamiento y la empresa subcontratista formalicen un contrato, en los términos previstos en el artículo 12 de la LOPD.

En este caso, el subcontratista tendrá la condición de encargado del tratamiento.

Por otro lado, si durante la prestación del servicio resulta necesario subcontratar una parte del mismo y dicha circunstancia no se ha previsto en el contrato, deberá obtenerse la autorización del responsable del tratamiento (servicio subcontratado y empresa subcontratada).

- *Conservación de los datos por el encargado del tratamiento*

Una vez **cumplida la prestación contractual**, los datos de carácter personal deberán ser **destruidos o devueltos** al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

No procederá la destrucción de los datos cuando exista una **previsión legal que exija su conservación**, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.

El encargado del tratamiento conservará, debidamente **bloqueados**, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

5.8. Cesión vs. Acceso

El acceso a datos difiere de la cesión en que:

- La prestación del servicio es a favor del responsable del fichero o tratamiento
- No existe un vínculo jurídico directo con el interesado
- Debe formalizarse el contrato exigido por la LOPD con el responsable del fichero o tratamiento (contrato de acceso a datos)
- El responsable del fichero no debe informar al interesado sobre el tratamiento realizado por el encargado del tratamiento ni obtener su consentimiento

En este sentido, los terceros a quienes nuestra organización cede datos personales (salida de datos) se denominan **Cesionarios**; mientras que los terceros que ceden datos a nuestra organización (entrada de datos) se denominan **Cedentes**.

Dicho de otro modo, la cesión se diferencia del acceso a datos en que:

- La prestación del servicio es a favor del interesado
- Existe un vínculo jurídico directo con el interesado
- No debe formalizarse ningún contrato por Ley
- El responsable del fichero debe informar al interesado sobre la cesión de sus datos (finalidad y tipo de actividad del Cesionario) y, en su caso, obtener su consentimiento

En este sentido, los terceros que prestan servicios que impliquen un acceso a datos personales de los que es responsable nuestra Organización (salida de datos) se denominan **Encargados del tratamiento**; mientras que los terceros a quienes nuestra Organización presta servicios que implican el acceso a datos personales de los que son responsables estos terceros (entrada de datos) se denominan **Entidad Gestionada**.

6. Seguridad y Protección

6.1. Principio de Seguridad

El principio de seguridad en materia de protección de datos, regulado en el artículo 9 de la LOPD, implica que "*el responsable del fichero y, en su caso, el encargado del tratamiento están obligados a adoptar las* ***medidas de índole técnica y organizativas necesarias para garantizar la seguridad*** *de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural*".

Asimismo, **se prohíbe** el registro de datos de carácter personal "*en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamientos, locales, equipos, sistemas y programas*". La regulación por vía reglamentaria de las condiciones de seguridad de los ficheros y sus sistemas de tratamiento y/o almacenamiento se desarrolla en el Título VIII del Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre (en adelante, RLOPD).

En resumen, el **principio de seguridad**:

- Obliga tanto al responsable del fichero[5] o tratamiento como a los encargados del tratamiento[6].
- Significa que los ficheros y sus sistemas de tratamiento y/almacenamiento deben cumplir, como mínimo, las medidas establecidas en el RLOPD.
- Implica la adopción de las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos y evitar su alteración, pérdida, tratamiento o acceso no autorizado, teniendo cuenta:
    - El estado de la tecnología
    - La naturaleza de los datos tratados
    - Los riesgos a que estén expuestos los datos, con independencia de su origen.

Teniendo en cuenta lo anterior, puede concluirse que las medidas de seguridad que debe implantar cualquier organización, que trate datos de carácter personal, se clasifican en: **medidas de seguridad mínimas** y **medidas de seguridad necesarias**.

---

[5] *Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del fichero o tratamiento.*

[6] *La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.*

En este sentido, son medidas de seguridad mínimas, las establecidas por el Reglamento de desarrollo de la LOPD, y medidas de seguridad necesarias, aquellas que deben implantarse habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural. Por tanto, si las medidas contempladas en el RLOPD no fueran suficientes para garantizar la seguridad de los datos, deberá implantarse, además, aquellas medidas que al efecto se considere oportunas para garantizar la confidencialidad, integridad y disponibilidad de los datos.

Ni la LOPD ni su Reglamento de desarrollo establecen la tecnología que debe utilizarse para cumplir con sus previsiones, pero sí que exigen las condiciones que debe reunir la misma para considerarse adecuada. Asimismo, se establece la temporalidad de dicha adecuación, ya que la misma se considerara adecuada en cuanto el estado de la tecnología así lo permita, siempre y cuando la tipología de datos tratados y los riesgos a los que se hallen éstos expuestos no varíen; en tal caso, deberán readecuarse las medidas adoptadas. En conclusión, el principio de seguridad es de cumplimiento constante e implica que debe readecuarse la situación técnica y organizativa de la organización permanentemente.

6.2. Niveles de Seguridad

Los responsables de los tratamientos o los ficheros y los encargados del tratamiento deben implantar las medidas de seguridad con arreglo a lo dispuesto en este Título VIII del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (en adelante, RLOPD).

En este sentido, las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en **tres niveles**: Básico, Medio y Alto.

El artículo 81 del RLOPD determina los criterios que deben seguirse para la aplicación de los niveles de seguridad indicados en el párrafo anterior, en atención a la tipología de datos, la finalidad del tratamiento y el responsable del fichero.

	Tipo de Datos
Nivel Alto	*Ficheros o tratamientos que contengan datos:* ▪ *Relativos a ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, siempre y cuando no se prevea la posibilidad de adoptar el nivel básico.* ▪ *Recabados para fines policiales sin consentimiento de los afectados.* ▪ *Derivados de actos de violencia de género.*
Nivel Medio	*Ficheros o tratamientos que contengan datos:* ▪ *Relativos a la comisión de infracciones administrativas o penales.* ▪ *Derivados de la prestación de servicios de solvencia patrimonial y crédito (artículo 29 de la LOPD).* ▪ *Un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los afectados y que permitan evaluar determinados aspectos de la misma o del comportamiento de éstos.* *Ficheros de los que sean responsables:* ▪ *Administraciones tributarias, cuando se relacionen con el ejercicio de sus potestades tributarias.* ▪ *Entidades financieras, para finalidades relacionadas con la prestación de servicios financieros*[7]. ▪ *Entidades Gestoras y Servicios Comunes de la Seguridad Social, cuando se relacionen con el ejercicio de sus competencias.* ▪ *Mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social, cuando se relacionen con el ejercicio de sus competencias.* ▪ *Operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas, respecto a los datos de tráfico y a los datos de localización*[8]

Nivel Básico	▪ *Cualquier otro fichero que contenga datos de carácter personal, siempre y cuando no pueda incluirse en ninguno de los niveles anteriores.*
	▪ *Ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, cuando:*
	  ▪ *Se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.*
	  ▪ *Se contengan de forma incidental o accesoria, sin guardar relación con la finalidad del fichero.*
	▪ *Ficheros que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.*

Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

[7] *Se incluye los epígrafes 65, 66 y 67 del Real Decreto 1560/1992, de 18 de diciembre, por el que se aprueba la clasificación nacional de actividades económica.*

[8] *El artículo 81.4 del RLOPD determina que este tipo de ficheros deben aplicar, además de las medidas de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 del RLOPD, relativa al registro de accesos a ficheros automatizados.*

Dichas medidas de seguridad son **acumulativas** y varían en función del nivel de seguridad aplicable al fichero y el sistema de tratamiento del fichero.

Por sistema de tratamiento, se entiende el modo en que se organiza o utiliza un sistema de información[9]. Los sistemas de tratamiento pueden ser automatizados, no automatizados (manual o papel) o parcialmente automatizados (mixtos).

Por otro lado, respecto al ***régimen de seguridad de los datos especialmente protegidos*** conviene tener presente que el nivel de seguridad aplicable a los mismos es, por defecto, el alto; únicamente cuando concurra algunas de las excepciones previstas por los artículos 81.5 y 6 del RLOPD será posible – por tanto, facultativo- aplicar el nivel básico sin infringir la normativa sobre protección de datos.

La Agencia Española de Protección de Datos se ha pronunciado, en múltiples informes, sobre los criterios interpretativos de la regla y excepciones aplicables al régimen de seguridad de los datos especialmente protegidos:

Excepciones	Descripción	Nivel
Tratamiento de **datos de salud en cumplimiento de deberes públicos**	Puede aplicarse la excepción en aquellos supuestos en los que la Ley imponga al responsable del fichero la obligación de conocer los datos, de modo que únicamente mediante el tratamiento de dichos datos pueda aquél dar pleno cumplimiento a los deberes que la Ley le impone. Así: El tratamiento referido al **grado de minusvalía del trabajador (porcentaje de discapacidad; discapacidad si/no; invalidez)**, la **existencia o inexistencia de incapacidad laboral (si/no, fecha, enfermedad común/accidente laboral/enfermedad profesional)**.	Básico
	Datos sobre la **enfermedad o situación de salud concreta** que causa la incapacidad laboral o la discapacidad. Inclusión de un **código numérico que permita determinar la patología concreta** (por ejemplo: para notificar los accidentes de trabajo a los órganos competentes).	Alto
Tratamiento de datos especialmente protegidos[10] con la **única finalidad** de realizar una **transferencia dineraria a las entidades** de las que los afectados sean asociados o miembros	El **tratamiento debe realizarse por parte de una entidad distinta a aquélla de la que "los afectados sean socios o miembros"** y con la única finalidad de proceder a la **transferencia dineraria con destino a la entidad de la que el afectado sea miembro o asociado** (por ejemplo: para la detracción de cuota sindical o domiciliaciones bancarias).	Básico
	Las entidades responsables del fichero o tratamiento son las beneficiarias de la transferencia (**asociación religiosa, partido o sindicato, etc**.) y tratan datos especialmente protegidos de sus socios o miembros.	Alto

[9] *Conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal (artículo 5.2.m RLOPD).*

[10] *Se consideran datos especialmente protegidos, los datos relativos a la ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual de una persona (artículo 7 de la LOPD).*

Excepciones	Descripción	Nivel
Ficheros o tratamientos en los que de **forma accidental o accesoria** se contengan datos especialmente protegidos	La **finalidad del fichero no debe ser tratar datos especialmente protegidos** y el **responsable no debe haber solicitado al titular este tipo de datos**. Generalmente será el titular de los datos personales u otro sujeto quién sin habérsele requerido para que facilite el dato, lo aporte.	Básico
	El responsable del fichero solicita al titular este tipo de datos para su inclusión en un fichero.	Alto

Tabla 3 - Excepciones del artículo 81.5 y 6 del RLOPD

Por otro lado, debe tenerse en cuenta que el nivel de seguridad de las medidas a aplicar a los ficheros y/o tratamientos únicamente depende de la tipología de datos que se tratan o de las finalidades de los tratamientos que se realizan, siendo indiferente, por tanto, la edad o cualquier otra condición del interesado para determinar el nivel aplicable (por ejemplo: ficheros con datos de menores de edad tendrá el nivel de seguridad correspondiente al tipo de datos que se traten).

6.3. Controles, Procedimientos y Medidas de Seguridad

Los controles, procedimientos y medidas de seguridad que los responsables del fichero o tratamiento y sus encargados del tratamiento deben aplicar en cumplimiento del principio de seguridad se hallan regulados en el Título VIII del Reglamento de desarrollo de la LOPD.

Medida de seguridad	RLOPD	Nivel
Documento de Seguridad	Artículo 88 y 82	Básico
Funciones y Obligaciones del Personal	Artículo 89	Básico
Registro de Incidencias	Artículo 90 Artículo 100	Básico Medio
Control de Acceso	Artículo 91 Artículo 99	Básico Medio
Gestión de Soportes y Documentos	Artículo 92 Artículo 97 Artículo 101	Básico Medio Alto
Responsable de Seguridad	Artículos 95 y 109	Medio
Auditoria	Artículos 110 y 96	Medio
Ficheros temporales o copias de documentos	Artículo 87	Básico
Identificación y Autenticación	Artículo 93	Básico
	Artículo 98	Medio

Medida de seguridad	RLOPD	Nivel
Copias de Respaldo y Recuperación	Artículo 94 Artículo 102	Básico Alto
Registro de Accesos	Artículo 103 Artículo 113	Alto Alto
Acceso a datos a través de redes de comunicaciones	Artículo 85	Básico
Telecomunicaciones	Artículo 104	Alto
Procedimiento de Archivo	Artículo 106	Básico
Almacenamiento de la información	Artículo 107 Artículo 111	Básico Alto
Custodia, copia y traslado de la documentación	Artículo 108 Artículo 114 Artículo 112	Básico Alto Alto

Tabla 4 - Cuadro resumen regulación medidas RLOPD

La asignación del nivel de seguridad a un fichero, en atención a la naturaleza de los datos tratados y/o la finalidad de su tratamiento, implica la adopción de **medidas específicas de seguridad**, las cuales se concretan, a su vez, en atención del sistema de tratamiento de los sistemas de información. No obstante lo anterior, existen ciertas **medidas generales de obligado cumplimiento** que deben implantar todas las organizaciones o entidades desde el momento en que realicen tratamientos de datos de carácter personal en el desarrollo de su actividad.

En este sentido, a continuación se analizan los controles, procedimientos y medidas de seguridad aplicables a los ficheros y/o tratamientos de datos de carácter personal, clasificándose las mismas en:

- *Medidas de Seguridad Generales de Obligado Cumplimiento*
- *Ficheros y Tratamientos Automatizados*
- *Ficheros y Tratamientos no Automatizados*

Dentro de cada uno de los puntos indicados, se analiza el contenido de la medida y en qué supuestos, o nivel de seguridad, es aplicable.

En último lugar, se analizan los plazos de implantación establecidos por el RLOPD en relación a las medidas de seguridad mínimas exigidas por el RLOPD.

6.4. Medidas de Seguridad Generales de Obligado Cumplimiento

Las medidas de seguridad que deben aplicarse a los ficheros y/o tratamientos de los que sea responsable cualquier organización en la que se traten datos de carácter personal son las contempladas en este punto del tema.

A continuación se identifican y analizan las medidas de seguridad que, como mínimo, deben aplicarse a los ficheros que contengan datos de carácter personal, así como a cualquier fase de su tratamiento.

	Medidas de seguridad
Documento de seguridad	*Debe elaborarse e implementarse la normativa de seguridad mediante un documento de obligado cumplimiento para todo el personal, cuyo contenido mínimo se establece por los artículos 82 y 88 del RLOPD.* *Puede ser único o individualizado* *Debe revisarse ante cambios relevantes: un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas*
Personal	*Deben definirse las funciones de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información y documentarlas en el documento de seguridad* *Deben definirse las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento* *Debe formarse e informar al personal para que conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento*
Incidencias	*Debe mantenerse un registro, cuyo contenido es: tipo de incidencia, momento en que se ha producido, persona que la notifica, persona a la que se comunica, efectos derivados y medidas correctoras* *Debe establecerse un procedimiento de notificación y gestión de incidencias que afecten a datos de carácter personal*
Gestión de soportes	*Deben adoptarse medidas que eviten acceso indebido o recuperación de la información contenida en soportes desechados (borrado o destrucción), así como para el transporte de soportes* *Deben adoptarse medidas que eviten la sustracción, pérdida o acceso indebido a los soportes y/o documentos durante su traslado* *Los soportes y documentos que contengan datos de carácter personal sólo deben ser accesibles a los usuarios autorizados en el documento de seguridad* *La salida de soportes o documentos fuera de los locales debe ser autorizada por el responsable del fichero o en el documento de seguridad (incluidas a través de e-mail)* *Debe realizarse un inventario de soportes, de forma que se identifique el tipo de información que contiene (mediante un sistema de etiquetado), salvo que sea imposible debido a las características físicas del soporte debiendo justificarse en el documento de seguridad*

<table>
<tr><th></th><th colspan="3">Medidas de seguridad</th></tr>
<tr><td>Control de acceso</td><td colspan="3">Cada usuario debe acceder únicamente a los datos y recursos necesarios para el desarrollo de sus funciones
Debe mantenerse una relación actualizada de usuarios y perfiles de usuarios, y accesos autorizados para éstos
Deben establecerse mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados
La concesión, alteración o anulación de permisos de acceso sólo debe realizarse por el personal autorizado en el documento de seguridad
El personal ajeno que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio</td></tr>
<tr><td>Trabajos fuera de los locales</td><td colspan="3">La ejecución de trabajos fuera de los locales del responsable del fichero o encargado del tratamiento debe ser previamente autorizada por el responsable del fichero, constando en el documento de seguridad, y garantizar el nivel de seguridad exigible</td></tr>
<tr><td>Ficheros temporales</td><td colspan="3">Los ficheros temporales deberán cumplir el nivel de seguridad correspondiente al tipo de datos que contengan y serán borrados una vez que hayan dejado de ser necesarios.</td></tr>
<tr><td rowspan="3">Encargado del tratamiento</td><td colspan="3">El acceso facilitado a un encargado del tratamiento deberá constar en el documento de seguridad y deberá comprometerse al cumplimiento de las medidas de seguridad previstas mediante el correspondiente contrato</td></tr>
<tr><td rowspan="2">Acceso a los datos</td><td>En locales del RF o de forma remota</td><td>Debe hacerse constar esta circunstancia en el documento de seguridad, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.</td></tr>
<tr><td>En locales del ET</td><td>El encargado del tratamiento debe elaborar un documento de seguridad, o completar el que ya hubiera elaborado, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.</td></tr>
<tr><td>Prestaciones sin acceso a datos</td><td colspan="3">Deben adoptarse 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.</td></tr>
</table>

Tabla 5 - Cuadro resumen de medidas de seguridad generales de obligado cumplimiento (I).

A partir del **NIVEL MEDIO** de seguridad, deberán aplicarse a todos los ficheros y/o tratamientos, además de las medidas indicadas anteriormente en relación al nivel básico de seguridad, las medidas siguientes:

	Medidas de seguridad
Documento de seguridad	*Debe identificarse al responsable o responsables de seguridad de la organización* *Deben establecerse controles periódicos para verificar el cumplimiento del Documento de Seguridad*
Responsable de seguridad	*El responsable del fichero debe designar uno o varios (es posible según procesos o tipo de ficheros)* *Se encarga de coordinar y controlar las medidas del documento de seguridad.* *No supone delegación de responsabilidad del responsable del fichero.*
Auditoría	*Debe realizarse una auditoria ordinaria (interna o externa cada dos años para verificar y controlar la adecuación y eficacia de las medidas y controles implantados en la organización.* *Debe realizarse una auditoria extraordinaria cuando se produzcan modificaciones sustanciales en los sistemas de información que repercutan en las medidas de seguridad implantadas. Esta auditoría inicia el cómputo de dos años.* *La auditoria, ordinaria o extraordinaria, concluye con un informe sobre las deficiencias detectadas y las medidas correctoras propuestas (artículo 96 RLOPD).* *Los informes de auditoría deben analizarse por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas.*

Tabla 6 - Cuadro resumen de medidas de seguridad generales de obligado cumplimiento (II).

6.5. Ficheros y Tratamientos Automatizados

Aquellos ficheros o tratamientos que sean automatizados o parcialmente automatizados, deberán aplicar, además de las medidas descritas en el punto anterior 6.4, las siguientes medidas de seguridad:

	Medidas de seguridad
Incidencias	**Medio** *Debe registrarse la realización de procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y, en su caso, datos grabados manualmente.* *Debe autorizarse la ejecución de procedimientos de recuperación por el responsables del fichero*
Gestión de soportes	**Medio** *Debe mantenerse un Registro de Entrada de soportes: documento o soporte, fecha, emisor, número, tipo de información, forma de envío, responsable autorizado para recepción.* *Debe mantenerse un Registro de Salida de soportes: documento o soporte, fecha, destinatario, número, tipo de información, forma de envío, responsable autorizado para entrega.* **Alto** *Sistema de etiquetado de los soportes críptico (sólo comprensible y significativo para usuarios autorizados).* *Cifrado de datos en la distribución de soportes.* *Cifrado de dispositivos portátiles fuera de las instalaciones del responsable del fichero, o medidas alternativas incluidas en el Documento de seguridad.*
Control de acceso	**Medio** *Control de acceso físico a los locales donde se ubican los equipos físicos que dan soporte a los sistemas de información.* **Alto** *Debe mantenerse un Registro de accesos, que contenga: usuario que accede, hora, fichero accedido, tipo acceso, acceso autorizado/denegado y, en su caso, registro accedido.* *En caso que el responsable del fichero o del tratamiento sea una persona física y sea el único que accede y trata los datos personales, no es necesario el registro de accesos. Debe hacerse constar en el documento de seguridad.* *Control del Registro de accesos por el responsable de seguridad (no debe permitirse la desactivación ni manipulación de los controles)* *El responsable de seguridad debe elaborar un informe mensual sobre la información registrada y los problemas detectados.* *Conservación datos registrados: 2 años*

	Medidas de seguridad
Identificación y autenticación	**Básico** *Identificación inequívoca y personalizada de usuarios que intenten acceder a los SI y verificación de su autorización (intentos de acceso y accesos autorizados).* *Si la autenticación de usuarios se basa en contraseña:* *Procedimiento de asignación, distribución y almacenamiento debe garantizar la confidencialidad e integridad de las mismas.* *Deben caducar cada 365 días.* *Deben almacenarse de forma ininteligible mientras se hallen activas.* **Medio** *Debe establecerse un mecanismo que limite número de intentos reiterados de acceso no autorizado a los sistemas de información.*
Copias de respaldo	**Básico** *Copias de respaldo semanal (si existe actualización de datos).* *Deben fijarse procedimientos para la recuperación de datos que garanticen la reconstrucción de los datos en el estado en que se encontraban en el momento de producirse la pérdida o destrucción.* *En ficheros parcialmente automatizados (mixtos) si existe documentación que permite la reconstrucción se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.* *Debe verificarse la definición, funcionamiento y aplicación de los procedimientos de copias de respaldo y recuperación de datos, como mínimo cada 6 meses.* *Las pruebas con datos reales requieren la realización de una copia de respaldo previa y la aplicación del nivel de seguridad correspondiente al tipo de datos. Debe anotarse su realización en el documento de seguridad.* **Alto** *Copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos.*
Telecomunicaciones	**Básico** *El acceso a datos a través de redes de comunicaciones debe garantizar un nivel de seguridad equivalente al acceso en modo local.* **Medio** *La transmisión de datos a través de redes electrónicas, públicas o privadas, debe realizarse cifrando los datos, o mecanismo equivalente.*

Tabla 7 - Cuadro resumen de medidas de seguridad específicas de ficheros y/o tratamientos automatizados

6.6. Ficheros y Tratamientos no Automatizados

Aquellos ficheros o tratamientos que sean no automatizados o parcialmente automatizados, deberán aplicar, además de las medidas descritas en el punto anterior 6.4, las siguientes medidas de seguridad:

	Medidas de seguridad
Control de acceso	**Alto** *El acceso a la documentación se limitará exclusivamente al personal autorizado.* *Deben establecerse mecanismos que permitan identificar los accesos realizados en el caso de documentos accesibles por múltiples usuarios.* *Debe quedar adecuadamente registrado el acceso por usuarios no autorizados de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.*
Criterios de archivo	**Básico** *El archivo de los soportes o documentos debe realizarse de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deben 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.* *En aquellos casos en los que no existe norma aplicable, el responsable del fichero debe establecer los criterios y procedimientos de actuación que deben seguirse para el archivo.*
Almacenamiento	**Básico** *Los dispositivos de almacenamiento deben estar dotados de mecanismos que dificulten su apertura e impidan el acceso a personas no autorizadas. Cuando las características físicas de éstos no permitan adoptar esta medida, deben adoptarse medidas que impidan el acceso de personas no autorizadas* **Alto** *Armarios o archivadores de documentos deben encontrarse ubicados en áreas de acceso protegido mediante de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deben permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.* *Si, atendidas las características de los locales, no fuera posible disponer de áreas cerradas deben adoptarse medidas alternativas que deben constar en el documento de seguridad.*
Custodia de soportes	**Alto** *Durante la revisión o tramitación de los documentos, la persona a cargo de los mismos debe ser diligente y custodiarla para evitar accesos no autorizados.*
Copia o reproducción	**Alto** *Únicamente pueden realizarse bajo el control del personal autorizado en el documento de seguridad.*
Traslado de documentación	**Alto** *Deben adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.*

Tabla 8 - Cuadro resumen de medidas de seguridad específicas de ficheros y/o tratamientos no automatizados

7. Derechos ARCO

7.1. Consideraciones Generales

Los derechos ARCO son **personalísimos**, es decir, solo podrán ser ejercitados por el afectado, por el representante legal del interesado, o a través de representante voluntario expresamente designado para el ejercicio del derecho ARCO de que se trate. Con tal fin, deberá acreditarse la identidad y capacidad del solicitante. Por ello, si ejercita el derecho:

- el afectado, deberá acreditar su identidad mediante la aportación de la Fotocopia del D.N.I.,
- el representante legal, en supuestos de incapacidad o minoría de edad que imposibilite el ejercicio de estos derechos por parte del interesado, deberá acreditar la identidad del representado y su capacidad representativa
- el representante voluntario, expresamente designado para el ejercicio del derecho ARCO de que se trate, deberá acreditar la identidad del representado y su capacidad representativa.

Son derechos **independientes**, de forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

Por ejemplo, es inadmisible entender que para ejercitar el derecho de rectificación, el interesado debe ejercitar previamente el derecho de acceso.

- ***Requisitos y Procedimiento***

Los derechos ARCO se ejercerán mediante petición o solicitud dirigida al responsable del fichero, formulada por cualquier medio que garantice la identificación del afectado.

El afectado deberá poder ejercitar los derechos ARCO a través de un medio sencillo y gratuito, y que permita acreditar el envío y la recepción de la solicitud.

En este sentido, se consideran no conformes a la ley, y por tanto no legítimos, los siguientes medios:

- El envío de cartas certificadas o semejantes,
- La utilización de servicios de telecomunicaciones de tarificación adicional
- Cualesquiera otros medios que impliquen un coste excesivo

La **solicitud** o comunicación dirigida al responsable del fichero **deberá contener** las siguientes previsiones:

- Nombre y apellidos del interesado,
- Fotocopia del D.N.I. del interesado y, en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación,
- Petición en que se concreta la solicitud (acceso, rectificación, cancelación, oposición),
- Dirección a efectos de notificaciones, fecha y firma del solicitante,
- Documentos acreditativos de la petición que formula, en su caso.

Corresponde al responsable del fichero la prueba del cumplimiento del **deber de respuesta**. En atención a dicho deber de respuesta, el responsable del fichero deberá:

- Proceder a la contestación figuren o no datos de carácter personal del afectado,
- Solicitar la subsanación de los errores en la solicitud, en caso de que las hubiere,
- Cumplir con los requisitos formales y temporales para cumplir con el deber de respuesta,
- Garantizar que las personas con acceso a datos dentro de su organización puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

Conviene tener presente que **la ausencia de datos del afectado en los sistemas de información, no exime del deber de contestación**, de modo que, igualmente deberá procederse a facilitar una respuesta al interesado.

En el supuesto de no contestar dentro de los plazos establecidos, o hacerlo de forma incompleta, el sujeto afectado tiene derecho a acudir a la Agencia Española de Protección de Datos, o Autoridad de Control autonómica competente, donde si acredita mínimamente dichas circunstancias, se abrirá por parte de la misma expediente sancionador pudiendo derivar el mismo en la imposición de una sanción.

Para que la AEPD pueda iniciar el **procedimiento de tutela de derechos**, resulta necesario que haya transcurrido un mes, respecto del derecho de acceso, o diez días, en relación al resto de derechos, desde la presentación de la solicitud por la que se ejercita el derecho ARCO de que se trate, sin que se haya producido contestación alguna, y que se aporte, junto con el escrito que en su caso haya realizado el responsable del fichero, alguno de los siguientes documentos:

- La negativa del responsable del fichero a facilitar la información solicitada; o bien cancelar o rectificar los datos conforme a la solicitud presentada.
- Copia sellada por el responsable del fichero del modelo de petición de derechos ARCO.
- Copia del resguardo del envío por correo certificado o de la copia de la solicitud con el sello de la oficina de correos.
- Cualesquiera otros medios de prueba facilitados por el responsable del fichero y de los que se pueda deducir la recepción de la solicitud

A continuación se analizan cada uno de los derechos ARCO, teniendo en cuenta los siguientes aspectos:

- ¿Cuál es el contenido del derecho?
- ¿Cómo se ejerce el derecho?
- ¿Cómo se atiende o responde al derecho?
- ¿Cuándo puede denegarse el derecho?

7.2. Derecho de Acceso

Es el derecho del afectado a obtener información sobre si sus propios datos están siendo objeto de tratamiento o incluidos en un fichero, la finalidad del tratamiento que se esté realizando, el origen de dichos datos y las comunicaciones realizadas o que se prevean realizar respecto de los mismos.

- ***Ejercicio del derecho***

El afectado podrá optar por uno o varios de los siguientes sistemas de consulta del fichero para recibir la información solicitada:

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

- ***Respuesta a la solicitud de acceso***

Una vez recibida la solicitud, el responsable del fichero resolverá la petición de acceso en un **plazo máximo de un mes** a contar desde la recepción de la solicitud. El cómputo del plazo anterior se realizará de fecha a fecha (p.ej. si la fecha de recepción de la solicitud de acceso fuese el 5 de marzo, se dispondría hasta el 5 de abril para contestar al interesado).

Transcurrido dicho plazo sin que de forma expresa se responda a la petición de acceso, se entenderá que ésta ha sido desestimada a los efectos de la interposición de la correspondiente reclamación ante la AEPD, regulada en el artículo 18 de la LOPD.

Si la solicitud fuera estimatoria, el responsable del fichero deberá hacer efectivo el acceso en un plazo no superior a los diez días hábiles siguientes a la notificación de la misma al interesado.

El derecho de acceso no podrá llevarse a cabo en intervalos inferiores a doce meses, salvo interés legítimo debidamente justificado.

- ***Denegación del acceso***

El responsable del fichero podrá denegar el derecho de acceso en los siguientes supuestos:

- Cuando ya se haya ejercitado en los doce meses anteriores a la solicitud actual.
- Cuando la solicitud sea formulada por persona distinta del afectado sin capacidad de representación suficiente.

- Cuando así lo prevea una ley o norma de derecho comunitario.

- ***Modelo***

DATOS DEL RESPONSABLE DEL FICHERO

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

DATOS DEL INTERESADO O REPRESENTANTE LEGAL

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., del que acompaña copia, por medio del presente escrito ejerce el derecho de acceso, de conformidad con lo previsto en el artículo 15 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en los artículos 12 y 13 del Real Decreto 1332/94, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, vigentes al amparo de la disposición transitoria tercera de la citada Ley Orgánica 15/1999, y en la Norma Segunda de la Instrucción 1/1998, de 19 de enero, relativa al ejercicio de los derechos de acceso, rectificación y cancelación, y en consecuencia,

SOLICITA,

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

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

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

Firmado:

7.3. Derecho de Rectificación

Se entiende por derecho de rectificación, el derecho del afectado a que se modifiquen aquellos datos que resulten ser inexactos o incompletos, con el fin de que los datos personales respondan con veracidad a la situación actual del afectado.

- ***Ejercicio del derecho***

El afectado podrá ejercitar el derecho de rectificación ante el responsable del fichero, remitiendo la correspondiente solicitud cuyo contenido mínimo debe ser:

- En relación a la solicitud de rectificación:
  - Los datos en los que se concreta la solicitud,
  - La corrección que haya de realizarse,
- La documentación justificativa de lo solicitado (acredite el carácter inexacto o incompleto de los datos que figuran en los ficheros).

- ***Respuesta a la solicitud***

Una vez recibida la solicitud, el responsable del fichero resolverá la petición de rectificación, en un **plazo máximo de diez días hábiles**, a contar desde la recepción de la solicitud.

Transcurrido dicho plazo sin que de forma expresa se responda a la petición de rectificación o cancelación, ésta podrá entenderse desestimada a los efectos de la interposición de la reclamación ante la AEPD, regulada en el artículo 18 de la LOPD.

En el supuesto de que el responsable del fichero, hubiera previamente procedido a la cesión de los datos del afectado, deberá comunicar la rectificación al Cesionario en idéntico plazo. De esta manera, el cesionario deberá rectificar o cancelar los datos en el plazo de diez días desde la recepción de la comunicación. La rectificación del Cesionario no requiere comunicación al interesado.

- ***Denegación de la rectificación***

El responsable del fichero podrá denegar la rectificación de los datos en los siguientes supuestos:

- Cuando así lo prevea una ley o norma de derecho comunitario de aplicación directa,
- Cuando dichas normas impidan revelar a los afectados el tratamiento de los datos.

- ***Modelo***

DATOS DEL RESPONSABLE DEL FICHERO

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

DATOS DEL AFECTADO O REPRESENTANTE LEGAL

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., del que acompaña copia, por medio del presente escrito ejerce el derecho de rectificación sobre los datos anexos, aportando los correspondientes justificantes, de conformidad con lo previsto en el artículo 16 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en el artículo 15 del Real Decreto 1332/94, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, vigentes al amparo de la disposición transitoria tercera de la citada Ley Orgánica 15/1999, y en la Norma Tercera de la Instrucción 1/1998, de 19 de enero, relativa al ejercicio de los derechos de acceso, rectificación y cancelación, y en consecuencia,

SOLICITA,

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

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

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

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

Firmado:

7.4. Derecho de Cancelación

Se entiende por derecho de cancelación, el derecho del afectado a que se supriman los datos que resulten inadecuados o excesivos, en relación a la finalidad para la que fueron recabados; sin perjuicio del deber de bloqueo.

La cancelación de los datos siempre dará lugar al bloqueo de los mismos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido dicho plazo deberá procederse a la supresión de los datos.

El dato será bloqueado, es decir, será identificado y reservado con el fin de impedir su tratamiento.

- ***Ejercicio del derecho***

El afectado podrá ejercitar el derecho de cancelación ante el responsable del fichero, remitiendo la correspondiente solicitud cuyo contenido mínimo debe ser:

- Respecto de la solicitud de cancelación:
    - Los datos en los que se concrete la solicitud,
- La documentación justificativa de lo solicitado.

- ***Respuesta a la solicitud***

Una vez recibida la solicitud, el responsable del fichero resolverá la petición de cancelación, en un **plazo máximo de diez días hábiles**, a contar desde la recepción de la solicitud.

Transcurrido dicho plazo sin que de forma expresa se responda a la petición de rectificación o cancelación, ésta podrá entenderse desestimada a los efectos de la interposición de la reclamación ante la AEPD, regulada en el artículo 18 de la LOPD.

En el supuesto de que el responsable del fichero, hubiera previamente procedido a la cesión de los datos del afectado, deberá comunicar la cancelación al Cesionario en idéntico plazo. De esta manera, el cesionario deberá cancelar los datos en el plazo de diez días desde la recepción de la comunicación. La cancelación del Cesionario no requiere comunicación al interesado.

- ***Denegación de la cancelación***

El responsable del fichero podrá denegar la rectificación de los datos en los siguientes supuestos:

- Cuando así lo prevea una ley o norma de derecho comunitario de aplicación directa,
- Cuando dichas normas impidan revelar a los afectados el tratamiento de los datos.

- ***Modelo***

DATOS DEL RESPONSABLE DEL FICHERO

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

DATOS DEL AFECTADO O REPRESENTANTE LEGAL

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., del que acompaña copia, por medio del presente escrito ejerce el derecho de cancelación, de conformidad con lo previsto en el artículo 16 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en los artículos 15 y 16 del Real Decreto 1332/94, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, vigentes al amparo de la disposición transitoria tercera de la citada Ley Orgánica 15/1999, y en la Norma Tercera de la Instrucción 1/1998, de 19 de enero, relativa al ejercicio de los derechos de acceso, rectificación y cancelación, y en consecuencia,

SOLICITA,

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

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

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

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

Firmado:

7.5. Derecho de Oposición

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

- Cuando no sea necesario su consentimiento.
- Cuando el tratamiento tenga por finalidad la realización de actividades de publicidad y prospección comercial.
- Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos.

• *Ejercicio del derecho*

El afectado podrá ejercitar el derecho de oposición ante el responsable del fichero, remitiendo la correspondiente solicitud, que deberá cumplir las formalidades descritas al regular los "Requisitos y procedimientos" en el apartado de "Cuestiones generales".

• *Respuesta a la solicitud*

Una vez recibida la petición, el responsable del fichero resolverá sobre la solicitud de oposición en el **plazo máximo de diez días hábiles** a contar desde la recepción de la solicitud.

Transcurrido dicho plazo sin que de forma expresa se responda a la petición de oposición, ésta podrá entenderse desestimada a los efectos de la interposición de la reclamación ante la AEPD, en los términos previstos por el artículo 18 de la LOPD.

La ausencia de datos del afectado en los sistemas de información, no exime del deber de contestación, de modo que, igualmente deberá procederse a facilitar una respuesta al interesado en los términos indicados anteriormente.

Si la resolución fuera estimatoria, el derecho de oposición se hará efectivo en el plazo de los diez días siguientes a la notificación de aquélla.

• *Denegación*

En el supuesto de que una Ley disponga la necesidad del tratamiento de los datos de carácter personal del interesado, el responsable del fichero podrá denegar la solicitud del afectado, pudiendo éste hacer uso de la reclamación prevista en el artículo, 18.1 de la Ley Orgánica 15/1999.

También se podrá denegar en los casos en los que el interesado no proporcione información suficiente para poder valorar que existen motivos fundados y legítimos relativos a una concreta situación personal.

- ***Modelo***

DATOS DEL RESPONSABLE DEL FICHERO

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

DATOS DEL INTERESADO O REPRESENTANTE LEGAL

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

EXPONGO,

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

Para acreditar la situación descrita, acompaño una copia de los siguientes documentos:

(enumerar los documentos que adjunta con esta solicitud para acreditar la situación que ha descrito)

SOLICITO,

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

En .....a.....de.....de 20.....
Firmado:

7.6. Cuadro Resumen

<table>
<tr><th>DERECHOS</th><th>Rectificación</th><th>Cancelación</th><th>Oposición</th><th>Acceso</th></tr>
<tr><td>Contenido</td><td>Derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos</td><td>Derecho a que se supriman los datos que resulten ser inadecuados o excesivos.</td><td rowspan="2">Derecho a que no se lleve a cabo el tratamiento de sus datos de carácter personal en los siguientes supuestos:
- Cuando no sea necesario su consentimiento
- Cuando el tratamiento tenga por finalidad realización de actividades de publicidad y prospección comercial
- Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos</td><td>Es el derecho del afectado a obtener información sobre si sus propios datos están siendo objeto de tratamiento o incluidos en un fichero, la finalidad del tratamiento que se esté realizando, el origen de dichos datos y las comunicaciones realizadas o que se prevean realizar respecto de los mismos.</td></tr>
<tr><td>Peculiaridades</td><td colspan="2">Rectificación y/o Cancelación → Supuesto de cesión de datos → RF debe comunicar la rectificación al cesionario en el plazo de 10 días, quien deberá rectificar en idéntico plazo (no requiere comunicación al interesado).

Cancelación → da lugar al BLOQUEO de los datos:
• Conservación a disposición únicamente de las Administraciones Públicas, Jueces y Tribunales.
• Para la atención de las posibles responsabilidades nacidas del tratamiento (durante el plazo de prescripción de éstas)
• Cumplido el plazo → Supresión.</td><td>Si la solicitud resulta estimatoria deberá concederse el acceso en el plazo de 10 DÍAS HÁBILES siguientes a la notificación de la respuesta.

El derecho de acceso no podrá llevarse a cabo en intervalos inferiores a 12 meses, salvo interés legítimo debidamente justificado.</td></tr>
<tr><td>Plazo de respuesta</td><td colspan="3">10 DÍAS HÁBILES DESDE LA RECEPCIÓN DE LA SOLICITUD</td><td>30 DÍAS NATURALES DESDE LA RECEPCIÓN DE LA SOLICITUD</td></tr>
<tr><td>Tutela</td><td colspan="4">Si Denegación del derecho o Silencio (el responsable del fichero no contesta en plazo), cabe demandar la tutela de la AEPD o Autoridad de Control autonómica competente.</td></tr>
</table>

8. Auditoría

8.1. Ámbito de aplicación

La finalidad de la auditoria exigida por el RLOPD tiene por objeto o finalidad, el verificar el cumplimiento de las disposiciones del RLOPD en los sistemas de información e instalaciones de tratamientos y almacenamiento de datos en la Organización.

- ***Subjetivo***

Deben desarrollar la auditoría tanto los responsables del fichero o tratamiento como los encargados del tratamiento.

- ***Objetivo***

Son objeto de auditoría los sistemas de información e instalaciones de tratamiento y almacenamiento de datos clasificados con nivel de seguridad medio y alto.

Son datos clasificados con nivel medio o alto de seguridad:

- La comisión de infracciones administrativas o penales.
- Ficheros y/o tratamientos de datos que contengan un conjunto de datos de carácter personal suficiente como para tener una evaluación de la personalidad del individuo.
- Datos relativos a la ideología, religión , creencias y afiliación sindical
- Datos relativos a la Origen racial, salud y vida sexual
- Datos recabados para fines policiales sin consentimiento de las personas afectadas
- Datos derivados de actos de violencia de género
- Ficheros de la Administración tributaria cuya finalidad está relacionada con el ejercicio de potestades tributarias
- Ficheros de entidades financieras cuya finalidad es la prestación de servicios financieros
- Datos de tráfico y localización de los que sean responsables que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas
- Ficheros sobre solvencia patrimonial y crédito
- Ficheros de los que sean responsables Entidades Gestoras y Servicios Comunes de la Seguridad Social, cuando se relacionen con el ejercicio de sus competencias.
- Ficheros de los que sean responsables Mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social, cuando se relacionen con el ejercicio de sus competencias.

8.2. Contenido

La auditoría regulada por los artículos 96 y 110 del Reglamento de desarrollo de la LOPD implica que debe comprobarse la adecuación de las medidas, los procedimientos y los controles de seguridad establecidos por el responsable del fichero y/o encargado de tratamiento en su organización, a lo dispuesto por el RLOPD e las instrucciones vigentes en la materia.

Por tanto, se verifica:

- La adecuación de los procedimientos implantados
- La adecuación de los controles existentes
- La adecuación de las medidas de seguridad

La verificación de la adecuación de los extremos anteriores depende el nivel de seguridad y del sistema de tratamiento utilizado en la Organización.

8.3. Tipos de Auditoría

A partir del nivel medio de seguridad, los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán […] a una auditoría interna o externa que verifique el cumplimiento del Título VIII del Reglamento de desarrollo de la LOPD.

Por tanto, **en función de quién realice la auditoría**, ésta será:

- Interna
- Externa

La legislación vigente, NO recoge ninguna exigencia ni homologación específica para desarrollar la labor de auditor en materia de protección de datos. No obstante, es recomendable, tanto si se desarrolla por personal interno como externo, que los auditores sean personal profesionalmente cualificado e independiente del responsable o, en su caso, del encargado de tratamiento y que actúe conforme a criterios de **independencia, imparcialidad y objetividad**.

Por otro lado, la auditoría también puede clasificarse: en **ordinaria y extraordinaria**, en función de si la misma se desarrolla por el transcurso del plazo establecido por el RLOPD o porqué se produce una modificación sustancial en los sistemas de información.

En este sentido, el RLOPD establece que "*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* […]" y "*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. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior".

Por tanto, hablaremos de auditoría:

- **Ordinaria**
  - Tiene carácter bienal, de forma que debe desarrollarse cada dos años como mínimo en ficheros y/o tratamientos con nivel de seguridad medio o alto
  - Implica la verificación de los sistemas de información e instalaciones de tratamiento y almacenamiento de datos
  - El cómputo se inicia con la inscripción de los ficheros o el inicio del tratamiento
- **Extraordinaria**
  - Debe realizarse siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento del principio de seguridad, es decir, que afecte a los procedimientos, controles o medidas de seguridad implantados
  - Implica la verificación de la adaptación, adecuación y eficacia de las medidas de seguridad implantadas
  - Inicia el cómputo de dos años

8.4. Informe de Auditoría

El informe de auditoría que se emita por el auditor, interno o externo, debe como mínimo:

- Dictaminar sobre la adecuación de las medidas y controles a la LOPD y al RLOPD
- Identificar sus deficiencias
- Proponer las medidas correctoras o complementarias necesarias.
- Incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

- **Identificación de deficiencias**

El auditor debe identificar con el mayor detalle posible las incidencias detectadas durante la auditoría, permitiendo así un mejor reconocimiento de su existencia por parte de la organización.

Dichas incidencias deben referirse tanto al tratamiento automatizado como no automatizado, ya sean de carácter técnico u organizativo.

- **Propuesta de medidas correctoras**

El auditor debe proponer las medidas correctoras y/o complementarias que la Organización debe implementar en aras a cumplir con las prescripciones del RLOPD.

A través de estas medidas se pretende subsanar las deficiencias y defectos de seguridad detectados, y completar aquellas medidas de seguridad que se consideran insuficientes para garantizar la seguridad de los datos.

Por ejemplo, son medidas correctoras o complementarias, el desarrollo de planes de formación a los usuarios, la determinación y establecimiento de ubicaciones alternativas a las copias de seguridad o la adopción de técnicas de cifrado en el transporte o transmisión de la información a través de redes de comunicaciones.

- **Enumeración y descripción**

El auditor debe exponer en el informe resultante la enumeración y descripción de todos los datos, hechos y observaciones en que fundamente sus valoraciones y recomendaciones:

- **Datos**

Se entiende por "*datos*", todos aquellos antecedentes necesarios para llegar al conocimiento exacto de las cuestiones que el auditor debe conocer para deducir y fundamentar las manifestaciones que realiza en el informe de auditoría.

Ejemplo: Indicación de la concreta documentación obtenida durante la realización de la auditoría, así como su contenido.

- **Hechos**

Se entiende por "*hechos*", todas aquellas circunstancias o acciones que han acontecido en la organización de la entidad auditada y que originan una situación que puede generar una obligación legal en materia de seguridad y, por tanto, que deben ser observadas por el auditor.

Ejemplo: Indicación de las pruebas efectuadas para comprobar la implantación y efectividad de las medidas definidas, en su caso, en el documento de seguridad.

- **Observaciones**

Las observaciones son aquellas valoraciones subjetivas del propio auditor, que nacen del examen atento que éste realiza de todo aquello a que tiene acceso respecto a la organización de la entidad auditada.

Ejemplo: Efectividad o deficiencia, así como su grado, de la medidas analizada (existe política de identificación y autenticación pero la contraseña no caduca).

- **Dictamen**

El auditor se pronunciará sobre el grado de adecuación de las medidas y controles a la normativa sobre protección de datos (conformidad / no conformidad), así como sobre el resultado global de la auditoría (apto / no apto).

El informe de auditoria será analizado por el Responsable de Seguridad, quien lo elevará al Responsable del fichero para que adopte las medidas pertinentes. Dicho informe deberá conservarse a disposición de la Autoridad de Control competente durante los plazos legalmente establecidos.

9. Autoridades de Control

9.1. Agencia Española de Protección de Datos

La Agencia Española de Protección de Datos (en lo sucesivo, AEPD) es un ente de derecho público, con **personalidad jurídica propia y plena capacidad pública y privada**, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones.

El artículo 37 de la LOPD determina que son **funciones** de la Agencia Española de Protección de Datos:

a) **Velar por el cumplimiento de la legislación sobre protección de datos** y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.

c) Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley.

d) **Atender las peticiones y reclamaciones formuladas por las personas afectadas**.

e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.

f) Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.

g) **Ejercer la potestad sancionadora** en los términos previstos por el Título VII de la Ley.

h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.

i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.

k) Redactar una memoria anual y remitirla al Ministerio de Justicia.

l) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

m) Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46 de la Ley.

n) Cuantas otras le sean atribuidas por normas legales o reglamentarias.

La página oficial o sede electrónica de esta entidad puede consultarse en el siguiente enlace:

https://www.agpd.es/portalwebAGPD/index-ides-idphp.php

9.2. Autoridades de Control Autonómicas

Las funciones de la Agencia Española de Protección de Datos reguladas en el artículo 37, a excepción de las mencionadas en los apartados j), k) y l), y en los apartados f) y g) en lo que se refiere a las transferencias internacionales de datos, así como en los artículos 46 y 49, en relación con sus específicas competencias serán ejercidas por las Autoridades de Control correspondientes de cada Comunidad, cuando dichas funciones afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial.

Además, las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros para el ejercicio de las competencias que se les reconoce sobre los mismos.

Existe un deber de colaboración de las Autoridades de Control autonómicas en relación a la AEPD, motivo por el que el Director de la Agencia Española de Protección de Datos puede convocarlas regularmente a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación. Asimismo, existe el deber de información mutua entre Autoridades de Control para el cumplimiento de las funciones que les son propias.

Las Autoridades de Control autonómicas que existen actualmente son:

- Agencia de Protección de Datos de la Comunidad de Madrid (en lo sucesivo, APDCM)
- Agencia Catalana de Protecció de Dades (en adelante, APDCAT)
- Agencia Vasca de Protección de Datos (en adelante, AVPD)

- ***APDCM***

La Agencia de Protección de Datos de la Comunidad de Madrid, de conformidad con la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, es competente en relación a los ficheros de titularidad pública creados o gestionados por:

- las Instituciones de la Comunidad de Madrid
- los Órganos, Organismos, Entidades de Derecho público y demás Entes públicos integrantes de la Administración Pública de la Comunidad de Madrid, exceptuándose las sociedades mercantiles a que se refiere el artículo 2.2.c).1 de la Ley 1/1984, de 19 de enero, reguladora de la Administración Institucional de la Comunidad de Madrid.
- los Entes que integran la Administración Local del ámbito territorial de la Comunidad de Madrid
- las Universidades públicas de la Comunidad de Madrid
- las Corporaciones de derecho público representativas de intereses económicos y profesionales de la Comunidad de Madrid, en este último caso siempre y cuando dichos ficheros sean creados o gestionados para el ejercicio de potestades de derecho público.
- las entidades y empresas de la Comunidad de Madrid y Entidades Locales, en relación a ficheros regulados por la Ley estatal 12/1989, de 9 de mayo, de la Función Estadística Pública, para fines no estatales.

La página oficial o sede electrónica de esta entidad puede consultarse en el siguiente enlace: http://www.madrid.org/cs/Satellite?pagename=PortalAPDCM/Page/PAPD_home

- ***APDCAT***

La *Agéncia Catalana de Protecció de Dades* es, de conformidad con la Ley 5/2002, de 19 de abril, de la *Agència Catalana de Protecció de Dades* y el Decreto 48/2003, de 20 de febrero, por el que se aprueba el Estatuto de la *Agència Catalana de Protecció de Dades*, competente en relación a los ficheros creados o gestionados por:

- los órganos, organismos y las entidades vinculadas o dependientes de les instituciones públicas de Cataluña, de la Administración de la Generalitat, de los entes locales de Cataluña, de las Universidades de Cataluña y de les Corporaciones de Derecho público que ejerzan sus funciones exclusivamente en Cataluña.
- Las personas físicas o jurídicas que, de conformidad con cualquier convenio, contrato o disposición normativa, gestionen servicios públicos o ejerzan funciones públicas, siempre que en este último caso el tratamiento se realice en Cataluña y sea en relación a materia de la competencia de la Generalitat de Cataluña o de los entes locales de Cataluña.

La página oficial o sede electrónica de esta entidad puede consultarse en el siguiente enlace: www.apdcat.net

- ***AVPD***

Datuak Babesteko Euskal Bulegoa
Agencia Vasca de Protección de Datos

La Agencia Vasca de Protección de Datos, de conformidad con la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos, tiene competencia respecto de los ficheros creados o gestionados por:

- la Administración General de la Comunidad Autónoma, los órganos forales de los territorios históricos y las administraciones locales del ámbito territorial de la Comunidad Autónoma del País Vasco, así como los entes públicos de cualquier tipo, dependientes o vinculados a las respectivas administraciones públicas, en tanto que los mismos hayan sido creados para el ejercicio de potestades de derecho público.
- El Parlamento Vasco.
- El Tribunal Vasco de Cuentas Públicas.
- El Ararteko.
- El Consejo de Relaciones Laborales.
- El Consejo Económico y Social.
- El Consejo Superior de Cooperativas.
- La Agencia Vasca de Protección de Datos.
- La Comisión Arbitral.
- Las corporaciones de derecho público, representativas de intereses económicos y profesionales, de la Comunidad Autónoma del País Vasco.
- Cualesquiera otros organismos o instituciones, con o sin personalidad jurídica, creados por ley del Parlamento Vasco, salvo que ésta disponga lo contrario.

La página oficial o sede electrónica de esta entidad puede consultarse en el siguiente enlace: www.avpd.euskadi.net/

9.3. Infracciones de las Administraciones Públicas

Cuando los sujetos presuntamente responsables sean las Administraciones públicas resulta de aplicación el régimen específico previsto por el artículo 46 de la LOPD.

Dicho artículo establece que en estos casos, el Director de la AEPD dictará resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Dicha resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente, a los afectados si los hubiera y, en su caso, al Defensor del Pueblo.

Asimismo, el Director AEPD puede proponer la iniciación de **actuaciones disciplinarias**.

El responsable del fichero deberá comunicar a la AEPD las medidas y actuaciones que se realicen en el sentido indicado en los párrafos anteriores.

10. Tratamientos específicos

10.1. Transferencia Internacional de Datos

La transferencia o movimiento internacional de datos es objeto de regulación específica por parte de la AEPD a través de la Instrucción 1/2000, de 1 de diciembre, de la AEPD, relativa a las normas por las que se rigen los movimientos internacionales de datos . Esta instrucción fue modificada como consecuencia de la Sentencia de la Audiencia Nacional, de 15 de marzo de 2002.

Antes de analizar el régimen aplicable a las transferencias internacionales de datos, conviene precisar qué se entiende por transferencia internacional y qué sujetos intervienen en la misma.

En este sentido, es **transferencia internacional**, *toda transmisión de los mismos fuera del territorio español. En particular, se consideran como tales las que constituyan una cesión o comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero*.

Los sujetos intervinientes son, por un lado, el **transmitente o exportador**, que es *el responsable del fichero o tratamiento de los datos de carácter personal que son objeto de transferencia internacional; y, por otro lado, el* **destinatario o importador**, que es *el tercero situado fuera del territorio español que recibe los datos transferidos*.

- ***Régimen Aplicable***

La transferencia internacional de datos (en lo sucesivo, TID) se regula en los artículos 33 y 34 de la LOPD, prohibiéndose la realización de TID con destino a países que no proporcionen un nivel de protección equiparable al de la LOPD.

En este sentido, el artículo 33.1 de la LOPD dispone que "*no podrán realizarse transferencias internacionales temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley*, ***salvo que***, *además de haberse observado lo dispuesto en ésta,* ***se obtenga autorización previa del Director de la AEPD****, que sólo podrá otorgarla si se obtienen las* ***garantías adecuadas***."

El apartado 2 del artículo 33 de la LOPD, determina los criterios que la AEPD evalúa para determinar el carácter adecuado del nivel de protección que ofrece el país de destino, dónde se ubica el exportador o destinatario.

En particular, se tomará en consideración:

- La naturaleza de los datos
- La finalidad y la duración del tratamiento o de los tratamientos previstos,
- El país de origen y el país de destino final,
- Las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate,
- El contenido de los informes de la Comisión de la Unión Europea
- Las normas profesionales y medidas de seguridad en vigor en dichos países.

A la regla general indicada anteriormente le son de aplicación las **excepciones** previstas en el artículo 34 de la LOPD. Dicho artículo establece que no será necesaria la autorización del Director de la AEPD para realizar transferencias internacionales de datos, siempre y cuando la misma:

a) Resulte de la aplicación de tratados o convenios en los que es parte España.
b) Se realice a efectos de prestar o solicitar auxilio judicial internacional.
c) Sea necesaria para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios.
d) Se refiera a transferencias dinerarias conforme a su legislación específica.
e) Haya sido consentida, de forma inequívoca, por el afectado.
f) 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.
g) 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.
h) Sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.
i) Sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
j) Se efectúe, a petición de persona con interés legítimo, desde un Registro Público y aquélla sea acorde con la finalidad del mismo.
k) 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 (publicación B.O.E).

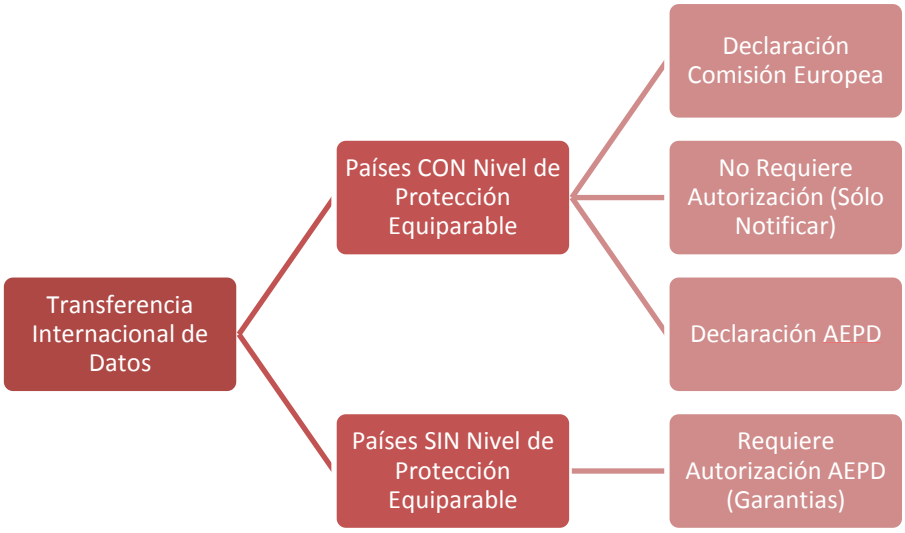


Ilustración 2 – Régimen aplicable a la Transferencia Internacional de Datos.

- ***Tipos de Transferencias Internacionales***

Las transferencias internacionales de datos pueden clasificarse, en atención al régimen descrito en el punto anterior, en:

- Transferencia a Estados con nivel de protección adecuado
- Transferencia conforme al artículo 34 de la LOPD
- Transferencia a Estados sin nivel de protección adecuado

A continuación se analizan los requisitos y/o peculiaridades aplicables a los distintos tipos de transferencia internacional.

- **Transferencia a Estados con Nivel de Protección Adecuado**

Se regula en el Capítulo II del Título VI del RLOPD.

Implica que **no sea precisa la autorización del Director** de la AEPD para realizar la transferencia internacional de datos, siempre y cuando las normas del Estado destinatario aporten un nivel de protección equiparable al de la LOPD.

La adecuación se establece a través de **Resolución del Director de la AEPD o por Decisión de la Comisión Europea**, en atención a la concurrencia de las condiciones de evaluación de la adecuación reguladas por el artículo 33.2 de la LOPD.

En relación con este tipo de transferencia, si bien es cierto que no es necesaria la autorización del Director de la AEPD para proceder a la misma, el Director de la AEPD dispone de la facultad de **suspender temporalmente** la transferencia internacional de datos, previa audiencia del Exportador, ante la concurrencia de alguna de las siguientes circunstancias:

- Las autoridades de Protección de Datos del Estado destinatario determinen que el Importador ha vulnerado las normas de protección de datos de derecho interno.
- Que existan indicios racionales de que se estén vulnerando las normas o principios de protección de datos por el Importador y las autoridades competentes del Estado destinatario no hayan adoptado o vayan a adoptar en el futuro las medidas oportunas para resolverlo.

Los Estados que actualmente disponen de un nivel de protección adecuado son:

- Alemania
- Argentina
- Austria
- Bélgica
- Bulgaria
- Chipre
- Dinamarca
- Eslovaquia
- Eslovenia
- Estonia
- Finlandia
- Francia
- Grecia
- Guernsey
- Hungría
- Irlanda
- Italia
- Isla de Man
- Islandia
- Letonia
- Liechtenstein
- Lituania
- Luxemburgo
- Malta
- Noruega
- Países Bajos
- Polonia
- Portugal
- Reino Unido
- República Checa
- Rumanía
- Suecia
- Suiza

- Entidades estadounidenses adheridas a los “principios de puerto seguro”
- Entidades canadienses sujetas al ámbito de aplicación de la ley canadiense de protección de datos.

- **Transferencia conforme al Artículo 34 de la LOPD**

Si alguna de las excepciones previstas por el artículo 34 de la LOPD resulta aplicable a la transferencia internacional de datos, tampoco será precisa la autorización del Director de la AEPD.

En este caso, el Responsable del fichero o tratamiento deberá acreditar la concurrencia de las excepciones alegadas para realizar la transferencia internacional de datos sin recabar la autorización del Director de la AEPD, a petición de la AEPD.

Por ejemplo: si se alega la concurrencia del consentimiento de los interesados, deberá acreditarse la obtención y la naturaleza inequívoca del mismo (artículos 5 y 6 de la LOPD).

- **Transferencia a Estados sin Nivel de Protección Adecuado**

Se regula en el Capítulo III del Título VI del RLOPD.

Implica que cuando la transferencia internacional tenga por destino un Estado respecto del que **no se ha declarado la equiparación**, y siempre que el Exportador no se funde en alguna de los supuestos del artículo 34 de la LOPD, deberá requerirse la autorización del Director de la AEPD.

Dicha autorización podrá ser otorgada:

- En caso de que el Exportador aporte un **contrato por escrito con 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.

  Se considera que establecen las adecuadas garantías los **contratos tipo aprobados por la Comisión Europea** a través de las siguientes normas comunitarias:

  - Decisión de la Comisión (2010/87/UE), de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo.
  - Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001, relativa a 'Cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE.
  - Decisión de la Comisión de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países.

- En el **seno de grupos multinacionales de empresas** cuando hubiesen sido adoptados por los mismos normas o reglas internas en que consten las necesarias garantías de respeto de a la protección de la vida privada y el derecho fundamental a la protección de los datos de los afectados y se garanticen los principios y ejercicio de derechos de la LOPD. Dichas normas o reglas deben ser vinculantes para las empresas del Grupo y exigibles conforme al ordenamiento jurídico español (**Reglas Corporativas Vinculantes**). Esta regulación se completa con los Documentos de Trabajo elaborados por el Grupo del Artículo 29 de la Directiva 95/46/CE relativos al contenido de las normas corporativas vinculantes, que pueden consultarse a través del siguiente enlace: http://ec.europa.eu/justice/policies/privacy/binding_rules/index_en.htm

También en relación con este tipo de transferencias, el Director de la AEPD dispone de la facultad de **suspender temporalmente o denegar** la transferencia internacional de datos, previa audiencia del Exportador, ante la concurrencia de 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.

- ***Procedimiento***

Para obtener la autorización al Director de la AEPD para realizar una transferencia internacional de datos, el exportador o responsable del fichero deberá remitir una **solicitud** en la que se identifiquen los siguientes **extremos**:

- La identificación del fichero o ficheros a cuyos datos se refiera la transferencia internacional, con indicación de su denominación y código de inscripción en el RGPD.
- La transferencia respecto de la que se solicita autorización, con indicación de la finalidad que la justifica.

Asimismo, deberá aportar la **documentación** que incorpore las garantías exigibles para la obtención de la autorización, así como la documentación que acredite el cumplimiento de los requisitos legales necesarios para la realización de la transferencia, en su caso.

Por ejemplo, deberá aportarse copia del contrato suscrito con el importador o destinatario y acreditar poder suficiente por parte de los firmantes.

Tras la recepción de la solicitud, la AEPD procederá a la apertura del período **información pública** mediante la publicación el BOE de la misma. Dentro de los 10 días siguientes a la misma podrán presentarse **alegaciones** por parte de los interesados.

En caso de existir alegaciones, se dará traslado de las mismas al solicitante para que en el plazo máximo de 10 días manifieste lo que estime conveniente a su derecho.

Transcurrido el plazo conferido, en su caso, al exportador, el Director de la AEPD dictará resolución acordando la concesión o denegación de la autorización solicitada.

En caso de concederse la autorización, el Director de la AEPD dará traslado de la misma al Registro General de Protección de Datos para su inscripción de oficio.

La AEPD dispone del plazo de **3 MESES** contados desde la fecha de entrada de la solicitud en la AEPD para resolver sobre la solicitud de autorización planteada; si transcurrido dicho plazo no existiese pronunciamiento expreso al respecto, se entenderá concedida ("*silencio administrativo positivo*").

En cualquier caso, sea necesaria o no la solicitud de autorización, el **exportador o responsable del fichero debe notificar las transferencias internacionales asociadas a los ficheros de los que es titular al Registro General de Protección de Datos para su inscripción**.

10.2. Videovigilancia

El tratamiento de imágenes con fines de vigilancia es objeto de regulación específica por parte de la AEPD a través de la *Instrucción 1/2006,* de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o ***videocámaras***

(cfr. 12.4).

- ***Ámbito de aplicación***

El régimen establecido por la Instrucción 1/2006 de la AEPD se aplica a los *tratamientos consistentes en la grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, siempre y cuando se utilicen para realizar estos tratamientos sistemas de cámaras o videocámaras, o por cualquier medio técnico análogo y, en general, por cualquier sistema que permita los tratamientos previstos en la misma*.

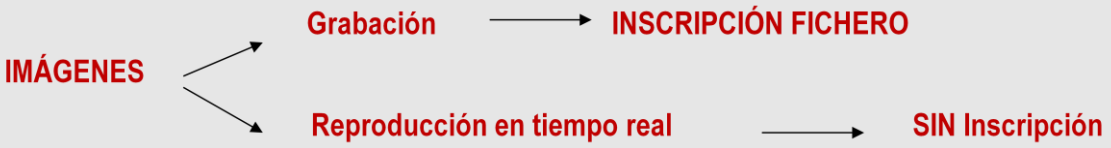
Por el contrario, se **excluye de su ámbito de aplicación** el tratamiento de imágenes obtenidas:

- Por las Fuerzas y Cuerpos de Seguridad.
- En el ámbito personal o doméstico (actividad exclusivamente privada o familiar).
- Por los medios de comunicación en el ejercicio legítimo de la libertad de expresión (artículo 20 CE).
-

- ***Inscripción del Fichero***

El Responsable del Fichero que prevea la creación de ficheros de videovigilancia debe notificarlo previamente (antes de iniciar el tratamiento) a la AEPD, para su inscripción en el RGPD.

La obligación de notificar el fichero de videovigilancia **no** es de aplicación en aquellos casos en que el tratamiento de datos consiste **exclusivamente** en la r**eproducción o emisión de imágenes en tiempo real**.



El **deber informativo subsiste** aunque no deba inscribirse el fichero de videovigilancia ante la Autoridad de Control competente.

- ***Cumplimiento de Principios***

  - **Principios Calidad, Proporcionalidad y Finalidad**

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

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

Las cámaras y videocámaras instaladas en espacios privados **no podrán obtener imágenes de espacios públicos salvo** que resulte **imprescindible para la finalidad** de vigilancia que se pretende, **o** resulte **imposible evitarlo** por razón de la **ubicación** de aquéllas.

Las imágenes deben **cancelarse** en el plazo máximo de **1 MES desde su captación** (bloqueo a disposición de las Administraciones públicas, Jueces y Tribunales).

  - **Deber de Información**

Los responsables del fichero o tratamiento que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de la LOPD. A tal fin deberán:

- Colocar, en las zonas videovigiladas, al menos un **distintivo informativo** ubicado en **lugar suficientemente visible**, tanto en espacios abiertos como cerrados (*en todos los accesos a las zonas vigiladas*),
- Tener **a disposición de los/las interesados/as impresos** en los que se detalle la información prevista en el artículo 5.1 de la LOPD (fichero, responsable y derechos ARCO).

  - **Legitimación para el Tratamiento**

Debido al régimen aplicable al consentimiento para el tratamiento (artículo 6 de la LOPD) y/o cesión (artículo 11 de la LOPD) de datos de carácter personal y la propia naturaleza del tratamiento de imágenes a través de dispositivos de videocámaras es necesario que una Ley autorice o habilite este tipo de tratamiento.

En este sentido, existen diversas normas que autorizan el tratamiento de imágenes con fines de vigilancia sin requerir del consentimiento de los interesados, por ejemplo la Ley 23/1992, de 30 de julio, de

Seguridad Privada, la cual determina que, siempre y cuando los aparatos, dispositivos y sistemas de seguridad estén conectados a centrales de alarma, deberá realizar la instalación o mantenimiento una empresa de seguridad debidamente inscrita en el Registro pertinente del Ministerio del Interior. Asimismo se exige la comunicación del contrato de prestación de servicios de seguridad debidamente formalizado al Ministerio del Interior.

Si por el contrario, dichos dispositivos y sistemas de seguridad no estuviesen conectados a centrales de alarma, podrá realizarse la instalación o mantenimiento cualquier empresa (no empresas de seguridad) o el propio particular.

En cualquier caso, independientemente de quién realice la instalación o mantenimiento, deberán cumplirse las normas establecidas en la legislación de protección de datos de carácter personal, entre las que se incluyen el deber de informar a los interesados, la inscripción de ficheros, y la implantación de las medidas de seguridad.

- **Prestaciones de Servicios**

Como ya se ha indicado anteriormente, la instalación y mantenimiento técnico de los equipos y sistemas de videovigilancia puede realizarse por Terceros prestadores de servicios.

En este sentido, en función del contenido del servicio, el responsable del fichero o tratamiento deberá formalizar un contrato u otro con el Tercero:

	Servicio	
	Sin acceso a las imágenes	**Utilización de los equipos o acceso a las imágenes**
Tercero	*Prestador sin acceso a datos*	*Encargado del Tratamiento*
Contrato	*Contrato de prestación de servicios sin acceso a datos*	*Contrato de acceso a datos*

• *Medidas de Seguridad*

El nivel de seguridad y las medidas aplicables al tratamiento dependen de la finalidad del mismo.

Nivel de seguridad	Finalidad
Básico	▪ Vigilancia o control de acceso a las instalaciones del responsable ▪ Vigilancia o control empresarial de los trabajadores
Medio	▪ Selección de personal
Alto	▪ Verificar la respuesta a determinados estímulos (psicología o medicina) ▪ Investigación y persecución de un delito

- ***Ejercicio Derechos ARCO***

Debido a la especialidad de este tipo de ficheros, el ejercicio de los derechos ARCO por parte de los interesados implica que éste deba facilitar una foto actualizada al responsable del fichero.

La concesión del derecho de acceso implicará la emisión de una certificación por parte del responsable del fichero en la que se indicará al interesado el contexto y contenido de la grabación. En ningún caso se aportará copia de la grabación ya que ello implicaría la colisión con derechos de terceros.

Por otro lado, el derecho de oposición y rectificación son de contenido imposible debido a la propia definición de su contenido (por ejemplo, la imagen no puede ser inexacta o incompleta). Por el contrario, el ejercicio del derecho de cancelación si es posible e implicará que el responsable del fichero proceda al bloqueo de las imágenes del interesado.

10.3. Padrón Municipal de Habitantes

- ***Legitimación del Tratamiento***

Tal y como dispone el artículo 15 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local (en adelante, LBRL), toda persona que viva en España está obligada a inscribirse en el padrón del municipio en el que resida habitualmente.

En este sentido, los ayuntamientos se ven afectados por la creación y uso de un fichero que contiene datos de carácter personal, correspondientes a todos los vecinos del municipio.

Sin embargo, dicho tratamiento no requiere de la obtención del consentimiento de los interesados, por encontrarse amparado por una de las excepciones recogidas en el artículo 6.2 de la LOPD:

"No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias […]."

- ***Cesión de Datos del Padrón Municipal a otras Administraciones Públicas***

La comunicación de datos contenidos en el fichero del Padrón Municipal a otros organismos públicos, como por ejemplo a Servicios Sociales o Entidades Locales Menores, constituye una cesión de datos de carácter personal definida ésta, por el artículo 3.j) de la LOPD, como:

"Toda revelación de datos realizada a persona distinta del interesado".

Como regla general, el artículo 11.1 de la LOPD, exige la obtención del consentimiento para la cesión de datos de carácter personal, salvo que pueda darse alguna de las excepciones recogidas en el apartado 2 del antedicho precepto, entre las que debe reseñarse la posibilidad de que exista una norma con rango de Ley habilitadora de la cesión.

En este sentido, el artículo 16.3 de la LBRL), establece lo siguiente:

"Los datos del Padrón municipal se cederán a otras Administraciones Públicas que lo soliciten sin consentimiento previo del afectado solamente cuando les sean necesarios para el ejercicio de sus respectivas competencias y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes."

En caso de que no se de dicho supuesto, los datos correspondientes al Padrón Municipal son confidenciales y la comunicación de los mismos deberá sujetarse a lo dispuesto por la LOPD.

- ***Cesión de Datos a la Policía Local***

La comunicación de datos a la Policía Local se encuadra dentro de la figura de la cesión, definida ésta por el artículo 3j) de la LOPD como:

"Toda revelación de datos realizada a persona distinta del interesado".

Como regla general, el artículo 11.1 de la LOPD, exige la obtención del consentimiento para la cesión de datos de carácter personal, salvo que pueda darse alguna de las excepciones recogidas en el apartado 2 del antedicho precepto, entre las que debe reseñarse la posibilidad de que exista una norma con rango de Ley habilitadora de la cesión.

En este sentido, los artículos 16.3 de la LBRL y 22 de la LOPD, legitiman la comunicación de datos a la Policía Local siempre que:

- Se asegure que se utilizan únicamente aquellos datos que son adecuados, pertinentes y no excesivos;
- La cesión se realice en el marco de expedientes concretos y con necesidades debidamente justificadas, relacionadas con la "prevención de un riesgo real para la seguridad o para la represión de infracciones penales, en cuyo caso deberá comunicarse la actuación de la Policía Municipal a las Fuerzas y Cuerpos de Seguridad del Estado competentes (artículo 53.2 de la Ley Orgánica 2/1986); y
- Se garanticen la confidencialidad y seguridad de los datos personales.

Por todo ello, la LOPD no permite la comunicación masiva y no justificada de todos los datos contenidos en los ficheros del Padrón Municipal a la Policía Local, siendo, no obstante, conforme a derecho la cesión concreta de determinados datos individualizados, solicitados en el marco de las competencias que tenga atribuidas.

- ***Acceso a Datos del Padrón Municipal por Entidad Prestadora del Servicio de Aguas***

En aquellos casos en los que se de la necesidad de la comunicación de datos del Padrón Municipal a la entidad que gestiona el abastecimiento de aguas, puede surgir la duda de si nos encontramos ante una cesión o un acceso a datos de carácter personal por cuenta de terceros.

Nos encontraremos ante la figura de la cesión de datos cuando, quién reciba los datos de carácter personal, pueda aplicarlos a sus propias finalidades, decidiendo sobre el objeto y la finalidad del tratamiento, convirtiéndose éste último en responsable del fichero, sin embargo, nos encontraremos ante la figura del acceso a datos por cuenta de terceros cuando, la entidad receptora de los datos, únicamente

se limite a llevar a cabo la prestación del servicio contratado por el Ayuntamiento, sin que pueda utilizarlos para otra finalidad distinta y debiendo devolver los datos una vez concluida la prestación contratada, convirtiéndose dicha entidad en encargada del tratamiento.

Una vez analizados los dos supuestos se puede concluir que, la comunicación de datos por los Ayuntamientos a entidades que gestionan el abastecimiento de aguas, se encuadra dentro de la figura del acceso a datos por cuenta de terceros, regulada en el artículo 12 de la LOPD.

En este sentido, dicho artículo, exige la celebración de un contrato entre el ayuntamiento y la entidad (Responsable del fichero y encargado del tratamiento) que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, especificando las circunstancias previstas en los apartados 2 y 3 del citado artículo.

10.4. Flujo de Datos entre Administraciones

- ***Comunicación de Datos a los Concejales de las Corporaciones Locales***

La comunicación de datos a concejales de las corporaciones locales constituye una cesión, definida, por el artículo 3 j) de la LOPD, como:

"Toda revelación de datos realizada a persona distinta del interesado".

Como regla general, el artículo 11.1 de la LOPD, exige la obtención del consentimiento para la cesión de datos de carácter personal, salvo que pueda darse alguna de las excepciones recogidas en el apartado 2 del antedicho precepto, entre las que debe reseñarse la posibilidad de que exista una norma con rango de Ley habilitadora de la cesión.

En este sentido, el artículo 77 de la LBRL, establece lo siguiente:

"Todos los miembros de las corporaciones locales tienen derecho a obtener del alcalde o Presidente de la Comisión de Gobierno cuantos antecedentes, datos o informaciones obren en poder de los servicios de la Corporación y resulten precisos para el desarrollo de su función."

Por todo ello, el acceso a datos del Ayuntamiento por parte de los concejales de las corporaciones locales, se encuentra legitimado por ley, siempre y cuando, dicho tratamiento se ajuste a la potestad de control que les es atribuida.

- ***Comunicación de Datos Tributarios de los vecinos del municipio a Órganos Superiores del Ayuntamiento***

La comunicación de datos a concejales de las corporaciones locales constituye una cesión, definida, por el artículo 3 j) de la LOPD, como:

"Toda revelación de datos realizada a persona distinta del interesado".

Como regla general, el artículo 11.1 de la LOPD, exige la obtención del consentimiento para la cesión de datos de carácter personal, salvo que pueda darse alguna de las excepciones recogidas en el apartado 2 del antedicho precepto, entre las que debe reseñarse la posibilidad de que exista una norma con rango de Ley habilitadora de la cesión.

Es conveniente tener en cuenta el artículo 2.2 del Real Decreto Legislativo 20/2004, de 5 de marzo por el que se aprueba el Texto Refundido de la Ley Reguladora de las Haciendas Locales, por el cual se puede

deducir que, resultarán de aplicación a las Haciendas Locales las mismas prerrogativas que la Ley General Tributaria atribuye a la Hacienda Estatal.

El artículo 95 de la Ley 57/2003, de 17 de diciembre, General Tributaria, establece lo siguiente:

"Los datos, informes o antecedentes obtenidos por la Administración tributaria en el desempeño de sus funciones tienen carácter reservado y sólo podrán ser utilizados para la efectiva aplicación de los tributos o recursos cuya gestión tenga encomendada, sin que puedan ser cedidos o comunicados a terceros, salvo que la cesión tenga por objeto:

a) *La investigación o persecución de delitos públicos por los órganos jurisdiccionales o el Ministerio Público.*
b) *La colaboración con otras Administraciones tributarias a efectos del cumplimiento de obligaciones fiscales en el ámbito de sus competencias.*
c) *La colaboración con la Tesorería General de la Seguridad Social para el correcto desarrollo de los fines recaudatorios encomendados a la misma.*
d) *La colaboración con cualesquiera otras Administraciones públicas para la lucha contra el fraude en la obtención o percepción de ayudas o subvenciones a cargo de fondos públicos o de la Unión Europea.*
e) *La colaboración con las comisiones parlamentarias de investigación en el marco legalmente establecido.*
f) *La protección de los derechos e intereses de los menores e incapacitados por los órganos jurisdiccionales o el Ministerio Público.*
g) *La colaboración con el Tribunal de Cuentas en el ejercicio de sus funciones de fiscalización de la Agencia Estatal de la Administración tributaria.*
h) *La colaboración con los Jueces y Tribunales para la ejecución de resoluciones judiciales firmes. La solicitud de información exigirá resolución expresa, en la que previa ponderación de los intereses públicos y privados afectados en el asunto de que se trate y por haberse agotado lo demás medios o fuentes de conocimiento sobre la existencia de bienes o derechos del deudor, se motive la necesidad de recabar datos de la Administración tributaria.*
i) *La colaboración con la Comisión de Vigilancia de Actividades de Financiación del Terrorismo en el ejercicio de sus funciones, de acuerdo con lo previsto en el artículo 8 de la Ley de Prevención y Bloqueo de la Financiación del Terrorismo.*
j) *La colaboración con el Servicio Ejecutivo creado por la Ley 19/1993, de 28 de diciembre, sobre Determinadas Medidas de Prevención del Blanqueo de Capitales, en las actividades que dicho servicio lleve a cabo en el ámbito de lo previsto en el artículo 1 de la mencionada Ley".*

En este sentido, debido al carácter reservado de la información tributaria, no se podrán ceder los datos de transcendencia tributaria a los Órganos enumerados en el artículo 130 de la LBRL, por no disponer de competencia tributaria, siempre y cuando no se de alguna de las excepciones anteriormente citadas.

- ***Delegación de Competencias***

En base a los siguientes preceptos se prevé por ley posibilidad de la delegación de competencias y encomiendas de gestión que pueda hacer una Administración a otros organismos o entidades.

"Es competencia de las entidades locales, la gestión, recaudación e inspección de sus tributos propios, sin perjuicio de las delegaciones que puedan otorgar a favor de las entidades locales de ámbito superior o de las respectivas Comunidades Autónomas, y de las fórmulas de colaboración con otras Entidades locales, con las Comunidades Autónomas o con el Estado, de acuerdo con lo que establezca la legislación del Estado." (Artículo 106.3 LBRL)

"1. […] Asimismo las Entidades locales podrán delegar en la Comunidad Autónoma o en otras Entidades locales en cuyo territorio estén integradas, las facultadas de gestión, liquidación, inspección y recaudación de los restantes ingresos de Derecho público que les correspondan.

2. El acuerdo que adopte el Pleno de la corporación habrá de fijar el alcance y contenido de la referida delegación y se publicará, una vez aceptada por el órgano correspondiente de gobierno, referido siempre al Pleno, y, en último término, ante la Jurisdicción Contencioso-Administrativa.

Las facultades delegadas serán ejercidas por el órgano de la entidad delegada que proceda conforme a las normas internas de distribución de competencias propias de dicha entidad.

*4. Las entidades que al amparo de lo previsto en este artículo hayan asumido por delegación de una Entidad local todas o algunas de las facultades de gestión, liquidación, inspección y recaudación de todos o algunos de los tributos o recursos de Derecho público de dicha Entidad local, podrán ejercer tales facultades delegadas en todo su ámbito territorial e incluso en el de otras Entidades locales que no le hayan delegado tales facultades."(*Artículo 7.1 TRLHL)

Por todo ello, en relación a la protección de datos, es conveniente dilucidar la posición que ocuparía la entidad gestora en relación al servicio encomendado.

En este sentido, en caso de que, quien desarrolla una competencia en virtud de una encomienda de gestión pueda ostentar la facultad de decidir sobre la finalidad, contenido y uso del tratamiento por sí mismo, con independencia de que dicho tratamiento se realice, precisamente para dar complimiento a la gestión encomendada, dicha entidad gestora se convertiría automáticamente en responsable del fichero,

lo cual supone, el surgimiento de un vínculo entre la entidad gestora y el titular de los datos de carácter personal.

Por otra parte, en caso de que, la entidad gestora, actúe siguiendo las instrucciones del responsable del fichero, y actuando en nombre de este último, sin que exista posibilidad de decisión en cuanto al uso y tratamiento de los datos con independencia del responsable del fichero, dicha entidad será considerada encargada del tratamiento. En consecuencia, habrá que estar a lo dispuesto por el artículo 12 de la LOPD, en cuanto a la exigencia de la celebración de un contrato entre ambas partes (Responsable del fichero-Encargado del tratamiento) que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, especificando las circunstancias previstas en los apartados 2 y 3 del citado artículo.

Por ejemplo, se daría una relación Responsable del fichero-Encargado del tratamiento, en el caso de que un Ayuntamiento encomiende la gestión de recaudación del tributo municipal a la Diputación Provincial, puesto que la potestad tributaria en el ámbito municipal corresponde al Ayuntamiento, actuando, la Diputación Provincial, únicamente en nombre y por cuenta del titular de dicha potestad.

10.5. Publicidad de Actuaciones Municipales

- ***Publicación de Datos en Procedimientos selectivos***

Respecto de los datos relacionados con procedimientos de concurrencia competitiva, las normas reguladoras de ingreso y promoción en la función pública vienen a establecer, como criterio esencial que funda su régimen, el principio de publicidad, cuestión lógica dado que resultará necesario el conocimiento por parte de los distintos aspirantes a las pruebas de los resultados de las mismas para conocer adecuada mente las circunstancias concurrentes en el proceso selectivo en el que han tomado parte.

En este sentido, es conveniente hacer referencia a la Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público, el cual recalca los principios de legalidad, cobertura presupuestaria, obligatoriedad de la negociación, buena fe, publicidad y transparencia que han de presidir los procedimientos.

Teniendo en cuenta lo anterior, el Real Decreto 364/1995, en su artículo 47, establece la necesaria publicación de los resultados a través de su publicación en el Boletín Oficial del Estado.

Además no puede obviarse lo dispuesto en el artículo 59.6 b) donde se señala que: "*Cuando se trate de actos integrantes de un procedimiento selectivo o de concurrencia competitiva de cualquier tipo. En este caso, la convocatoria del procedimiento deberá indicar el tablón de anuncios o medio de comunicación donde se efectuarán las sucesivas publicaciones, careciendo de validez las que se lleven a cabo en lugares distintos*".

Por otro lado, en relación a la publicación de datos relativos a procedimientos de concurrencia no competitiva, la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común no prevé la publicación de los datos relativos a este tipo de procedimientos, por lo que se recomienda que se analice, en cada caso, la posible existencia de una previsión legal sectorial que autorice la publicación de los datos de carácter personal, o se solicite y obtenga el consentimiento del interesado.

- ***Publicación de Sesiones del Pleno y de la Junta Directiva***

La publicación en Internet de los datos contenidos en las actas de los Plenos y Juntas de Gobierno del Ayuntamiento se encuadra dentro de la figura de la cesión, definida por el artículo 3 j) de la LOPD, como:

"Toda revelación de datos realizada a persona distinta del interesado".

Como regla general, el artículo 11.1 de la LOPD, exige la obtención del consentimiento para la cesión de datos de carácter personal, salvo que pueda darse alguna de las excepciones recogidas en el apartado 2 del antedicho precepto, entre las que debe reseñarse la posibilidad de que exista una norma con rango de Ley habilitadora de la cesión o cuando se refiera a datos incorporados en fuentes accesibles al público.

Se entienden por fuentes accesibles al público (artículo 11.2.j LOPD):

"exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los ´diarios y Boletines oficiales y los medios de comunicación."

En este sentido, es conveniente tener en cuenta el artículo 70 de la LBRL, en cuanto a la publicidad de las actividades municipales:

"1. Las sesiones del Pleno de las corporaciones locales son públicas. No obstante, podrán ser secretos el debate y votación de aquellos asuntos que puedan afectar al derecho fundamental de los ciudadanos a que se refiere el artículo 18.1 de la Constitución, cuando así se acuerde por mayoría absoluta.

No son públicas las sesiones de la Junta de Gobierno Local.

2. los acuerdos que adopten las corporaciones locales se publican o notifican en la forma prevista por la Ley. Las ordenanzas, incluidos el articulado de las normas de los planes urbanísticos, así como los acuerdos correspondientes a éstos cuya aprobación definitiva sea competencia de los entes locales, se publicarán en el "Boletín Oficial" de la provincia y no entrarán en vigor hasta que se haya publicado completamente su texto y haya transcurrido el plazo previsto en el artículo 65.2 salvo los presupuestos y las ordenanzas fiscales que se publican y entran en vigor en los términos establecidos en la Ley 39/1988, de 28 de diciembre, Reguladora de las Haciendas Locales. Las Administraciones públicas con competencias urbanísticas deberán tener, a disposición de los ciudadanos que lo soliciten, copias completas del planeamiento vigente en su ámbito territorial.

3. Todos los ciudadanos tienen derecho a obtener copias y certificaciones acreditativas de los acuerdos de las corporaciones locales y sus antecedentes, así como a consultar los archivos y registros en los términos que disponga la legislación de desarrollo del artículo 105, párrafo b), de la Constitución. La denegación o limitación de este derecho, en todo cuanto afecte a la seguridad y defensa del Estado, la averiguación de los delitos o la intimidad de las personas, deberá verificarse mediante resolución motivada."

Por todo ello, se encuentra legitimada la comunicación de datos, por medio de internet, cuando los mismos se refieran a actos debatidos en Pleno de la Corporación, por tratarse de una cesión habilitada por

legal, o a disposiciones objeto de publicación en el Boletín Oficial correspondiente, por tratarse de datos incorporados en fuentes accesibles al público.

En cualquier otro supuesto, como por ejemplo, la publicación de datos relativos a sesiones de la Junta de Gobierno Local, únicamente se podría proceder a la comunicación de dichos datos cuando intervenga el consentimiento de los interesados.

10.6. Publicación Web

- ***Publicación de Directorios en Sitios Web Institucionales***

En relación a la publicación de datos de carácter personal de empleados públicos integrantes de un organismo, se recomienda que no se publiquen en los sitios web institucionales, la dirección de correo electrónico ni el número de teléfono de los empleados públicos al servicio de la Administración Pública, recomendándose la publicación de números de teléfono y direcciones de correo electrónico institucionales.

En consecuencia, es recomendable que , en su caso, la publicación de los datos personales que componen los directorios institucionales se realice a través de una Intranet administrativa o de área privada ubicada en el sitio web institucional, que requieran la identificación y autenticación por mecanismos fiables que permitan acreditar indubitadamente la identidad de la persona que acceda a dicha información.

No obstante lo anterior, en el supuesto del personal con responsabilidades políticas, se entiende que puede procederse a la publicación de su nombre y apellidos, dirección postal y dirección de correo electrónico, sin consentimiento del mismo, atendiendo al principio democrático y representativo. La dirección de correo electrónico personal deberá ser sustituida en estos casos por una dirección de correo electrónico institucional.

- ***Publicación de Ponencias, Seminarios o Imágenes de Eventos***

Respecto de la publicación de ponencias, seminarios o imágenes de eventos en sitios web institucionales, debe tenerse en cuenta que la participación en el mismo no lleva aparejado automáticamente el consentimiento de los participantes. No obstante, a efectos de publicidad del seminario, jornada o evento, la participación en el mismo conlleva el consentimiento para publicar la agenda u orden del día con los datos personales del ponente.

En este sentido, para poder proceder a la publicación de los restantes datos de carácter personal que se refieran a personas físicas identificadas o identificables ajenas a la Administración Pública u órgano administrativo competente, se deberá solicitar y obtener el consentimiento.

Dicha obligación no será exigible cuando los datos personales se refieran a cargos políticos o empleados públicos pertenecientes a la organización, al entenderse que, en estos supuestos, resulta de aplicación lo dispuesto en el artículo 11.2.c) de la LOPD, respondiendo la publicación de los datos a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimento y control implica la publicación de los datos de carácter personal.

- ***Publicación de Imágenes de Interesados***

En el caso de que se proceda a la publicación de la imagen de un ciudadano en un sitio web institucional, el organismo deberá obtener el consentimiento del interesado para dicha publicación, salvo que la imagen fuera captada por un medio de comunicación en ejercicio de la libertad de información reconocida por el artículo 20 de la Constitución Española.

Por otro lado, en el supuesto de imágenes de contenido o carácter histórico se podrá proceder a la publicación de las mismas siempre y cuando gocen de la condición de documento histórico de acuerdo con lo dispuesto en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español.

10.7. Comunicación de Datos entre Administraciones Públicas

Las sedes electrónicas y los registros telemáticos donde se reciban las solicitudes presentadas por los ciudadanos para el acceso a un determinado servicio de administración electrónica, están legitimadas para la cesión de los datos recibidos a los órganos administrativos en quien reside la competencia para la tramitación y resolución del correspondiente expediente administrativo, en virtud de la relación jurídica que se establece entre el ciudadano y el órgano receptor de la solicitud, así como para tratarse de datos recabados con destino a otras Administraciones Públicas.

Los datos de carácter personal, recabados o elaborados por una Administración Pública, en el ejercicio de sus competencias, que causen estado y puedan producir efectos jurídicos, podrán ser cedidos a otros órganos de la misma o distinta Administración, sin consentimiento del interesado, al objeto de que se realicen las comprobaciones necesarias para acreditar la autenticidad de los mismos y su tratamiento en la tramitación de los expedientes administrativos que fueran necesarios. No obstante, en los formularios en que se recaben los datos del interesado, al dar complimiento del deber de información se informará expresamente de los datos que serán objeto de verificación mediante la consulta a los datos o documentos obrantes en otros órganos de la misma o distinta administración pública.

El acceso a cualquier fichero o repositorio por otro órgano de la misma o distinta Administración Pública solo podrá realizarse acreditando disponer del consentimiento del interesado para su acceso o que es necesario para verificar la exactitud de un dato aportado por el ciudadano, tal y como dispone el artículo 9 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

11. Glosario

Accesos Autorizados

Autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.

Afectado o Interesado

Persona física titular de los datos que sean objeto del tratamiento.

Autenticación

Procedimiento de comprobación de la identidad de un usuario.

Cancelación

Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.

Cesión o Comunicación de Datos

Tratamiento de datos que supone su revelación a una persona distinta del interesado.

Consentimiento del Interesado

Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

Contraseña

Información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.

Control de Acceso

Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

Copia de Respaldo

Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

Dato Disociado

Aquél que no permite la identificación de un afectado o interesado.

Datos de Carácter Personal

Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

Datos de Carácter Personal relacionados con la Salud

Las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.

Derecho de Acceso

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.

Derecho de Oposición

Derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo, en los casos previstos por el artículo 34 del RLOPD.

Derecho de Rectificación

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

Derecho de Cancelación

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

Destinatario o Cesionario

La persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos. Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

Documento

Todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.

Encargado del Tratamiento

La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio. Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

Exportador de Datos Personales

La persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero.

Fichero

Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Ficheros de Titularidad Privada

Los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.

Ficheros de Titularidad Pública

Los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre público.

Fichero no Automatizado

Todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

Ficheros Temporales

Ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

Fuentes Accesibles al Público

Aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

Importador de Datos Personales

La persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

Identificación

Procedimiento de reconocimiento de la identidad de un usuario.

Incidencia

Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

Persona Identificable

Toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

Perfil de Usuario

Accesos autorizados a un grupo de usuarios.

Procedimiento de Disociación

Todo tratamiento de datos personales que permita la obtención de datos disociados.

Recurso

Cualquier parte componente de un sistema de información.

Responsable del Fichero o del Tratamiento

Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente. Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

Responsable de Seguridad

Persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

Sistema de Información

Conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.

Sistema de Tratamiento

Modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

Soporte

Objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

Tercero

La persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento. Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

Transferencia Internacional de Datos

Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

Transmisión de Documentos

Cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.

Tratamiento de Datos

Cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Usuario

Sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

12. Normativa

12.1. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal[11]

TÍTULO I. Disposiciones generales

Artículo 1. Objeto.

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

Artículo 2. Ámbito de aplicación.

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

Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.
b) 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.
c) 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.

2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:

a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas.

[11] Modificada conforme al artículo 79 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social (B.O.E.. núm. 313, de 31 de diciembre).

c) 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.

3. Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:

a) Los ficheros regulados por la legislación de régimen electoral.
b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.
c) Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas.
d) Los derivados del Registro Civil y del Registro Central de penados y rebeldes.
e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

Artículo 3. Definiciones.

A los efectos de la presente Ley Orgánica se entenderá por:

a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.
b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
c) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
d) 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.
e) Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.
f) Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.
g) Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

h) Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

i) Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado.

j) Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

TÍTULO II. Principios de la protección de datos

Artículo 4. Calidad de los datos.

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

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

3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

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

Artículo 5. Derecho de información en la recogida de datos.

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

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

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 trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

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

3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

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

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

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

Artículo 6. Consentimiento del afectado.

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

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

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

4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

Artículo 7. Datos especialmente protegidos.

1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

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

2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

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

6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Artículo 8. Datos relativos a la salud.

Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

Artículo 9. Seguridad de los datos.

1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

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

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

Artículo 10. Deber de secreto.

El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Artículo 11. Comunicación de datos.

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

2. El consentimiento exigido en el apartado anterior no será preciso:

a) Cuando la cesión está autorizada en una ley.
b) Cuando se trate de datos recogidos de fuentes accesibles al público.
c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

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

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

5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.

6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

Artículo 12. Acceso a los datos por cuenta de terceros.

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

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

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

TÍTULO III. Derechos de las personas

Artículo 13. Impugnación de valoraciones.

1. Los ciudadanos 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 de datos destinados a evaluar determinados aspectos de su personalidad.

2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.

3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.

4. La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

Artículo 14. Derecho de consulta al Registro General de Protección de Datos.

Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita.

Artículo 15. Derecho de acceso.

1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.

Artículo 16. Derecho de rectificación y cancelación.

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.

2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.

3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

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

5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

Artículo 17. Procedimiento de oposición, acceso, rectificación o cancelación.

1. Los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación serán establecidos reglamentariamente.

2. No se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación.

Artículo 18. Tutela de los derechos.

1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia Española de Protección de Datos, en la forma que reglamentariamente se determine.

2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia Española de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación.

3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses.

4. Contra las resoluciones de la Agencia Española de Protección de Datos procederá recurso contencioso-administrativo.

Artículo 19. Derecho a indemnización.

1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

2. 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.

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

TÍTULO IV. Disposiciones sectoriales

CAPÍTULO I. Ficheros de titularidad pública

Artículo 20. Creación, modificación o supresión.

1. La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el «Boletín Oficial del Estado» o Diario oficial correspondiente.

2. Las disposiciones de creación o de modificación de ficheros deberán indicar:

a) La finalidad del fichero y los usos previstos para el mismo.
b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
c) El procedimiento de recogida de los datos de carácter personal.
d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.

f) Los órganos de las Administraciones responsables del fichero.

g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

3. En las disposiciones que se dicten para la supresión de los ficheros, se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.

Artículo 21. Comunicación de datos entre Administraciones públicas.

1. Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos[12].

2. Podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración pública obtenga o elabore con destino a otra.

3. No obstante lo establecido en el artículo 11.2.b), la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una ley prevea otra cosa.

4. En los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley.

Artículo 22. Ficheros de las Fuerzas y Cuerpos de Seguridad.

1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.

2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

[12] Redactado conforme a la STC 292/2000, de 30 de noviembre, que ha declarado inconstitucional y nulo el inciso *[cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o]*.

3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.

4. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Artículo 23. Excepciones a los derechos de acceso, rectificación y cancelación.

1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia Española de Protección de Datos o del organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.

***Artículo 24. Otras excepciones a los derechos de los afectados*[13].**

1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales.

CAPÍTULO II. Ficheros de titularidad privada

Artículo 25. Creación.

Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas.

Artículo 26. Notificación e inscripción registral.

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

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

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

4. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles.

En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.

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

---

[13] Redactado conforme a la STC 292/2000, de 30 de noviembre, que ha declarado inconstitucional y nulo el inciso *[impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas]* y *[o administrativas]* del apartado 1 y *[2. Lo dispuesto en el artículo 15 y en el apartado 1 del artículo 16 no será de aplicación si, ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección. Si el órgano administrativo responsable del fichero invocase lo dispuesto en este apartado, dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de la Agencia de Protección de Datos o, en su caso, del órgano equivalente de las Comunidades Autónomas.]*.

Artículo 27. Comunicación de la cesión de datos.

1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.

2. La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c), d), e) y 6 del artículo 11, ni cuando la cesión venga impuesta por ley.

Artículo 28. Datos incluidos en las fuentes de acceso público.

1. Los datos personales que figuren en el censo promocional, o las listas de personas pertenecientes a grupos de profesionales a que se refiere el artículo 3, j) de esta Ley deberán limitarse a los que sean estrictamente necesarios para cumplir la finalidad a que se destina cada listado. La inclusión de datos adicionales por las entidades responsables del mantenimiento de dichas fuentes requerirá el consentimiento del interesado, que podrá ser revocado en cualquier momento.

2. Los interesados tendrán derecho a que la entidad responsable del mantenimiento de los listados de los Colegios profesionales indique gratuitamente que sus datos personales no pueden utilizarse para fines de publicidad o prospección comercial.

Los interesados tendrán derecho a exigir gratuitamente la exclusión de la totalidad de sus datos personales que consten en el censo promocional por las entidades encargadas del mantenimiento de dichas fuentes.

La atención a la solicitud de exclusión de la información innecesaria o de inclusión de la objeción al uso de los datos para fines de publicidad o venta a distancia deberá realizarse en el plazo de diez días respecto de las informaciones que se realicen mediante consulta o comunicación telemática y en la siguiente edición del listado cualquiera que sea el soporte en que se edite.

3. Las fuentes de acceso público que se editen en forma de libro o algún otro soporte físico, perderán el carácter de fuente accesible con la nueva edición que se publique.

En el caso de que se obtenga telemáticamente una copia de la lista en formato electrónico, ésta perderá el carácter de fuente de acceso público en el plazo de un año, contado desde el momento de su obtención.

4. Los datos que figuren en las guías de servicios de telecomunicaciones disponibles al público se regirán por su normativa específica.

Artículo 29. Prestación de servicios de información sobre solvencia patrimonial y crédito.

1. 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.

2. Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley.

3. En los supuestos a que se refieren los dos apartados anteriores, cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos.

4. Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos.

Artículo 30. Tratamientos con fines de publicidad y de prospección comercial.

1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento.

2. Cuando los datos procedan de fuentes accesibles al público, de conformidad con lo establecido en el párrafo segundo del artículo 5.5 de esta Ley, en cada comunicación que se dirija al interesado se informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.

3. En el ejercicio del derecho de acceso los interesados tendrán derecho a conocer el origen de sus datos de carácter personal, así como del resto de información a que se refiere el artículo 15.

4. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

Artículo 31. Censo promocional.

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

2. El uso de cada lista de censo promocional tendrá un plazo de vigencia de un año. Transcurrido el plazo citado, la lista perderá su carácter de fuente de acceso público.

3. Los procedimientos mediante los que los interesados podrán solicitar no aparecer en el censo promocional se regularán reglamentariamente. Entre estos procedimientos, que serán gratuitos para los interesados, se incluirá el documento de empadronamiento. Trimestralmente se editará una lista actualizada del censo promocional, excluyendo los nombres y domicilios de los que así lo hayan solicitado.

4. Se podrá exigir una contraprestación por la facilitación de la citada lista en soporte informático.

Artículo 32. Códigos tipo.

1. Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo.

2. Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación.

En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.

3. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de acuerdo con el artículo 41. El Registro General de Protección de Datos podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia Española de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas.

TÍTULO V. Movimiento internacional de datos

Artículo 33. Norma general.

1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia Española de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia Española de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Artículo 34. Excepciones.

Lo dispuesto en el artículo anterior no será de aplicación:

a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.
b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.
c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.
d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.
e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.
f) Cuando la transferencia 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.
g) Cuando la transferencia 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.
h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.
i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.

k) Cuando la transferencia 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.

TÍTULO VI. Agencia Española de Protección de Datos

Artículo 35. Naturaleza y régimen jurídico.

1. La Agencia Española de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno.

2. En el ejercicio de sus funciones públicas, y en defecto de lo que disponga la presente Ley y sus disposiciones de desarrollo, la Agencia Española de Protección de Datos actuará de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En sus adquisiciones patrimoniales y contratación estará sujeta al derecho privado.

3. Los puestos de trabajo de los órganos y servicios que integren la Agencia Española de Protección de Datos serán desempeñados por funcionarios de las Administraciones públicas y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo. Este personal está obligado a guardar secreto de los datos de carácter personal de que conozca en el desarrollo de su función.

4. La Agencia Española de Protección de Datos contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos:

a) Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado.

b) Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.

c) Cualesquiera otros que legalmente puedan serle atribuidos.

5. La Agencia Española de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno para que sea integrado, con la debida independencia, en los Presupuestos Generales del Estado.

Artículo 36. El Director.

1. El Director de la Agencia Española de Protección de Datos dirige la Agencia y ostenta su representación. Será nombrado, de entre quienes componen el Consejo Consultivo, mediante Real Decreto, por un período de cuatro años.

2. Ejercerá sus funciones con plena independencia y objetividad y no estará sujeto a instrucción alguna en el desempeño de aquéllas.

En todo caso, el Director deberá oír al Consejo Consultivo en aquellas propuestas que éste le realice en el ejercicio de sus funciones.

3. El Director de la Agencia Española de Protección de Datos sólo cesará antes de la expiración del período a que se refiere el apartado 1, a petición propia o por separación acordada por el Gobierno, previa instrucción de expediente, en el que necesariamente serán oídos los restantes miembros del Consejo Consultivo, por incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por delito doloso.

4. El Director de la Agencia Española de Protección de Datos tendrá la consideración de alto cargo y quedará en la situación de servicios especiales si con anterioridad estuviera desempeñando una función pública. En el supuesto de que sea nombrado para el cargo algún miembro de la carrera judicial o fiscal, pasará asimismo a la situación administrativa de servicios especiales.

Artículo 37. Funciones[14].

1. Son funciones de la Agencia Española de Protección de Datos:

a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.
b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.
c) Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley.
d) Atender las peticiones y reclamaciones formuladas por las personas afectadas.
e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.

[14] Redactado conforme al apartado Uno del artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social (B.O.E. núm. 313, de 31 de diciembre). Añade el apartado 2.

f) Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.

g) Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley.

h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.

i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.

k) Redactar una memoria anual y remitirla al Ministerio de Justicia.

l) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

m) Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46.

n) Cuantas otras le sean atribuidas por normas legales o reglamentarias.

2. Las resoluciones de la Agencia Española de Protección de Datos se harán públicas, una vez hayan sido notificadas a los interesados. La publicación se realizará preferentemente a través de medios informáticos o telemáticos. Reglamentariamente podrán establecerse los términos en que se lleve a cabo la publicidad de las citadas resoluciones.

Lo establecido en los párrafos anteriores no será aplicable a las resoluciones referentes a la inscripción de un fichero o tratamiento en el Registro General de Protección de Datos ni a aquéllas por las que se resuelva la inscripción en el mismo de los Códigos tipo, regulados por el artículo 32 de esta ley orgánica.

Artículo 38. Consejo Consultivo.

El Director de la Agencia Española de Protección de Datos estará asesorado por un Consejo Consultivo compuesto por los siguientes miembros:

Un Diputado, propuesto por el Congreso de los Diputados.

Un Senador, propuesto por el Senado.

Un representante de la Administración Central, designado por el Gobierno.

Un representante de la Administración Local, propuesto por la Federación Española de Municipios y Provincias.

Un miembro de la Real Academia de la Historia, propuesto por la misma.

Un experto en la materia, propuesto por el Consejo Superior de Universidades.

Un representante de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente.

Un representante de cada Comunidad Autónoma que haya creado una agencia de protección de datos en su ámbito territorial, propuesto de acuerdo con el procedimiento que establezca la respectiva Comunidad Autónoma.

Un representante del sector de ficheros privados, para cuya propuesta se seguirá el procedimiento que se regule reglamentariamente.

El funcionamiento del Consejo Consultivo se regirá por las normas reglamentarias que al efecto se establezcan.

Artículo 39. El Registro General de Protección de Datos.

1. El Registro General de Protección de Datos es un órgano integrado en la Agencia Española de Protección de Datos.

2. Serán objeto de inscripción en el Registro General de Protección de Datos:

a) Los ficheros de que sean titulares las Administraciones públicas.
b) Los ficheros de titularidad privada.
c) Las autorizaciones a que se refiere la presente Ley.
d) Los códigos tipo a que se refiere el artículo 32 de la presente Ley.
e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

3. Por vía reglamentaria se regulará el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, en el Registro General de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes.

Artículo 40. Potestad de inspección.

1. Las autoridades de control podrán inspeccionar los ficheros a que hace referencia la presente Ley, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos.

A tal efecto, podrán solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados.

2. Los funcionarios que ejerzan la inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

Artículo 41. Órganos correspondientes de las Comunidades Autónomas.

1. Las funciones de la Agencia Española de Protección de Datos reguladas en el artículo 37, a excepción de las mencionadas en los apartados j), k) y l), y en los apartados f) y g) en lo que se refiere a las transferencias internacionales de datos, así como en los artículos 46 y 49, en relación con sus específicas competencias serán ejercidas, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial, por los órganos correspondientes de cada Comunidad, que tendrán la consideración de autoridades de control, a los que garantizarán plena independencia y objetividad en el ejercicio de su cometido.

2. Las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros para el ejercicio de las competencias que se les reconoce sobre los mismos.

3. El Director de la Agencia Española de Protección de Datos podrá convocar regularmente a los órganos correspondientes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación. El Director de la Agencia Española de Protección de Datos y los órganos correspondientes de las Comunidades Autónomas podrán solicitarse mutuamente la información necesaria para el cumplimiento de sus funciones.

Artículo 42. Ficheros de las Comunidades Autónomas en materia de su exclusiva competencia.

1. Cuando el Director de la Agencia Española de Protección de Datos constate que el mantenimiento o uso de un determinado fichero de las Comunidades Autónomas contraviene algún precepto de esta Ley en materia de su exclusiva competencia podrá requerir a la Administración correspondiente que se adopten las medidas correctoras que determine en el plazo que expresamente se fije en el requerimiento.

2. Si la Administración pública correspondiente no cumpliera el requerimiento formulado, el Director de la Agencia Española de Protección de Datos podrá impugnar la resolución adoptada por aquella Administración.

TÍTULO VII. Infracciones y sanciones

Artículo 43. Responsables.

1. Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley.

2. Cuando se trate de ficheros de los que sean responsables las Administraciones públicas se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en el artículo 46, apartado 2.

Artículo 44. Tipos de infracciones.

1. Las infracciones se calificarán como leves, graves o muy graves.

2. Son infracciones leves:

a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.
b) No proporcionar la información que solicite la Agencia Española de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.
c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.
d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley.
e) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave.

3. Son infracciones graves:

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

b) Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.

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

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

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

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

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

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

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

j) La obstrucción al ejercicio de la función inspectora.

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

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

4. Son infracciones muy graves:

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

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

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

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

e) La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia Española de Protección de Datos.

f) Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

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

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

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

Artículo 45. Tipo de sanciones[15].

1. Las infracciones leves serán sancionadas con multa de 601,01 a 60.101,21 €.

2. Las infracciones graves serán sancionadas con multa de 60.101,21 a 300.506,05 €.

3. Las infracciones muy graves serán sancionadas con multa de 300.506,05 a 601.012,10 €.

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

[15] Redactado conforme a la Resolución de 11 de diciembre de 2001, de la Subsecretaría, por la que se da publicidad a la conversión a euros de los valores correspondientes a los procedimientos sancionadores establecidos en diversas normas y a los precios privados del Ministerio de Justicia (B.O.E. núm. 303, de 10 de diciembre).

5. Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate.

6. En ningún caso podrá imponerse una sanción más grave que la fijada en la Ley para la clase de infracción en la que se integre la que se pretenda sancionar.

7. El Gobierno actualizará periódicamente la cuantía de las sanciones de acuerdo con las variaciones que experimenten los índices de precios.

Artículo 46. Infracciones de las Administraciones públicas.

1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de los que sean responsables las Administraciones públicas, el Director de la Agencia Española de Protección de Datos dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

2. El Director de la Agencia podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones públicas.

3. Se deberán comunicar a la Agencia las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores.

Artículo 47. Prescripción.

1. Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año.

2. El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido.

3. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.

4. Las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año.

5. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que adquiera firmeza la resolución por la que se impone la sanción.

6. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

Artículo 48. Procedimiento sancionador.

1. Por vía reglamentaria se establecerá el procedimiento a seguir para la determinación de las infracciones y la imposición de las sanciones a que hace referencia el presente Título.

2. Las resoluciones de la Agencia Española de Protección de Datos u órgano correspondiente de la Comunidad Autónoma agotan la vía administrativa.

3. Los procedimientos sancionadores tramitados por la Agencia Española de Protección de Datos, en ejercicio de las potestades que a la misma atribuyan esta u otras Leyes, salvo los referidos a infracciones de la Ley 32/2003,de 3 de noviembre, General de Telecomunicaciones, tendrán una duración máxima de seis meses[16].

Artículo 49. Potestad de inmovilización de ficheros.

En los supuestos, constitutivos de infracción muy grave, de utilización o cesión ilícita de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia Española de Protección de Datos podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido, la Agencia Española de Protección de Datos podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas.

[16] Introducido por el apartado Dos del artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social (B.O.E. núm. 313, de 31 de diciembre).

Disposición adicional primera. Ficheros preexistentes.

Los ficheros y tratamientos automatizados inscritos o no en el Registro General de Protección de Datos deberán adecuarse a la presente Ley Orgánica dentro del plazo de tres años, a contar desde su entrada en vigor. En dicho plazo, los ficheros de titularidad privada deberán ser comunicados a la Agencia Española de Protección de Datos y las Administraciones públicas, responsables de ficheros de titularidad pública, deberán aprobar la pertinente disposición de regulación del fichero o adaptar la existente.

En el supuesto de ficheros y tratamientos no automatizados, su adecuación a la presente Ley Orgánica, y la obligación prevista en el párrafo anterior deberán cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados.

Disposición adicional segunda. Ficheros y Registro de Población de las Administraciones públicas.

1. La Administración General del Estado y las Administraciones de las Comunidades Autónomas podrán solicitar al Instituto Nacional de Estadística, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en los padrones municipales de habitantes y en el censo electoral correspondientes a los territorios donde ejerzan sus competencias, para la creación de ficheros o registros de población.

2. Los ficheros o registros de población tendrán como finalidad la comunicación de los distintos órganos de cada Administración pública con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico administrativas derivadas de las competencias respectivas de las Administraciones públicas.

Disposición adicional tercera. Tratamiento de los expedientes de las derogadas Leyes de Vagos y Maleantes y de Peligrosidad y Rehabilitación Social.

Los expedientes específicamente instruidos al amparo de las derogadas Leyes de Vagos y Maleantes, y de Peligrosidad y Rehabilitación Social, que contengan datos de cualquier índole susceptibles de afectar a la seguridad, al honor, a la intimidad o a la imagen de las personas, no podrán ser consultados sin que medie consentimiento expreso de los afectados, o hayan transcurrido cincuenta años desde la fecha de aquéllos.

En este último supuesto, la Administración General del Estado, salvo que haya constancia expresa del fallecimiento de los afectados, pondrá a disposición del solicitante la documentación, suprimiendo de la misma los datos aludidos en el párrafo anterior, mediante la utilización de los procedimientos técnicos pertinentes en cada caso.

Disposición adicional cuarta. Modificación del artículo 112.4 de la Ley General Tributaria.

El apartado cuarto del artículo 112 de la Ley General Tributaria pasa a tener la siguiente redacción:

«4. La cesión de aquellos datos de carácter personal, objeto de tratamiento, que se debe efectuar a la Administración tributaria conforme a lo dispuesto en el artículo 111, en los apartados anteriores de este artículo o en otra norma de rango legal, no requerirá el consentimiento del afectado. En este ámbito tampoco será de aplicación lo que respecto a las Administraciones públicas establece el apartado 1 del artículo 21 de la Ley Orgánica de Protección de Datos de carácter personal.»

Disposición adicional quinta. Competencias del Defensor del Pueblo y órganos autonómicos semejantes.

Lo dispuesto en la presente Ley Orgánica se entiende sin perjuicio de las competencias del Defensor del Pueblo y de los órganos análogos de las Comunidades Autónomas.

Disposición adicional sexta. Modificación del artículo 24.3 de la Ley de Ordenación y Supervisión de los Seguros Privados.

Se modifica el artículo 24.3, párrafo 2. o de la Ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión de los Seguros Privados, con la siguiente redacción:

«Las entidades aseguradoras podrán establecer ficheros comunes que contengan datos de carácter personal para la liquidación de siniestros y la colaboración estadístico actuarial con la finalidad de permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora. La cesión de datos a los citados ficheros no requerirá el consentimiento previo del afectado, pero sí la comunicación al mismo de la posible cesión de sus datos personales a ficheros comunes para los fines señalados con expresa indicación del responsable para que se puedan ejercitar los derechos de acceso, rectificación y cancelación previstos en la ley.

También podrán establecerse ficheros comunes cuya finalidad sea prevenir el fraude en el seguro sin que sea necesario el consentimiento del afectado. No obstante, será necesaria en estos casos la comunicación al afectado, en la primera introducción de sus datos, de quién sea el responsable del fichero y de las formas de ejercicio de los derechos de acceso, rectificación y cancelación.

En todo caso, los datos relativos a la salud sólo podrán ser objeto de tratamiento con el consentimiento expreso del afectado.»

Disposición transitoria primera. Tratamientos creados por Convenios internacionales.

La Agencia Española de Protección de Datos será el organismo competente para la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal respecto de los tratamientos establecidos en cualquier Convenio Internacional del que sea parte España que atribuya a una autoridad nacional de control esta competencia, mientras no se cree una autoridad diferente para este cometido en desarrollo del Convenio.

Disposición transitoria segunda. Utilización del censo promocional.

Reglamentariamente se desarrollarán los procedimientos de formación del censo promocional, de oposición a aparecer en el mismo, de puesta a disposición de sus solicitantes, y de control de las listas difundidas. El Reglamento establecerá los plazos para la puesta en operación del censo promocional.

Disposición transitoria tercera. Subsistencia de normas preexistentes.

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

Disposición derogatoria única. Derogación normativa.

Queda derogada la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de los datos de carácter personal.

Disposición final primera. Habilitación para el desarrollo reglamentario.

El Gobierno aprobará, o modificará, las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la presente Ley.

Disposición final segunda. Preceptos con carácter de Ley ordinaria.

Los Títulos IV, VI excepto el último inciso del párrafo 4 del artículo 36 y VII de la presente Ley, la disposición adicional cuarta, la disposición transitoria primera y la final primera tienen el carácter de Ley ordinaria.

Disposición final tercera. Entrada en vigor.

La presente Ley entrará en vigor en el plazo de un mes, contado desde su publicación en el «Boletín Oficial del Estado».

12.2. Real Decreto 12/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LOPD

I

La actual Ley Orgánica 15/1999, de 13 de diciembre de Protección de datos de carácter personal adaptó nuestro ordenamiento a lo dispuesto por la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, derogando a su vez la hasta entonces vigente Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de datos de carácter personal.

La nueva ley, que ha nacido con una amplia vocación de generalidad, prevé en su artículo 1 que «tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal». Comprende por tanto el tratamiento automatizado y el no automatizado de los datos de carácter personal.

A fin de garantizar la necesaria seguridad jurídica en un ámbito tan sensible para los derechos fundamentales como el de la protección de datos, el legislador declaró subsistentes las normas reglamentarias existentes y, en especial, los reales decretos 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre de Regulación del tratamiento automatizado de los datos de carácter personal y 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, a la vez que habilitó al Gobierno para la aprobación o modificación de las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la Ley Orgánica 15/1999.

Por otra parte, la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico y la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones atribuyen competencias en materia sancionadora a la Agencia Española de Protección de Datos. Éstas requieren de desarrollo reglamentario con la peculiaridad de que ambas normas se ordenan a la tutela no sólo de los derechos de las personas físicas, sino también de las jurídicas.

II

Este Reglamento comparte con la Ley Orgánica la finalidad de hacer frente a los riesgos que para los derechos de la personalidad pueden suponer el acopio y tratamiento de datos personales. Por ello, ha de destacarse que esta norma reglamentaria nace con la vocación de no reiterar los contenidos de la norma superior y de desarrollar, no sólo los mandatos contenidos en la Ley Orgánica de acuerdo con los principios que emanan de la Directiva, sino también aquellos que en estos años de vigencia de la Ley se ha demostrado que precisan de un mayor desarrollo normativo.

Por tanto, se aprueba este Reglamento partiendo de la necesidad de dotar de coherencia a la regulación reglamentaria en todo lo relacionado con la transposición de la Directiva y de desarrollar los aspectos novedosos de la Ley Orgánica 15/1999, junto con aquellos en los que la experiencia ha aconsejado un cierto de grado de precisión que dote de seguridad jurídica al sistema.

III

El reglamento viene a abarcar el ámbito tutelado anteriormente por los reales decretos 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, teniendo en cuenta la necesidad de fijar criterios aplicables a los ficheros y tratamientos de datos personales no automatizados. Por otra parte, la atribución de funciones a la Agencia Española de Protección de Datos por la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico y la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones obliga a desarrollar también los procedimientos para el ejercicio de la potestad sancionadora por la Agencia.

El reglamento se estructura en nueve títulos cuyo contenido desarrolla los aspectos esenciales en esta materia.

El título I contempla el objeto y ámbito de aplicación del reglamento. A lo largo de la vigencia de la Ley Orgánica 15/1999, se ha advertido la conveniencia de desarrollar el apartado 2 de su artículo 2 para aclarar qué se entiende por ficheros y tratamientos relacionados con actividades personales o domésticas, aspecto muy relevante dado que están excluidos de la normativa sobre protección de datos de carácter personal.

Por otra parte, el presente reglamento no contiene previsiones para los tratamientos de datos personales a los que se refiere el apartado 3 del artículo 2 de la ley orgánica, dado que se rigen por sus disposiciones específicas y por lo especialmente previsto, en su caso, por la propia Ley Orgánica 15/1999. En consecuencia, se mantiene el régimen jurídico propio de estos tratamientos y ficheros.

Además, en este título se aporta un conjunto de definiciones que ayudan al correcto entendimiento de la norma, lo que resulta particularmente necesario en un ámbito tan tecnificado como el de la protección de datos personales.

Por otra parte, fija el criterio a seguir en materia de cómputo de plazos con el fin de homogeneizar esta cuestión evitando distinciones que suponen diferencias de trato de los ficheros públicos respecto de los privados.

El título II, se refiere a los principios de la protección de datos. Reviste particular importancia la regulación del modo de captación del consentimiento atendiendo a aspectos muy específicos como el caso de los servicios de comunicaciones electrónicas y, muy particularmente, la captación de datos de los menores. Asimismo, se ofrece lo que no puede definirse sino como un estatuto del encargado del tratamiento, que sin duda contribuirá a clarificar todo lo relacionado con esta figura. Las previsiones en este ámbito se completan con lo dispuesto en el título VIII en materia de seguridad dotando de un marco coherente a la actuación del encargado.

El título III se ocupa de una cuestión tan esencial como los derechos de las personas en este ámbito. Estos derechos de acceso, rectificación, cancelación y oposición al tratamiento, según ha afirmado el Tribunal Constitucional en su sentencia número 292/2000, constituyen el haz de facultades que emanan del derecho fundamental a la protección de datos y «sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer».

A continuación, los títulos IV a VII permiten clarificar aspectos importantes para el tráfico ordinario, como la aplicación de criterios específicos a determinado tipo de ficheros de titularidad privada que por su trascendencia lo requerían –los relativos a la solvencia patrimonial y crédito y los utilizados en actividades de publicidad y prospección comercial–, el conjunto de obligaciones materiales y formales que deben conducir a los responsables a la creación e inscripción de los ficheros, los criterios y procedimientos para la realización de las transferencias internacionales de datos, y, finalmente, la regulación de un instrumento, el código tipo, llamado a jugar cada vez un papel más relevante como elemento dinamizador del derecho fundamental a la protección de datos.

El título VIII regula un aspecto esencial para la tutela del derecho fundamental a la protección de datos, la seguridad, que repercute sobre múltiples aspectos organizativos, de gestión y aún de inversión, en todas las organizaciones que traten datos personales. La repercusión del deber de seguridad obligaba a un particular rigor ya que en esta materia han confluido distintos elementos muy relevantes. Por una parte, la experiencia dimanante de la aplicación del Real Decreto 994/1999 permitía conocer las dificultades que habían enfrentado los responsables e identificar los puntos débiles y fuertes de la regulación.

Por otra, se reclamaba la adaptación de la regulación en distintos aspectos. En este sentido, el reglamento trata de ser particularmente riguroso en la atribución de los niveles de seguridad, en la fijación de las medidas que corresponda adoptar en cada caso y en la revisión de las mismas cuando ello resulte necesario. Por otra parte, ordena con mayor precisión el contenido y las obligaciones vinculadas al mantenimiento del documento de seguridad.

Además, se ha pretendido regular la materia de modo que contemple las múltiples formas de organización material y personal de la seguridad que se dan en la práctica. Por último, se regula un conjunto de medidas destinadas a los ficheros y tratamientos estructurados y no automatizados que ofrezca a los responsables un marco claro de actuación.

Finalmente en el título IX, dedicado a los procedimientos tramitados por la Agencia Española de Protección de Datos, se ha optado por normar exclusivamente aquellas especialidades que diferencian a los distintos procedimientos tramitados por la Agencia de las normas generales previstas para los procedimientos en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, cuya aplicación se declara supletoria al presente reglamento.

En su virtud, a propuesta del Ministro de Justicia, con la aprobación previa de la Ministra de Administraciones Públicas, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 21 de diciembre de 2007.

D I S P O N G O:

Artículo único. Aprobación del reglamento.

Se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal, cuyo texto se incluye a continuación.

Disposición transitoria primera. Adaptación de los códigos tipo inscritos en el Registro General de Protección de Datos.

En el plazo de un año desde la entrada en vigor del presente real decreto deberán notificarse a la Agencia Española de Protección de Datos las modificaciones que resulten necesarias en los códigos tipo inscritos en el Registro General de Protección de Datos para adaptar su contenido a lo dispuesto en el título VII del mismo.

Disposición transitoria segunda. Plazos de implantación de las medidas de seguridad.

La implantación de las medidas de seguridad previstas en el presente real decreto deberá producirse con arreglo a las siguientes reglas:

1.ª Respecto de los ficheros automatizados que existieran en la fecha de entrada en vigor del presente real decreto:

a) En el plazo de un año desde su entrada en vigor, deberán implantarse las medidas de seguridad de nivel medio exigibles a los siguientes ficheros:

   1.º Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias.

   2.º Aquéllos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

   3.º Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos, respecto de las medidas de este nivel que no fueran exigibles conforme a lo previsto en el artículo 4.4 del Reglamento de Medidas de seguridad de los ficheros automatizados de datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio.

b) En el plazo de un año desde su entrada en vigor deberán implantarse las medidas de seguridad de nivel medio y en el de dieciocho meses desde aquella fecha, las de nivel alto exigibles a los siguientes ficheros:

   1.º Aquéllos que contengan datos derivados de actos de violencia de género.

   2.º Aquéllos de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización.

c) En los demás supuestos, cuando el presente reglamento exija la implantación de una medida adicional, no prevista en el Reglamento de Medidas de seguridad de los ficheros automatizados de datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio, dicha medida deberá implantarse en el plazo de un año desde la entrada en vigor del presente real decreto.

2.ª Respecto de los ficheros no automatizados que existieran en la fecha de entrada en vigor del presente real decreto:

a) Las medidas de seguridad de nivel básico deberán implantarse en el plazo de un año desde su entrada en vigor.

b) Las medidas de seguridad de nivel medio deberán implantarse en el plazo de dieciocho meses desde su entrada en vigor.

c) Las medidas de seguridad de nivel alto deberán implantarse en el plazo de dos años desde su entrada en vigor.

3.ª Los ficheros, tanto automatizados como no automatizados, creados con posterioridad a la fecha de entrada en vigor del presente real decreto deberán tener implantadas, desde el momento de su creación la totalidad de las medidas de seguridad reguladas en el mismo.

Disposición transitoria tercera. Régimen transitorio de las solicitudes para el ejercicio de los derechos de las personas.

A las solicitudes para el ejercicio de los derechos de acceso, oposición, rectificación y cancelación que hayan sido efectuadas antes de la entrada en vigor del presente real decreto, no les será de aplicación el mismo, rigiéndose por la normativa anterior.

Disposición transitoria cuarta. Régimen transitorio de los procedimientos.

A los procedimientos ya iniciados antes de la entrada en vigor del presente real decreto, no les será de aplicación el mismo, rigiéndose por la normativa anterior.

Disposición transitoria quinta. Régimen transitorio de las actuaciones previas.

A las actuaciones previas iniciadas con anterioridad a la entrada en vigor del presente real decreto, no les será de aplicación el mismo, rigiéndose por la normativa anterior.

El presente real decreto se aplicará a las actuaciones previas que se inicien después de su entrada en vigor.

Disposición derogatoria única. Derogación normativa.

Quedan derogados el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de los datos de carácter personal, el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal y todas las normas de igual o inferior rango que contradigan o se opongan a lo dispuesto en el presente real decreto.

Disposición final primera. Título competencial.

El título I, con excepción del apartado c) del artículo 4, los títulos II, III, VII y VIII, así como los artículos 52, 53.3, 53.4, 54, 55.1, 55.3, 56, 57, 58 y 63.3 del reglamento se dictan al amparo de lo dispuesto en el artículo 149.1.1.ª de la Constitución, que atribuye al Estado la competencia exclusiva para la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales.

Disposición final segunda. Entrada en vigor.

El presente real decreto entrará en vigor a los tres meses de su íntegra publicación en el «Boletín Oficial del Estado».

Dado en Madrid, el 21 de diciembre de 2007.

JUAN CARLOS R.

El Ministro de Justicia,

MARIANO FERNÁNDEZ BERMEJO

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

TÍTULO I. Disposiciones generales

Artículo 1. Objeto.

1. El presente reglamento tiene por objeto el desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal.

2. Asimismo, el capítulo III del título IX de este reglamento desarrolla las disposiciones relativas al ejercicio por la Agencia Española de Protección de Datos de la potestad sancionadora, en aplicación de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, en el título VII de la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico, y en el título VIII de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Artículo 2. Ámbito objetivo de aplicación.

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

2. Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.

3. Asimismo, los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal.

4. Este reglamento no será de aplicación a los datos referidos a personas fallecidas. No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos.

Artículo 3. Ámbito territorial de aplicación.

1. Se regirá por el presente reglamento todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento, siempre que dicho establecimiento se encuentre ubicado en territorio español.

   Cuando no resulte de aplicación lo dispuesto en el párrafo anterior, pero exista un encargado del tratamiento ubicado en España, serán de aplicación al mismo las normas contenidas en el título VIII del presente reglamento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española, según las normas de Derecho internacional público.

c) 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.

En este supuesto, el responsable del tratamiento deberá designar un representante establecido en territorio español.

2. A los efectos previstos en los apartados anteriores, se entenderá por establecimiento, con independencia de su forma jurídica, cualquier instalación estable que permita el ejercicio efectivo y real de una actividad.

Artículo 4. Ficheros o tratamientos excluidos.

El régimen de protección de los datos de carácter personal que se establece en el presente reglamento no será de aplicación a los siguientes ficheros y tratamientos:

a) A los realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

   Sólo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares.

b) A los sometidos a la normativa sobre protección de materias clasificadas.

c) A los establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos.

Artículo 5. Definiciones.

1. A los efectos previstos en este reglamento, se entenderá por:

a) Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento.

b) Cancelación: Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.

c) Cesión o comunicación de datos: Tratamiento de datos que supone su revelación a una persona distinta del interesado.

d) Consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

e) Dato disociado: aquél que no permite la identificación de un afectado o interesado.

f) Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

g) Datos de carácter personal relacionados con la salud: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.

h) Destinatario o cesionario: la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos.

   Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

i) Encargado del tratamiento: La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

   Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

j) Exportador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero.

k) Fichero: Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

l) Ficheros de titularidad privada: los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.

m) Ficheros de titularidad pública: los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público.

n) Fichero no automatizado: todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

ñ) Importador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

o) Persona identificable: toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social.

Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

p) Procedimiento de disociación: Todo tratamiento de datos personales que permita la obtención de datos disociados.

q) Responsable del fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

r) Tercero: la persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.

Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

s) Transferencia internacional de datos: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

t) Tratamiento de datos: cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

2. En particular, en relación con lo dispuesto en el título VIII de este reglamento se entenderá por:

a) Accesos autorizados: autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.

b) Autenticación: procedimiento de comprobación de la identidad de un usuario.

c) Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.

d) Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

e) Copia de respaldo: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

f) Documento: todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.

g) Ficheros temporales: ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

h) Identificación: procedimiento de reconocimiento de la identidad de un usuario.

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

j) Perfil de usuario: accesos autorizados a un grupo de usuarios.

k) Recurso: cualquier parte componente de un sistema de información.

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

m) Sistema de información: conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.

n) Sistema de tratamiento: modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

o) Soporte: objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

p) Transmisión de documentos: cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.

q) 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.

Artículo 6. Cómputo de plazos.

En los supuestos en que este reglamento señale un plazo por días se computarán únicamente los hábiles.

Cuando el plazo sea por meses, se computarán de fecha a fecha.

Artículo 7. Fuentes accesibles al público.

1. A efectos del artículo 3, párrafo j) de la Ley Orgánica 15/1999, se entenderá que sólo tendrán el carácter de fuentes accesibles al público:

a) El censo promocional, regulado conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre.
b) Las guías de servicios de comunicaciones electrónicas, en los términos previstos por su normativa específica.
c) Las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección profesional e indicación de su pertenencia al grupo. La dirección profesional podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica. En el caso de Colegios profesionales, podrán indicarse como datos de pertenencia al grupo los de número de colegiado, fecha de incorporación y situación de ejercicio profesional.
d) Los diarios y boletines oficiales.
e) Los medios de comunicación social.

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

TÍTULO II. Principios de protección de datos

CAPÍTULO I. Calidad de los datos

Artículo 8. Principios relativos a la calidad de los datos.

1. 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.

2. Los datos de carácter personal sólo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento.

3. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

4. Sólo podrán ser objeto de tratamiento los datos que sean adecuados, pertinentes y no excesivos en relación con las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

5. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Si los datos fueran recogidos directamente del afectado, se considerarán exactos los facilitados por éste.

Si los datos de carácter personal sometidos a tratamiento resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados en el plazo de diez días desde que se tuviese conocimiento de la inexactitud, salvo que la legislación aplicable al fichero establezca un procedimiento o un plazo específico para ello.

Cuando los datos hubieran sido comunicados previamente, el responsable del fichero o tratamiento deberá notificar al cesionario, en el plazo de diez días, la rectificación o cancelación efectuada, siempre que el cesionario sea conocido.

En el plazo de diez días desde la recepción de la notificación, el cesionario que mantuviera el tratamiento de los datos, deberá proceder a la rectificación y cancelación notificada.

Esta actualización de los datos de carácter personal no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre.

Lo dispuesto en este apartado se entiende sin perjuicio de las facultades que a los afectados reconoce el título III de este reglamento.

6. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No obstante, podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado.

Una vez cumplido el período al que se refieren los párrafos anteriores, los datos sólo podrán ser conservados previa disociación de los mismos, sin perjuicio de la obligación de bloqueo prevista en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

7. Los datos de carácter personal serán tratados de forma que permitan el ejercicio del derecho de acceso, en tanto no proceda su cancelación.

Artículo 9. Tratamiento con fines estadísticos, históricos o científicos.

1. No se considerará incompatible, a los efectos previstos en el apartado 3 del artículo anterior, el tratamiento de los datos de carácter personal con fines históricos, estadísticos o científicos.

Para la determinación de los fines a los que se refiere el párrafo anterior se estará a la legislación que en cada caso resulte aplicable y, en particular, a lo dispuesto en la Ley 12/1989, de 9 de mayo, Reguladora de la función estadística pública, la Ley 16/1985, de 25 junio, del Patrimonio histórico español y la Ley 13/1986, de 14 de abril de Fomento y coordinación general de la investigación científica y técnica, y sus respectivas disposiciones de desarrollo, así como a la normativa autonómica en estas materias.

2. Por vía de excepción a lo dispuesto en el apartado 6 del artículo anterior, la Agencia Española de Protección de Datos o, en su caso, las autoridades de control de las comunidades autónomas podrán, previa solicitud del responsable del tratamiento y conforme al procedimiento establecido en la sección segunda del capítulo VII del título IX del presente reglamento, acordar el mantenimiento íntegro de determinados datos, atendidos sus valores históricos, estadísticos o científicos de acuerdo con las normas a las que se refiere el apartado anterior.

Artículo 10. Supuestos que legitiman el tratamiento o cesión de los datos.

1. Los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento para ello.

2. No obstante, será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando:

a) a) Lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los supuestos siguientes:

   El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre.

   El tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas.

b) Los datos objeto de tratamiento o de cesión figuren en fuentes accesibles al público y el responsable del fichero, o el tercero a quien se comuniquen los datos, tenga un interés legítimo para su tratamiento o conocimiento, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

   No obstante, las Administraciones públicas sólo podrán comunicar al amparo de este apartado los datos recogidos de fuentes accesibles al público a responsables de ficheros de titularidad privada cuando se encuentren autorizadas para ello por una norma con rango de ley.

3. Los datos de carácter personal podrán tratarse sin necesidad del consentimiento del interesado cuando:

a) Se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de las competencias que les atribuya una norma con rango de ley o una norma de derecho comunitario.
b) Se recaben por el responsable del tratamiento con ocasión de la celebración de un contrato o precontrato o de la existencia de una relación negocial, laboral o administrativa de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento.
c) El tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del apartado 6 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre.

4. Será posible la cesión de los datos de carácter personal sin contar con el consentimiento del interesado cuando:

a) La cesión responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control comporte la comunicación de los datos. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
b) La comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas o a las instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas y se realice en el ámbito de las funciones que la ley les atribuya expresamente.
c) La cesión entre Administraciones públicas cuando concurra uno de los siguientes supuestos:

   Tenga por objeto el tratamiento de los datos con fines históricos, estadísticos o científicos.

   Los datos de carácter personal hayan sido recogidos o elaborados por una Administración pública con destino a otra.

   La comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias.

5. Los datos especialmente protegidos podrán tratarse y cederse en los términos previstos en los artículos 7 y 8 de la Ley Orgánica 15/1999, de 13 de diciembre.

En particular, no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

Artículo 11. Verificación de datos en solicitudes formuladas a las Administraciones públicas.

Cuando se formulen solicitudes por medios electrónicos en las que el interesado declare datos personales que obren en poder de las Administraciones públicas, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la autenticidad de los datos.

CAPÍTULO II. Consentimiento para el tratamiento de los datos y deber de información

SECCIÓN 1.ª OBTENCIÓN DEL CONSENTIMIENTO DEL AFECTADO

Artículo 12. Principios generales.

1. El responsable del tratamiento deberá obtener el consentimiento del interesado para el tratamiento de sus datos de carácter personal salvo en aquellos supuestos en que el mismo no sea exigible con arreglo a lo dispuesto en las leyes.

La solicitud del consentimiento deberá ir referida a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones que concurran en el tratamiento o serie de tratamientos.

2. Cuando se solicite el consentimiento del afectado para la cesión de sus datos, éste deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y el tipo de actividad desarrollada por el cesionario. En caso contrario, el consentimiento será nulo.

3. Corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho.

Artículo 13. Consentimiento para el tratamiento de datos de menores de edad.

1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.

2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.

3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.

4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales.

Artículo 14. Forma de recabar el consentimiento.

1. El responsable del tratamiento podrá solicitar el consentimiento del interesado a través del procedimiento establecido en este artículo, salvo cuando la Ley exija al mismo la obtención del consentimiento expreso para el tratamiento de los datos.

2. El responsable podrá dirigirse al afectado, informándole en los términos previstos en los artículos 5 de la Ley Orgánica 15/1999, de 13 de diciembre y 12.2 de este reglamento y deberá concederle un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal.

En particular, cuando se trate de responsables que presten al afectado un servicio que genere información periódica o reiterada, o facturación periódica, la comunicación podrá llevarse a cabo de forma conjunta a esta información o a la facturación del servicio prestado, siempre que se realice de forma claramente visible.

3. En todo caso, será necesario que el responsable del tratamiento pueda conocer si la comunicación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

4. Deberá facilitarse al interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos. En particular, se considerará ajustado al presente reglamento los procedimientos en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento, la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.

5. Cuando se solicite el consentimiento del interesado a través del procedimiento establecido en este artículo, no será posible solicitarlo nuevamente respecto de los mismos tratamientos y para las mismas finalidades en el plazo de un año a contar de la fecha de la anterior solicitud.

Artículo 15. Solicitud del consentimiento en el marco de una relación contractual para fines no relacionados directamente con la misma.

Si el responsable del tratamiento solicitase el consentimiento del afectado durante el proceso de formación de un contrato para finalidades que no guarden relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir al afectado que manifieste expresamente su negativa al tratamiento o comunicación de datos.

En particular, se entenderá cumplido tal deber cuando se permita al afectado la marcación de una casilla claramente visible y que no se encuentre ya marcada en el documento que se le entregue para la celebración del contrato o se establezca un procedimiento equivalente que le permita manifestar su negativa al tratamiento.

Artículo 16. Tratamiento de datos de facturación y tráfico en servicios de comunicaciones electrónicas.

La solicitud del consentimiento para el tratamiento o cesión de los datos de tráfico, facturación y localización por parte de los sujetos obligados, o en su caso la revocación de aquél, según la legislación reguladora de las telecomunicaciones se someterá a lo establecido en su normativa específica y, en lo que no resulte contrario a la misma, a lo establecido en la presente sección.

Artículo 17. Revocación del consentimiento.

1. El afectado podrá revocar su consentimiento a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento.

En particular, se considerará ajustado al presente reglamento el procedimiento en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento o la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, los supuestos en que el responsable establezca como medio para que el interesado pueda manifestar su negativa al tratamiento el envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste adicional al interesado.

2. El responsable cesará en el tratamiento de los datos en el plazo máximo de diez días a contar desde el de la recepción de la revocación del consentimiento, sin perjuicio de su obligación de bloquear los datos conforme a lo dispuesto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre.

3. Cuando el interesado hubiera solicitado del responsable del tratamiento la confirmación del cese en el tratamiento de sus datos, éste deberá responder expresamente a la solicitud.

4. Si los datos hubieran sido cedidos previamente, el responsable del tratamiento, una vez revocado el consentimiento, deberá comunicarlo a los cesionarios, en el plazo previsto en el apartado 2, para que éstos, cesen en el tratamiento de los datos en caso de que aún lo mantuvieran, conforme al artículo 16.4 de la Ley Orgánica 15/1999, de 13 de diciembre.

SECCIÓN 2.ª DEBER DE INFORMACIÓN AL INTERESADO

Artículo 18. Acreditación del cumplimiento del deber de información.

1. El deber de información al que se refiere el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado.

2. El responsable del fichero o tratamiento deberá conservar el soporte en el que conste el cumplimiento del deber de informar. Para el almacenamiento de los soportes, el responsable del fichero o tratamiento podrá utilizar medios informáticos o telemáticos. En particular podrá proceder al escaneado de la documentación en soporte papel, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los soportes originales.

Artículo 19. Supuestos especiales.

En los supuestos en que se produzca una modificación del responsable del fichero como consecuencia de una operación de fusión, escisión, cesión global de activos y pasivos, aportación o transmisión de negocio o rama de actividad empresarial, o cualquier operación de reestructuración societaria de análoga naturaleza, contemplada por la normativa mercantil, no se producirá cesión de datos, sin perjuicio del cumplimiento por el responsable de lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO III. Encargado del tratamiento

Artículo 20. Relaciones entre el responsable y el encargado del tratamiento.

1. El acceso a los datos por parte de un encargado del tratamiento que resulte necesario para la prestación de un servicio al responsable no se considerará comunicación de datos, siempre y cuando se cumpla lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente capítulo.

El servicio prestado por el encargado del tratamiento podrá tener o no carácter remunerado y ser temporal o indefinido.

No obstante, se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado.

2. Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento.

3. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato al que se refiere el apartado 2 del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo.

Artículo 21. Posibilidad de subcontratación de los servicios.

1. El encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste autorización para ello. En este caso, la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento.

2. No obstante lo dispuesto en el apartado anterior, será posible la subcontratación sin necesidad de autorización siempre y cuando se cumplan los siguientes requisitos:

a) Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar.

   Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.

b) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.
c) Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior.

En este caso, el subcontratista será considerado encargado del tratamiento, siéndole de aplicación lo previsto en el artículo 20.3 de este reglamento.

3. Si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del tratamiento los extremos señalados en el apartado anterior.

Artículo 22. Conservación de los datos por el encargado del tratamiento.

1. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.

2. El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

TÍTULO III. Derechos de acceso, rectificación, cancelación y oposición

CAPÍTULO I. Disposiciones generales

Artículo 23. Carácter personalísimo.

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

2. Tales derechos se ejercitarán:

a) Por el afectado, acreditando su identidad, del modo previsto en el artículo siguiente.
b) 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.

c) 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.

Cuando el responsable del fichero sea un órgano de las Administraciones públicas o de la Administración de Justicia, podrá acreditarse la representación por cualquier medio válido en derecho que deje constancia fidedigna, o mediante declaración en comparecencia personal del interesado.

3. 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.

Artículo 24. Condiciones generales para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

1. 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.

2. Deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

3. El ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición será gratuito y en ningún caso podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar sus derechos el envío de cartas certificadas o semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado.

4. Cuando el responsable del fichero o tratamiento disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, podrá concederse la posibilidad al afectado de ejercer sus derechos de acceso, rectificación, cancelación y oposición a través de dichos servicios. 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.

5. El responsable del fichero o tratamiento deberá atender la solicitud de acceso, rectificación, cancelación u oposición ejercida por el 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, y que ésta contenga los elementos referidos en el párrafo 1 del artículo siguiente.

Artículo 25. Procedimiento.

1. Salvo en el supuesto referido en el párrafo 4 del artículo anterior, el ejercicio de los derechos deberá llevarse a cabo mediante comunicación dirigida al responsable del fichero, que contendrá:

a) Nombre y apellidos del interesado; fotocopia de su documento nacional de identidad, o de su pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación. La utilización de firma electrónica identificativa del afectado eximirá de la presentación de las fotocopias del DNI o documento equivalente.

   El párrafo anterior se entenderá sin perjuicio de la normativa específica aplicable a la comprobación de datos de identidad por las Administraciones Públicas en los procedimientos administrativos.

b) Petición en que se concreta la solicitud.

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

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

2. 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.

3. En el caso de que la solicitud no reúna los requisitos especificados en el apartado primero, el responsable del fichero deberá solicitar la subsanación de los mismos.

4. La respuesta deberá ser conforme con los requisitos previstos para cada caso en el presente título.

5. Corresponderá al responsable del tratamiento la prueba del cumplimiento del deber de respuesta al que se refiere el apartado 2, debiendo conservar la acreditación del cumplimiento del mencionado deber.

6. 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.

7. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición podrá modularse por razones de seguridad pública en los casos y con el alcance previsto en las Leyes.

8. Cuando las leyes aplicables a determinados ficheros concretos establezcan un procedimiento especial para la rectificación o cancelación de los datos contenidos en los mismos, se estará a lo dispuesto en aquéllas.

Artículo 26. Ejercicio de los derechos ante un 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.

CAPÍTULO II. Derecho de acceso

Artículo 27. Derecho de acceso.

1. 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.

2. 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.

3. 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.

Artículo 28. Ejercicio del derecho de acceso.

1. 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:

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

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

2. Los sistemas de consulta del fichero previstos en el apartado anterior 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.

3. El responsable del fichero deberá cumplir al facilitar el acceso lo establecido en el Título VIII de este Reglamento. Si tal responsable ofreciera un determinado sistema para hacer efectivo el derecho de acceso y el afectado lo rechazase, aquél no responderá por los posibles riesgos que para la seguridad de la información pudieran derivarse de la elección.

Del mismo modo, si el responsable ofreciera 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.

Artículo 29. Otorgamiento del acceso.

1. El responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición de acceso, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

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

2. Si la solicitud fuera estimada y el responsable no acompañase a su comunicación la información a la que se refiere el artículo 27.1, el acceso se hará efectivo durante los diez días siguientes a dicha comunicación.

3. 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.

Artículo 30. Denegación del acceso.

1. El responsable del fichero o tratamiento 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.

2. Podrá también 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.

3. En todo caso, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO III. Derechos de rectificación y cancelación

Artículo 31. Derechos de rectificación y cancelación.

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

2. El ejercicio del derecho de cancelación dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo conforme a este reglamento.

En los supuestos en que el interesado invoque el ejercicio del derecho de cancelación para revocar el consentimiento previamente prestado, se estará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente reglamento.

Artículo 32. Ejercicio de los derechos de rectificación y cancelación.

1. 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.

2. 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. Transcurrido el plazo sin que de forma expresa se responda a la petición, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

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

3. 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 Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 33. Denegación de los derechos de rectificación y cancelación.

1. 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.

2. 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.

3. En todo caso, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las Comunidades Autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO IV. Derecho de oposición

Artículo 34. Derecho de oposición.

El 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:

a) 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.
b) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, en los términos previstos en el artículo 51 de este reglamento, cualquiera que sea la empresa responsable de su creación.

c) 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, en los términos previstos en el artículo 36 de este reglamento.

Artículo 35. Ejercicio del derecho de oposición.

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

Cuando la oposición se realice con base en la letra a) del artículo anterior, en la solicitud deberán hacerse constar los motivos fundados y legítimos, relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho.

2. 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. Transcurrido el plazo sin que de forma expresa se responda a la petición, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

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

3. 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 previsto en el apartado 2 de este artículo.

Artículo 36. Derecho de oposición a las decisiones basadas únicamente en un tratamiento automatizado de datos.

1. 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.

2. No obstante, los afectados podrán verse sometidos a una de las decisiones contempladas en el apartado 1 cuando dicha decisión:

a) 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 informar previamente al afectado, de forma clara y precisa, de que se adoptarán decisiones con las características señaladas en el apartado 1 y cancelará los datos en caso de que no llegue a celebrarse finalmente el contrato.

b) Esté autorizada por una norma con rango de Ley que establezca medidas que garanticen el interés legítimo del interesado.

TÍTULO IV. Disposiciones aplicables a determinados ficheros de titularidad privada

CAPÍTULO I. Ficheros de información sobre solvencia patrimonial y crédito

SECCIÓN 1. ª DISPOSICIONES GENERALES

Artículo 37. Régimen aplicable.

1. El tratamiento de datos de carácter personal sobre solvencia patrimonial y crédito, previsto en el apartado 1 del artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre, se someterá a lo establecido, con carácter general, en dicha ley orgánica y en el presente reglamento.

2. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición en el caso de los ficheros a que se refiere el apartado anterior, se rige por lo dispuesto en los capítulos I a IV del título III del presente reglamento, con los siguientes criterios:

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

3. De conformidad con el apartado 2 del artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre, también podrán tratarse los datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés.

Estos datos deberán conservarse en ficheros creados con la exclusiva finalidad de facilitar información crediticia del afectado y su tratamiento se regirá por lo dispuesto en el presente reglamento y, en particular, por las previsiones contenidas en la sección segunda de este capítulo.

SECCIÓN 2.ª TRATAMIENTO DE DATOS RELATIVOS AL CUMPLIMIENTO O INCUMPLIMIENTO DE OBLIGACIONES DINERARIAS FACILITADOS POR EL ACREEDOR O POR QUIEN ACTÚE POR SU CUENTA O INTERÉS

Artículo 38. Requisitos para la inclusión de los datos.

1. Sólo será posible la inclusión en estos ficheros de datos de carácter personal que sean determinantes para enjuiciar la solvencia económica del afectado, siempre que concurran los siguientes requisitos:

a) Existencia previa de una deuda cierta, vencida, exigible, que haya resultado impagada y respecto de la cual no se haya entablado reclamación judicial, arbitral o administrativa, o tratándose de servicios financieros, no se haya planteado una reclamación en los términos previstos en el Reglamento de los Comisionados para la defensa del cliente de servicios financieros, aprobado por Real Decreto 303/2004, de 20 de febrero.
b) 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.
c) Requerimiento previo de pago a quien corresponda el cumplimiento de la obligación.

2. No podrán incluirse en los ficheros de esta naturaleza datos personales sobre los que exista un principio de prueba que de forma indiciaria contradiga alguno de los requisitos anteriores.

Tal circunstancia determinará asimismo la cancelación cautelar del dato personal desfavorable en los supuestos en que ya se hubiera efectuado su inclusión en el fichero.

3. 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 en este artículo y del requerimiento previo al que se refiere el artículo siguiente.

Artículo 39. Información previa a la inclusión.

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 al que se refiere la letra c) del apartado 1 del artículo anterior, que en caso de no producirse el pago en el término previsto para ello y cumplirse los requisitos previstos en el citado artículo, los datos relativos al impago podrán ser comunicados a ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias.

Artículo 40. Notificación de inclusión.

1. 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 Ley Orgánica 15/1999, de 13 de diciembre.

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

3. 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.

4. 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.

5. 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.

Artículo 41. Conservación de los datos.

1. 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.

2. 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.

Artículo 42. Acceso a la información contenida en el fichero.

1. 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:

a) Que el afectado mantenga con el tercero algún tipo de relación contractual que aún no se encuentre vencida.
b) Que el afectado pretenda celebrar con el tercero un contrato que implique el pago aplazado del precio.
c) Que el afectado pretenda contratar con el tercero la prestación de un servicio de facturación periódica.

2. Los terceros deberán informar por escrito a las personas en las que concurran los supuestos contemplados en las letras b) y c) precedentes de su derecho a consultar el fichero.

En los supuestos de contratación telefónica de los productos o servicios a los que se refiere el párrafo anterior, la información podrá realizarse de forma no escrita, correspondiendo al tercero la prueba del cumplimiento del deber de informar.

Artículo 43. Responsabilidad.

1. El acreedor o quien actúe por su cuenta o interés deberá asegurarse que concurren todos los requisitos exigidos en los artículos 38 y 39 en el momento de notificar los datos adversos al responsable del fichero común.

2. El acreedor o quien actúe por su cuenta o interés será responsable de la inexistencia o inexactitud de los datos que hubiera facilitado para su inclusión en el fichero, en los términos previstos en la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 44. Ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

1. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición se rige por lo dispuesto en los capítulos I a IV del título III de este reglamento, sin perjuicio de lo señalado en el presente artículo.

2. Cuando el interesado ejercite su derecho de acceso en relación con la inclusión de sus datos en un fichero regulado por el artículo 29.2 de la Ley Orgánica 15/1999, de 13 de diciembre, se tendrán en cuenta las siguientes reglas:

1.ª 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.

2.ª 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.

3. Cuando el interesado ejercite sus derechos de rectificación o cancelación en relación con la inclusión de sus datos en un fichero regulado por el artículo 29.2 de la Ley Orgánica 15/1999, de 13 de diciembre, se tendrán en cuenta las siguientes reglas:

1.ª Si la solicitud se dirige al titular del fichero común, éste tomará las medidas oportunas para trasladar dicha solicitud a la entidad que haya facilitado los datos, para que ésta la resuelva. En el caso de que el responsable del fichero común no haya recibido contestación por parte de la entidad en el plazo de siete días, procederá a la rectificación o cancelación cautelar de los mismos.

2.ª Si la solicitud se dirige a quien haya facilitado los datos al fichero común procederá a la rectificación o cancelación de los mismos en sus ficheros y a notificarlo al titular del fichero común en el plazo de diez días, dando asimismo respuesta al interesado en los términos previstos en el artículo 33 de este reglamento.

3.ª Si la solicitud se dirige a otra entidad participante en el sistema, que no hubiera facilitado al fichero común los datos, dicha entidad informará al afectado sobre este hecho en el plazo máximo de diez días, proporcionándole, además, la identidad y dirección del titular del fichero común para, que en su caso, puedan ejercitar sus derechos ante el mismo.

CAPÍTULO II. Tratamientos para actividades de publicidad y prospección comercial

Artículo 45. Datos susceptibles de tratamiento e información al interesado.

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

a) Figuren en alguna de las fuentes accesibles al público a las que se refiere la letra j) del artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre y el artículo 7 de este reglamento 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.

b) 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.

2. 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 y de la identidad del responsable del tratamiento así como de los derechos que le asisten, con indicación de ante quién podrán ejercitarse.

A tal efecto, el interesado deberá ser informado de que sus datos han sido obtenidos de fuentes accesibles al público y de la entidad de la que hubieran sido obtenidos.

Artículo 46. Tratamiento de datos en campañas publicitarias.

1. Para que una entidad pueda realizar por sí misma una actividad publicitaria de sus productos o servicios entre sus clientes será preciso que el tratamiento se ampare en alguno de los supuestos contemplados en el artículo 6 de la Ley Orgánica 15/1999, de 13 de diciembre.

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

a) 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.
b) Cuando los parámetros fueran determinados únicamente por la entidad o entidades contratadas, dichas entidades serán las responsable del tratamiento.
c) Cuando en la determinación de los parámetros intervengan ambas entidades, serán ambas responsables del tratamiento.

3. En el supuesto contemplado en el apartado anterior, la entidad que encargue la realización de la campaña publicitaria deberá adoptar las medidas necesarias para asegurarse de que la entidad contratada ha recabado los datos cumpliendo las exigencias establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

4. A los efectos previstos en este artículo, se consideran parámetros identificativos de los destinatarios las variables utilizadas para identificar el público objetivo o destinatario de una campaña o promoción comercial de productos o servicios que permitan acotar los destinatarios individuales de la misma.

Artículo 47. Depuración de datos personales.

Cuando dos o más responsables por sí mismos o mediante encargo a terceros pretendieran constatar sin consentimiento de los afectados, con fines de promoción o comercialización de sus productos o servicios y mediante un tratamiento cruzado de sus ficheros quiénes ostentan la condición de clientes de una u otra o de varios de ellos, el tratamiento así realizado constituirá una cesión o comunicación de datos.

Artículo 48. Ficheros de exclusión del envío de comunicaciones comerciales.

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

Artículo 49. Ficheros comunes de exclusión del envío de comunicaciones comerciales.

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

A tal efecto, los citados ficheros podrán contener los mínimos datos imprescindibles para identificar al afectado.

2. Cuando el afectado manifieste ante un concreto responsable su negativa u oposición a que sus datos sean tratados con fines de publicidad o prospección comercial, aquél deberá ser informado de la existencia de los ficheros comunes de exclusión generales o sectoriales, así como de la identidad de su responsable, su domicilio y la finalidad del tratamiento.

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

3. La entidad responsable del fichero común podrá tratar los datos de los interesados que hubieran manifestado su negativa u oposición al tratamiento de sus datos con fines de publicidad o prospección comercial, cumpliendo las restantes obligaciones establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento.

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

Artículo 50. Derechos de acceso, rectificación y cancelación.

1. El ejercicio de los derechos de acceso, rectificación y cancelación en relación con los tratamientos vinculados a actividades de publicidad y prospección comercial se someterá a lo previsto en los capítulos I a IV del título III de este reglamento.

2. 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.

Lo dispuesto en el párrafo anterior se entenderá sin perjuicio del deber impuesto a la entidad mencionada en el apartado anterior, en todo caso, por el párrafo segundo del artículo 5.5 de la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 51. Derecho de oposición.

1. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

La oposición a la que se refiere el párrafo anterior deberá entenderse sin perjuicio del derecho del interesado a revocar cuando lo estimase oportuno el consentimiento que hubiera otorgado, en su caso, para el tratamiento de los datos.

2. A tal efecto, deberá concederse al interesado un medio sencillo y gratuito para oponerse al tratamiento. En particular, se considerará cumplido lo dispuesto en este precepto cuando los derechos puedan ejercitarse mediante la llamada a un número telefónico gratuito o la remisión de un correo electrónico.

3. Cuando el responsable del fichero o tratamiento disponga de servicios de cualquier índole para la atención a sus clientes o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, deberá concederse la posibilidad al afectado de ejercer su oposición a través de dichos servicios.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar su oposición el envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado.

En todo caso, el ejercicio por el afectado de sus derechos no podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.

4. 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.

Lo dispuesto en el párrafo anterior se entenderá sin perjuicio del deber impuesto a la entidad mencionada en el apartado anterior, en todo caso, por el párrafo segundo del artículo 5.5 de la Ley Orgánica 15/1999, de 13 de diciembre.

TÍTULO V. Obligaciones previas al tratamiento de los datos

CAPÍTULO I. Creación, modificación o supresión de ficheros de titularidad pública

Artículo 52. Disposición o Acuerdo de creación, modificación o supresión del fichero.

1. La creación, modificación o supresión de los ficheros de titularidad pública sólo podrá hacerse por medio de disposición general o acuerdo publicados en el «Boletín Oficial del Estado» o diario oficial correspondiente.

2. En todo caso, la disposición o acuerdo deberá dictarse y publicarse con carácter previo a la creación, modificación o supresión del fichero.

Artículo 53. Forma de la disposición o acuerdo.

1. Cuando la disposición se refiera a los órganos de la Administración General del Estado o a las entidades u organismos vinculados o dependientes de la misma, deberá revestir la forma de orden ministerial o resolución del titular de la entidad u organismo correspondiente.

2. En el caso de los órganos constitucionales del Estado, se estará a lo que establezcan sus normas reguladoras.

3. En relación con los ficheros de los que sean responsables las comunidades autónomas, entidades locales y las entidades u organismos vinculados o dependientes de las mismas, las universidades públicas, así como los órganos de las comunidades autónomas con funciones análogas a los órganos constitucionales del Estado, se estará a su legislación específica.

4. La creación, modificación o supresión de los ficheros de los que sean responsables las corporaciones de derecho público y que se encuentren relacionados con el ejercicio por aquéllas de potestades de derecho público deberá efectuarse a través de acuerdo de sus órganos de gobierno, en los términos que establezcan sus respectivos Estatutos, debiendo ser igualmente objeto de publicación en el «Boletín Oficial del Estado» o diario oficial correspondiente.

Artículo 54. Contenido de la disposición o acuerdo.

1. La disposición o acuerdo de creación del fichero deberá contener los siguientes extremos:

a) La identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos.
b) El origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia.
c) La estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización.
d) Las comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios.
e) Las transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos.
f) Los órganos responsables del fichero.
g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
h) El nivel básico, medio o alto de seguridad que resulte exigible, de acuerdo con lo establecido en el título VIII del presente reglamento.

2. La disposición o acuerdo de modificación del fichero deberá indicar las modificaciones producidas en cualquiera de los extremos a los que se refiere el apartado anterior.

3. En las disposiciones o acuerdos que se dicten para la supresión de los ficheros se establecerá el destino que vaya a darse a los datos o, en su caso, las previsiones que se adopten para su destrucción.

CAPÍTULO II. Notificación e inscripción de los ficheros de titularidad pública o privada

Artículo 55. Notificación de ficheros.

1. Todo fichero de datos de carácter personal de titularidad pública será notificado a la Agencia Española de Protección de Datos por el órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, en el plazo de treinta días desde la publicación de su norma o acuerdo de creación en el diario oficial correspondiente.

2. Los ficheros de datos de carácter personal de titularidad privada serán notificados a la Agencia Española de Protección de Datos por la persona o entidad privada que pretenda crearlos, con carácter previo a su creación. 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.

3. Cuando la obligación de notificar afecte a ficheros sujetos a la competencia de la autoridad de control de una comunidad autónoma que haya creado su propio registro de ficheros, la notificación se realizará a la autoridad autonómica competente, que dará traslado de la inscripción al Registro General de Protección de Datos.

El Registro General de Protección de Datos podrá solicitar de las autoridades de control de las comunidades autónomas el traslado al que se refiere el párrafo anterior, procediendo, en su defecto, a la inclusión de oficio del fichero en el Registro.

4. La notificación se realizará conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente reglamento.

Artículo 56. Tratamiento de datos en distintos soportes.

1. La notificación de un fichero de datos de carácter personal es independiente del sistema de tratamiento empleado en su organización y del soporte o soportes empleados para el tratamiento de los datos.

2. Cuando los datos de carácter personal objeto de un tratamiento estén almacenados en diferentes soportes, automatizados y no automatizados o exista una copia en soporte no automatizado de un fichero automatizado sólo será precisa una sola notificación, referida a dicho fichero.

Artículo 57. Ficheros en los que exista más de un responsable.

Cuando se tenga previsto crear un fichero del que resulten responsables varias personas o entidades simultáneamente, cada una de ellas deberá notificar, a fin de proceder a su inscripción en el Registro General de Protección de Datos y, en su caso, en los Registros de Ficheros creados por las autoridades de control de las comunidades autónomas, la creación del correspondiente fichero.

Artículo 58. Notificación de la modificación o supresión de ficheros.

1. La inscripción del fichero deberá encontrarse actualizada en todo momento. Cualquier modificación que afecte al contenido de la inscripción de un fichero deberá ser previamente notificada a la Agencia Española de Protección de Datos o a las autoridades de control autonómicas competentes, a fin de proceder a su inscripción en el registro correspondiente, conforme a lo dispuesto en el artículo 55.

2. Cuando el responsable del fichero decida su supresión, deberá notificarla a efectos de que se proceda a la cancelación de la inscripción en el registro correspondiente.

3. Tratándose de ficheros de titularidad pública, cuando se pretenda la modificación que afecte a alguno de los requisitos previstos en el artículo 55 o la supresión del fichero deberá haberse adoptado, con carácter previo a la notificación la correspondiente norma o acuerdo en los términos previstos en el capítulo I de este título.

Artículo 59. Modelos y soportes para la notificación.

1. La Agencia Española de Protección de Datos publicará mediante la correspondiente Resolución del Director los modelos o formularios electrónicos de notificación de creación, modificación o supresión de ficheros, que permitan su presentación a través de medios telemáticos o en soporte papel, así como, previa consulta de las autoridades de protección de datos de las comunidades autónomas, los formatos para la comunicación telemática de ficheros públicos por las autoridades de control autonómicas, de conformidad con lo establecido en los artículos 55 y 58 del presente reglamento.

2. Los modelos o formularios electrónicos de notificación se podrán obtener gratuitamente en la página web de la Agencia Española de Protección de Datos.

3. El Director de la Agencia Española de Protección de Datos podrá establecer procedimientos simplificados de notificación en atención a las circunstancias que concurran en el tratamiento o el tipo de fichero al que se refiera la notificación.

Artículo 60. Inscripción de los ficheros.

1. El Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, dictará resolución acordando, en su caso, la inscripción, una vez tramitado el procedimiento previsto en el capítulo IV del título IX.

2. La inscripción contendrá el código asignado por el Registro, la identificación del responsable del fichero, la identificación del fichero o tratamiento, la descripción de su finalidad y usos previstos, el sistema de tratamiento empleado en su organización, en su caso, 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, y la indicación del nivel de medidas de seguridad exigible conforme a lo dispuesto en el artículo 81.

Asimismo, se incluirán, en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales.

En el caso de ficheros de titularidad pública también se hará constar la referencia de la disposición general por la que ha sido creado, y en su caso, modificado.

3. La inscripción de un fichero en el Registro General de Protección de Datos, no exime al responsable del cumplimiento del resto de las obligaciones previstas en la Ley Orgánica 15/1999, de 13 de diciembre, y demás disposiciones reglamentarias.

Artículo 61. Cancelación de la inscripción.

1. Cuando el responsable del tratamiento comunicase, en virtud de lo dispuesto en el artículo 58 de este reglamento, la supresión del fichero, el Director de la Agencia Española de Protección de Datos, previa la tramitación del procedimiento establecido en la sección primera del capítulo IV del título IX, dictará resolución acordando la cancelación de la inscripción correspondiente al fichero.

2. El Director de la Agencia Española de Protección de Datos podrá, en ejercicio de sus competencias, acordar de oficio la cancelación de la inscripción de un fichero cuando concurran circunstancias que acrediten la imposibilidad de su existencia, previa la tramitación del procedimiento establecido en la sección segunda del capítulo IV del título IX de este reglamento.

Artículo 62. Rectificación de errores.

El Registro General de Protección de Datos podrá rectificar en cualquier momento, de oficio o a instancia de los interesados, los errores materiales, de hecho o aritméticos que pudieran existir en las inscripciones, de conformidad con lo dispuesto en el artículo 105 de la Ley 30/1992, de 26 de noviembre.

Artículo 63. Inscripción de oficio de ficheros de titularidad pública.

1. En supuestos excepcionales con el fin de garantizar el derecho a la protección de datos de los afectados, y sin perjuicio de la obligación de notificación, se podrá proceder a la inscripción de oficio de un determinado fichero en el Registro General de Protección de Datos.

2. Para que lo dispuesto en el apartado anterior resulte de aplicación, será requisito indispensable que la correspondiente norma o acuerdo regulador de los ficheros que contengan datos de carácter personal haya sido publicado en el correspondiente diario oficial y cumpla los requisitos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.

3. El Director de la Agencia Española de Protección de Datos podrá, a propuesta del Registro General de Protección de Datos, acordar la inscripción del fichero de titularidad pública en el Registro, notificándose dicho acuerdo al órgano responsable del fichero.

Cuando la inscripción se refiera a ficheros sujetos a la competencia de la autoridad de control de una comunidad autónoma que haya creado su propio registro de ficheros, se comunicará a la referida autoridad de control autonómica para que proceda, en su caso, a la inscripción de oficio.

Artículo 64. Colaboración con las autoridades de control de las comunidades autónomas.

El Director de la Agencia Española de Protección de Datos podrá celebrar con los directores de las autoridades de control de las comunidades autónomas los convenios de colaboración o acuerdos que estime pertinentes, a fin de garantizar la inscripción en el Registro General de Protección de Datos de los ficheros sometidos a la competencia de dichas autoridades autonómicas.

TÍTULO VI. Transferencias internacionales de datos

CAPÍTULO I. Disposiciones generales

Artículo 65. Cumplimiento de las disposiciones de la Ley Orgánica 15/1999, de 13 de diciembre.

La transferencia internacional de datos no excluye en ningún caso la aplicación de las disposiciones contenidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

Artículo 66. Autorización y notificación.

1. Para que la transferencia internacional de datos pueda considerarse conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento será necesaria la autorización del Director de la Agencia Española de Protección de Datos, que se otorgará en caso de que el exportador aporte las garantías a las que se refiere el artículo 70 del presente reglamento.

La autorización se otorgará conforme al procedimiento establecido en la sección primera del capítulo V del título IX de este reglamento.

2. La autorización no será necesaria:

a) Cuando el Estado en el que se encontrase el importador ofrezca un nivel adecuado de protección conforme a lo previsto en el capítulo II de este título.
b) Cuando la transferencia se encuentre en uno de los supuestos contemplados en los apartados a) a j) del artículo 34 de la Ley Orgánica 15/1999, de 13 de diciembre.

3. 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, conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente reglamento.

CAPÍTULO II. Transferencias a estados que proporcionen un nivel adecuado de protección

Artículo 67. Nivel adecuado de protección acordado por la Agencia Española de Protección de Datos.

1. No será precisa autorización del Director de la Agencia Española de Protección de Datos a una transferencia internacional de datos cuando las normas aplicables al Estado en que se encontrase el importador ofrezcan dicho nivel adecuado de protección a juicio del Director de la Agencia Española de Protección de Datos.

El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Las resoluciones del Director de la Agencia Española de Protección de Datos por las que se acordase que un determinado país proporciona un nivel adecuado de protección de datos serán publicadas en el «Boletín Oficial del Estado».

2. El Director de la Agencia Española de Protección de Datos acordará la publicación de la relación de países cuyo nivel de protección haya sido considerado equiparable conforme a lo dispuesto en el apartado anterior.

Esta lista se publicará y mantendrá actualizada asimismo a través de medios informáticos o telemáticos.

Artículo 68. Nivel adecuado de protección declarado por Decisión de la Comisión Europea.

No será necesaria la autorización del Director de la Agencia Española de Protección de Datos para la realización de una transferencia internacional de datos que tuvieran por importador una persona o entidad, pública o privada, situada en el territorio de un Estado respecto del que se haya declarado por la Comisión Europea la existencia de un nivel adecuado de protección.

Artículo 69. Suspensión temporal de las transferencias.

1. En los supuestos previstos en los artículos precedentes, el Director de la Agencia Española de Protección de Datos, en uso de la potestad que le otorga el artículo 37.1 f) de la Ley Orgánica 15/1999, de 13 de diciembre, podrá acordar, previa audiencia del exportador, la suspensión temporal de la transferencia de datos hacia un importador ubicado en un tercer Estado del que se haya declarado la existencia de un nivel adecuado de protección, cuando concurra alguna de las circunstancias siguientes:

a) Que las autoridades de Protección de Datos del Estado importador o cualquier otra competente, en caso de no existir las primeras, resuelvan que el importador ha vulnerado las normas de protección de datos establecidas en su derecho interno.
b) Que existan indicios racionales de que se estén vulnerando las normas o, en su caso, los principios de protección de datos por la entidad importadora de la transferencia y que las autoridades competentes en el Estado en que se encuentre el importador no han adoptado o no van a adoptar en el futuro las medidas oportunas para resolver el caso en cuestión, habiendo sido advertidas de la situación por la Agencia Española de Protección de Datos. En este caso se podrá suspender la transferencia cuando su continuación pudiera generar un riesgo inminente de grave perjuicio a los afectados.

2. La suspensión se acordará previa la tramitación del procedimiento establecido en la sección segunda del capítulo V del título IX del presente reglamento.

En estos casos, la decisión del Director de la Agencia Española de Protección de Datos será notificada a la Comisión Europea.

CAPÍTULO III. Transferencias a Estados que no proporcionen un nivel adecuado de protección

Artículo 70. Transferencias sujetas a autorización del Director de la Agencia Española de Protección de Datos.

1. 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 de la transferencia se tramitará conforme al procedimiento establecido en la sección primera del capítulo V del título IX del presente reglamento.

2. 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.

A tal efecto, se considerará que establecen las adecuadas garantías los contratos que se celebren de acuerdo con lo previsto en las Decisiones de la Comisión Europea 2001/497/CE, de 15 de Junio de 2001, 2002/16/CE, de 27 de diciembre de 2001, y 2004/915/CE, de 27 de diciembre de 2004 o de lo que dispongan las Decisiones de la Comisión que den cumplimiento a lo establecido en el artículo 26.4 de la Directiva 95/46/CE.

3. En el supuesto contemplado en el apartado anterior, el Director de la Agencia Española de Protección de Datos podrá denegar o, en uso de la potestad que le otorga el artículo 37.1 f) de la Ley Orgánica 15/1999, de 13 de diciembre, suspender temporalmente, previa audiencia del exportador, la transferencia, cuando concurra alguna de las circunstancias siguientes:

a) 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.
b) Que la entidad destinataria haya incumplido previamente las garantías establecidas en cláusulas contractuales de este tipo.
c) Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el importador.
d) Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos.
e) Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una situación de riesgo de daño efectivo a los afectados.

La suspensión se acordará previa la tramitación del procedimiento establecido en la sección segunda del capítulo V del título IX del presente reglamento.

Las resoluciones del Director de la Agencia Española de Protección de Datos por las que se deniegue o suspenda una transferencia internacional de datos en virtud de las causas a las que se refiere este apartado serán notificadas a la Comisión de las Comunidades Europeas cuando así sea exigible.

4. También podrá otorgarse la autorización para la transferencia internacional de datos en el seno de grupos multinacionales de empresas cuando hubiesen sido adoptados por los mismos normas o reglas internas en que consten las necesarias garantías de respeto a la protección de la vida privada y el derecho fundamental a la protección de datos de los afectados y se garantice asimismo el cumplimiento de los principios y el ejercicio de los derechos reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.

En este caso, para que proceda la autorización del Director de la Agencia Española de Protección de Datos será preciso que las normas o reglas resulten vinculantes para las empresas del Grupo y exigibles conforme al ordenamiento jurídico español.

En todo caso, la autorización del Director de la Agencia Española de Protección de Datos implicará la exigibilidad de lo previsto en las normas o reglas internas tanto por la Agencia como por los afectados cuyos datos hubieran sido objeto de tratamiento.

TÍTULO VII. Códigos tipo

Artículo 71. Objeto y naturaleza.

1. Los códigos tipo a los que se refiere el artículo 32 de la Ley Orgánica 15/1999, de 13 de diciembre, tienen por objeto adecuar lo establecido en la citada Ley Orgánica y en el presente reglamento a las peculiaridades de los tratamientos efectuados por quienes se adhieren a los mismos.

A tal efecto, contendrán reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos, facilitar el ejercicio de los derechos de los afectados y favorecer el cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.

2. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional y serán vinculantes para quienes se adhieran a los mismos.

Artículo 72. Iniciativa y ámbito de aplicación.

1. Los códigos tipo tendrán carácter voluntario.

2. Los códigos tipo de carácter sectorial podrán referirse a la totalidad o a parte de los tratamientos llevados a cabo por entidades pertenecientes a un mismo sector, debiendo ser formulados por organizaciones representativas de dicho sector, al menos en su ámbito territorial de aplicación, y sin perjuicio de la potestad de dichas entidades de ajustar el código tipo a sus peculiaridades.

3. Los códigos tipo promovidos por una empresa deberán referirse a la totalidad de los tratamientos llevados a cabo por la misma.

4. Las Administraciones públicas y las corporaciones de Derecho Público podrán adoptar códigos tipo de acuerdo con lo establecido en las normas que les sean aplicables.

Artículo 73. Contenido.

1. Los códigos tipo deberán estar redactados en términos claros y accesibles.

2. Los códigos tipo deben respetar la normativa vigente e incluir, como mínimo, con suficiente grado de precisión:

a) La delimitación clara y precisa de su ámbito de aplicación, las actividades a que el código se refiere y los tratamientos sometidos al mismo.
b) Las previsiones específicas para la aplicación de los principios de protección de datos.
c) El establecimiento de estándares homogéneos para el cumplimiento por los adheridos al código de las obligaciones establecidas en la Ley Orgánica 15/1999, de 13 de diciembre.
d) El establecimiento de procedimientos que faciliten el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición.
e) La determinación de las cesiones y transferencias internacionales de datos que, en su caso, se prevean, con indicación de las garantías que deban adoptarse.
f) Las acciones formativas en materia de protección de datos dirigidas a quienes los traten, especialmente en cuanto a su relación con los afectados.
g) Los mecanismos de supervisión a través de los cuales se garantice el cumplimiento por los adheridos de lo establecido en el código tipo, en los términos previstos en el artículo 74 de este reglamento.

3. En particular, deberán contenerse en el código:

a) Cláusulas tipo para la obtención del consentimiento de los afectados al tratamiento o cesión de sus datos.
b) Cláusulas tipo para informar a los afectados del tratamiento, cuando los datos no sean obtenidos de los mismos.
c) Modelos para el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición.
d) Modelos de cláusulas para el cumplimiento de los requisitos formales exigibles para la contratación de un encargado del tratamiento, en su caso.

Artículo 74. Compromisos adicionales.

1. Los códigos tipo podrán incluir cualquier otro compromiso adicional que asuman los adheridos para un mejor cumplimiento de la legislación vigente en materia de protección de datos.

2. Además podrán contener cualquier otro compromiso que puedan establecer las entidades promotoras y, en particular, sobre:

a) La adopción de medidas de seguridad adicionales a las exigidas por la Ley Orgánica 15/1999, de 13 de diciembre, y el presente Reglamento.
b) La identificación de las categorías de cesionarios o importadores de los datos.
c) Las medidas concretas adoptadas en materia de protección de los menores o de determinados colectivos de afectados.
d) El establecimiento de un sello de calidad que identifique a los adheridos al código.

Artículo 75. Garantías del cumplimiento de los códigos tipo.

1. Los códigos tipo deberán incluir procedimientos de supervisión independientes para garantizar el cumplimiento de las obligaciones asumidas por los adheridos, y establecer un régimen sancionador adecuado, eficaz y disuasorio.

2. El procedimiento que se prevea deberá garantizar:

a) La independencia e imparcialidad del órgano responsable de la supervisión.
b) La sencillez, accesibilidad, celeridad y gratuidad para la presentación de quejas y reclamaciones ante dicho órgano por los eventuales incumplimientos del código tipo.
c) El principio de contradicción.
d) Una graduación de sanciones que permita ajustarlas a la gravedad del incumplimiento. Esas sanciones deberán ser disuasorias y podrán implicar la suspensión de la adhesión al código o la expulsión de la entidad adherida. Asimismo, podrá establecerse, en su caso, su publicidad.
e) La notificación al afectado de la decisión adoptada.

3. Asimismo, y sin perjuicio de lo dispuesto en el artículo 19 de la Ley Orgánica 15/1999, de 13 de diciembre, los códigos tipo podrán contemplar procedimientos para la determinación de medidas reparadoras en caso de haberse causado un perjuicio a los afectados como consecuencia del incumplimiento del código tipo.

4. Lo dispuesto en este artículo se aplicará sin perjuicio de las competencias de la Agencia Española de Protección de Datos y, en su caso, de las autoridades de control de las comunidades autónomas.

Artículo 76. Relación de adheridos.

El código tipo deberá incorporar como anexo una relación de adheridos, que deberá mantenerse actualizada, a disposición de la Agencia Española de Protección de Datos.

Artículo 77. Depósito y publicidad de los códigos tipo.

1. Para que los códigos tipo puedan ser considerados como tales a los efectos previstos en el artículo 32 de la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento, deberán ser depositados e inscritos en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos o, cuando corresponda, en el registro que fuera creado por las comunidades autónomas, que darán traslado para su inclusión al Registro General de Protección de Datos.

2. A tal efecto, los códigos tipo deberán ser presentados ante la correspondiente autoridad de control, tramitándose su inscripción, en caso de estar sometidos a la decisión de la Agencia Española de Protección de Datos, conforme al procedimiento establecido en el capítulo VI del título IX de este reglamento.

3. En todo caso, la Agencia Española de Protección de Datos dará publicidad a los códigos tipo inscritos, preferentemente a través de medios informáticos o telemáticos.

Artículo 78. Obligaciones posteriores a la inscripción del código tipo.

Las entidades promotoras o los órganos, personas o entidades que al efecto se designen en el propio código tipo tendrán, una vez el mismo haya sido publicado, las siguientes obligaciones:

a) Mantener accesible al público la información actualizada sobre las entidades promotoras, el contenido del código tipo, los procedimientos de adhesión y de garantía de su cumplimiento y la relación de adheridos a la que se refiere el artículo anterior.

   Esta información deberá presentarse de forma concisa y clara y estar permanentemente accesible por medios electrónicos.

b) Remitir a la Agencia Española de Protección de Datos una memoria anual sobre las actividades realizadas para difundir el código tipo y promover la adhesión a éste, las actuaciones de verificación del cumplimiento del código y sus resultados, las quejas y reclamaciones tramitadas y el curso que se les hubiera dado y cualquier otro aspecto que las entidades promotoras consideren adecuado destacar.

   Cuando se trate de códigos tipo inscritos en el registro de una autoridad de control de una comunidad autónoma, la remisión se realizará a dicha autoridad, que dará traslado al registro General de Protección de Datos.

c) Evaluar periódicamente la eficacia del código tipo, midiendo el grado de satisfacción de los afectados y, en su caso, actualizar su contenido para adaptarlo a la normativa general o sectorial de protección de datos existente en cada momento.

   Esta evaluación deberá tener lugar, al menos, cada cuatro años, salvo que sea precisa la adaptación de los compromisos del código a la modificación de la normativa aplicable en un plazo menor.

d) Favorecer la accesibilidad de todas las personas, con especial atención a las que tengan alguna discapacidad o de edad avanzada a toda la información disponible sobre el código tipo.

TÍTULO VIII. De las medidas de seguridad en el tratamiento de datos de carácter personal

CAPÍTULO I. Disposiciones generales

Artículo 79. Alcance.

Los responsables de los tratamientos o los ficheros y los encargados del tratamiento deberán implantar las medidas de seguridad con arreglo a lo dispuesto en este Título, con independencia de cual sea su sistema de tratamiento.

Artículo 80. Niveles de seguridad.

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

Artículo 81. Aplicación de los niveles de seguridad.

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

2. Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los relativos a la comisión de infracciones administrativas o penales.
b) Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre.
c) Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.
d) Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.
e) Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

f) Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

3. Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.
c) Aquéllos que contengan datos derivados de actos de violencia de género.

4. A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento.

5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.
b) Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

6. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

7. Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

8. A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad.

Artículo 82. Encargado del tratamiento.

1. 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.

2. 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 en los términos exigidos por el artículo 88 de este reglamento 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.

3. En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en este reglamento.

Artículo 83. 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.

Artículo 84. Delegación de autorizaciones.

Las autorizaciones que en este título se atribuyen al responsable del fichero o tratamiento podrán ser delegadas en las personas designadas al efecto. En el documento de seguridad deberán constar las personas habilitadas para otorgar estas autorizaciones así como aquellas en las que recae dicha delegación. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero.

Artículo 85. Acceso a datos a través de redes de comunicaciones.

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, conforme a los criterios establecidos en el artículo 80.

Artículo 86. Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.

1. 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, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

2. La autorización a la que se refiere el párrafo anterior tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas.

Artículo 87. Ficheros temporales o copias de trabajo de documentos.

1. 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 conforme a los criterios establecidos en el artículo 81.

2. Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

CAPÍTULO II. Del documento de seguridad

Artículo 88. El documento de seguridad.

1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.

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

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.
c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.
d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
e) Procedimiento de notificación, gestión y respuesta ante las incidencias.
f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.
g) Las medidas que sea necesario adoptar 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.

4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:

a) La identificación del responsable o responsables de seguridad.
b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

5. 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.

6. 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 al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados.

En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento.

7. El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado 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, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

8. 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.

CAPÍTULO III. Medidas de seguridad aplicables a ficheros y tratamientos automatizados

SECCIÓN 1.ª MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO

Artículo 89. Funciones y obligaciones del personal.

1. 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.

También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

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

Artículo 90. Registro de incidencias.

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.

Artículo 91. Control de acceso.

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. 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.

3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

4. 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.

5. 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.

Artículo 92. Gestión de soportes y documentos.

1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.

Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.

2. 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.

3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

4. 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. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá 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.

Artículo 93. Identificación y autenticación.

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

3. 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.

4. 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.

Artículo 94. Copias de respaldo y recuperación.

1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

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.

3. 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.

4. 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.

Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

SECCIÓN 2.ª MEDIDAS DE SEGURIDAD DE NIVEL MEDIO

Artículo 95. Responsable de seguridad.

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.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.

Artículo 96. Auditoría.

1. 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. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.

2. 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.

3. 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.

Artículo 97. Gestión de soportes y documentos.

1. 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.

2. Igualmente, 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.

Artículo 98. Identificación y autenticación.

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

Artículo 99. Control de acceso físico.

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

Artículo 100. Registro de incidencias.

1. En el registro regulado en el artículo 90 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.

2. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

SECCIÓN 3.ª MEDIDAS DE SEGURIDAD DE NIVEL ALTO

Artículo 101. Gestión y distribución de soportes.

1. 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.

2. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.

3. 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.

Artículo 102. Copias de respaldo y recuperación.

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, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Artículo 103. Registro de accesos.

1. 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.

2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3. 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.

4. El período mínimo de conservación de los datos registrados será de dos años.

5. 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.

6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

a) Que el responsable del fichero o del tratamiento sea una persona física.
b) 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.

Artículo 104. Telecomunicaciones.

Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de 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.

CAPÍTULO IV. Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados

SECCIÓN 1.ª MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO

Artículo 105. Obligaciones comunes.

1. Además de lo dispuesto en el presente capítulo, a los ficheros no automatizados les será de aplicación lo dispuesto en los capítulos I y II del presente título en lo relativo a:

a) Alcance.
b) Niveles de seguridad.
c) Encargado del tratamiento.
d) Prestaciones de servicios sin acceso a datos personales.
e) Delegación de autorizaciones.
f) Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.
g) Copias de trabajo de documentos.
h) Documento de seguridad.

2. Asimismo se les aplicará lo establecido por la sección primera del capítulo III del presente título en lo relativo a:

a) Funciones y obligaciones del personal.
b) Registro de incidencias.
c) Control de acceso.
d) Gestión de soportes.

Artículo 106. Criterios de archivo.

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán 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.

En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

Artículo 107. Dispositivos de almacenamiento.

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.

Artículo 108. Custodia de los soportes.

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.

SECCIÓN 2.ª MEDIDAS DE SEGURIDAD DE NIVEL MEDIO

Artículo 109. Responsable de seguridad.

Se designará uno o varios responsables de seguridad en los términos y con las funciones previstas en el artículo 95 de este reglamento.

Artículo 110. Auditoría.

Los ficheros comprendidos en la presente sección se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

SECCIÓN 3.ª MEDIDAS DE SEGURIDAD DE NIVEL ALTO

Artículo 111. Almacenamiento de la información.

1. 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.

2. Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.

Artículo 112. Copia o reproducción.

1. 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.

2. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

Artículo 113. Acceso a la documentación.

1. El acceso a la documentación se limitará exclusivamente al personal autorizado.

2. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

3. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

Artículo 114. Traslado de documentación.

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.

TÍTULO IX. Procedimientos tramitados por la Agencia Española de Protección de Datos

CAPÍTULO I. Disposiciones generales

Artículo 115. Régimen aplicable.

1. Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el presente título, y supletoriamente, por la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

2. Específicamente serán de aplicación las normas reguladoras del procedimiento administrativo común al régimen de representación en los citados procedimientos.

Artículo 116. Publicidad de las resoluciones.

1. La Agencia Española de Protección de Datos hará públicas sus resoluciones, con excepción de las correspondientes a la inscripción de un fichero o tratamiento en el Registro General de Protección de Datos y de aquéllas por las que se resuelva la inscripción en el mismo de los códigos tipo, siempre que se refieran a procedimientos que se hubieran iniciado con posterioridad al 1 de enero de 2004, o correspondan al archivo de actuaciones inspectoras incoadas a partir de dicha fecha.

2. La publicación de estas resoluciones se realizará preferentemente mediante su inserción en el sitio web de la Agencia Española de Protección de Datos, dentro del plazo de un mes a contar desde la fecha de su notificación a los interesados.

3. En la notificación de las resoluciones se informará expresamente a los interesados de la publicidad prevista en el artículo 37.2 de la Ley Orgánica 15/1999, de 13 de diciembre.

4. La publicación se realizará aplicando los criterios de disociación de los datos de carácter personal que a tal efecto se establezcan mediante Resolución del Director de la Agencia.

CAPÍTULO II. Procedimiento de tutela de los derechos de acceso, rectificación, cancelación y oposición

Artículo 117. Instrucción del procedimiento.

1. El procedimiento se iniciará a instancia del afectado o afectados, expresando con claridad el contenido de su reclamación y de los preceptos de la Ley Orgánica 15/1999, de 13 de diciembre, que se consideran vulnerados.

2. Recibida la reclamación en la Agencia Española de Protección de Datos, se dará traslado de la misma al responsable del fichero, para que, en el plazo de quince días, formule las alegaciones que estime pertinentes.

3. Recibidas las alegaciones o transcurrido el plazo previsto en el apartado anterior, la Agencia Española de Protección de Datos, previos los informes, pruebas y otros actos de instrucción pertinentes, incluida la audiencia del afectado y nuevamente del responsable del fichero, resolverá sobre la reclamación formulada.

Artículo 118. Duración del procedimiento y efectos de la falta de resolución expresa.

1. El plazo máximo para dictar y notificar resolución en el procedimiento de tutela de derechos será de seis meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la reclamación del afectado o afectados.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su reclamación por silencio administrativo positivo.

Artículo 119. Ejecución de la resolución.

Si la resolución de tutela fuese estimatoria, se requerirá al responsable del fichero para que, en el plazo de diez días siguientes a la notificación, haga efectivo el ejercicio de los derechos objeto de la tutela, debiendo dar cuenta por escrito de dicho cumplimiento a la Agencia Española de Protección de Datos en idéntico plazo.

CAPÍTULO III. Procedimientos relativos al ejercicio de la potestad sancionadora

SECCIÓN 1.ª DISPOSICIONES GENERALES

Artículo 120. Ámbito de aplicación.

1. Las disposiciones contenidas en el presente capítulo serán de aplicación a los procedimientos relativos al ejercicio por la Agencia Española de Protección de Datos de la potestad sancionadora que le viene atribuida por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal, en la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico, y en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

2. No obstante, las disposiciones previstas en el artículo 121 y en la sección cuarta de este capítulo únicamente serán aplicables a los procedimientos referidos al ejercicio de la potestad sancionadora prevista en la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 121. Inmovilización de ficheros.

1. En el supuesto previsto como infracción muy grave en la Ley Orgánica 15/1999, de 13 de diciembre, consistente en la utilización o cesión ilícita de los datos de carácter personal en la que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia Española de Protección de Datos podrá, en cualquier momento del procedimiento, requerir a los responsables de ficheros o tratamientos de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos.

2. El requerimiento deberá ser atendido en el plazo improrrogable de tres días, durante el cual el responsable del fichero podrá formular las alegaciones que tenga por convenientes en orden al levantamiento de la medida.

3. Si el requerimiento fuera desatendido, el Director de la Agencia Española de Protección de Datos podrá, mediante resolución motivada, acordar la inmovilización de tales ficheros o tratamientos, a los solos efectos de restaurar los derechos de las personas afectadas.

SECCIÓN 2.ª ACTUACIONES PREVIAS

Artículo 122. Iniciación.

1. Con anterioridad a la iniciación del procedimiento sancionador, se podrán realizar actuaciones previas con objeto de determinar si concurren circunstancias que justifiquen tal iniciación. En especial, estas actuaciones se orientarán a determinar, con la mayor precisión posible, los hechos que pudieran justificar la incoación del procedimiento, identificar la persona u órgano que pudiera resultar responsable y fijar las circunstancias relevantes que pudieran concurrir en el caso.

2. Las actuaciones previas se llevarán a cabo de oficio por la Agencia Española de Protección de Datos, bien por iniciativa propia o como consecuencia de la existencia de una denuncia o una petición razonada de otro órgano.

3. Cuando las actuaciones se lleven a cabo como consecuencia de la existencia de una denuncia o de una petición razonada de otro órgano, la Agencia Española de Protección de Datos acusará recibo de la denuncia o petición, pudiendo solicitar cuanta documentación se estime oportuna para poder comprobar los hechos susceptibles de motivar la incoación del procedimiento sancionador.

4. Estas actuaciones previas tendrán una duración máxima de doce meses a contar desde la fecha en la que la denuncia o petición razonada a las que se refiere el apartado 2 hubieran tenido entrada en la Agencia Española de Protección de Datos o, en caso de no existir aquéllas, desde que el Director de la Agencia acordase la realización de dichas actuaciones.

El vencimiento del plazo sin que haya sido dictado y notificado acuerdo de inicio de procedimiento sancionador producirá la caducidad de las actuaciones previas.

Artículo 123. Personal competente para la realización de las actuaciones previas.

1. Las actuaciones previas serán llevadas a cabo por el personal del área de la Inspección de Datos habilitado para el ejercicio de funciones inspectoras.

2. En supuestos excepcionales, el Director de la Agencia Española de Protección de Datos podrá designar para la realización de actuaciones específicas a funcionarios de la propia Agencia no habilitados con carácter general para el ejercicio de funciones inspectoras o a funcionarios que no presten sus funciones en la Agencia, siempre que reúnan las condiciones de idoneidad y especialización necesarias para la realización de tales actuaciones. En estos casos, la autorización indicará expresamente la identificación del funcionario y las concretas actuaciones previas de inspección a realizar.

3. Los funcionarios que ejerzan la inspección a los que se refieren los dos apartados anteriores tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

Artículo 124. Obtención de información.

Los inspectores podrán recabar cuantas informaciones precisen para el cumplimiento de sus cometidos. A tal fin podrán requerir la exhibición o el envío de los documentos y datos y examinarlos en el lugar en que se encuentren depositados, como obtener copia de los mismos, inspeccionar los equipos físicos y lógicos, así como requerir la ejecución de tratamientos y programas o procedimientos de gestión y soporte del fichero o ficheros sujetos a investigación, accediendo a los lugares donde se hallen instalados.

Artículo 125. Actuaciones presenciales.

1. En el desarrollo de las actuaciones previas se podrán realizar visitas de inspección por parte de los inspectores designados, en los locales o sede del inspeccionado, o donde se encuentren ubicados los ficheros, en su caso. A tal efecto, los inspectores habrán sido previamente autorizados por el Director de la Agencia Española de Protección de Datos.

Las inspecciones podrán realizarse en el domicilio del inspeccionado, en la sede o local concreto relacionado con el mismo o en cualquiera de sus locales, incluyendo aquéllos en que el tratamiento sea llevado a cabo por un encargado.

La autorización se limitará a indicar la habilitación del inspector autorizado y la identificación de la persona u órgano inspeccionado.

2. En el supuesto contemplado en el apartado anterior, las inspecciones concluirán con el levantamiento de la correspondiente acta, en la que quedará constancia de las actuaciones practicadas durante la visita o visitas de inspección.

3. El acta, que se emitirá por duplicado, será firmada por los inspectores actuantes y por el inspeccionado, que podrá hacer constar en la misma las alegaciones o manifestaciones que tenga por conveniente.

En caso de negativa del inspeccionado a la firma del acta, se hará constar expresamente esta circunstancia en la misma. En todo caso, la firma por el inspeccionado del acta no supondrá su conformidad, sino tan sólo la recepción de la misma.

Se entregará al inspeccionado uno de los originales del acta de inspección, incorporándose el otro a las actuaciones.

Artículo 126. Resultado de las actuaciones previas.

1. Finalizadas las actuaciones previas, éstas se someterán a la decisión del Director de la Agencia Española de Protección de Datos.

Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso.

2. En caso de apreciarse la existencia de indicios susceptibles de motivar la imputación de una infracción, el Director de la Agencia Española de Protección de Datos dictará acuerdo de inicio de procedimiento sancionador o de infracción de las Administraciones públicas, que se tramitarán conforme a lo dispuesto, respectivamente, en las secciones tercera y cuarta del presente capítulo.

SECCIÓN 3.ª PROCEDIMIENTO SANCIONADOR

Artículo 127. Iniciación del procedimiento.

Con carácter específico el acuerdo de inicio del procedimiento sancionador deberá contener:

a) Identificación de la persona o personas presuntamente responsables.
b) Descripción sucinta de los hechos imputados, su posible calificación y las sanciones que pudieran corresponder, sin perjuicio de lo que resulte de la instrucción.
c) Indicación de que el órgano competente para resolver el procedimiento es el Director de la Agencia Española de Protección de Datos.

d) Indicación al presunto responsable de que puede reconocer voluntariamente su responsabilidad, en cuyo caso se dictará directamente resolución.

e) Designación de instructor y, en su caso, secretario, con expresa indicación del régimen de recusación de los mismos.

f) Indicación expresa del derecho del responsable a formular alegaciones, a la audiencia en el procedimiento y a proponer las pruebas que estime procedentes.

g) Medidas de carácter provisional que pudieran acordarse, en su caso, conforme a lo establecido en la sección primera del presente capítulo.

Artículo 128. Plazo máximo para resolver.

1. El plazo para dictar resolución será el que determinen las normas aplicables a cada procedimiento sancionador y se computará desde la fecha en que se dicte el acuerdo de inicio hasta que se produzca la notificación de la resolución sancionadora, o se acredite debidamente el intento de notificación.

2. El vencimiento del citado plazo máximo, sin que se haya dictada y notificada resolución expresa, producirá la caducidad del procedimiento y el archivo de las actuaciones.

SECCIÓN 4.ª PROCEDIMIENTO DE DECLARACIÓN DE INFRACCIÓN DE LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, POR LAS ADMINISTRACIONES PÚBLICAS

Artículo 129. Disposición general.

El procedimiento por el que se declare la existencia de una infracción de la Ley Orgánica 15/1999, de 13 de diciembre, cometida por las Administraciones públicas será el establecido en la sección tercera de este capítulo.

CAPÍTULO IV. Procedimientos relacionados con la inscripción o cancelación de ficheros

SECCIÓN 1.ª PROCEDIMIENTO DE INSCRIPCIÓN DE LA CREACIÓN, MODIFICACIÓN O SUPRESIÓN DE FICHEROS

Artículo 130. Iniciación del procedimiento.

1. El procedimiento se iniciará como consecuencia de la notificación de la creación, modificación o supresión del fichero por el interesado o, en su caso, de la comunicación efectuada por las autoridades de control de las comunidades autónomas, a la que se refiere el presente reglamento.

2. La notificación se deberá efectuar cumplimentando los modelos o formularios electrónicos publicados al efecto por la Agencia Española de Protección de Datos, en virtud de lo dispuesto en el apartado 1 del artículo 59 de este reglamento.

Tratándose de la notificación de la modificación o supresión de un fichero, deberá indicarse en la misma el código de inscripción del fichero en el Registro General de Protección de Datos.

3. La notificación se efectuará en soporte electrónico, ya mediante comunicación electrónica a través de Internet mediante firma electrónica o en soporte informático, utilizando al efecto el programa de ayuda para la generación de notificaciones que la Agencia pondrá a disposición de los interesados de forma gratuita.

Será igualmente válida la notificación efectuada en soporte papel cuando para su cumplimentación hayan sido utilizados los modelos o formularios publicados por la Agencia.

4. En la notificación, el responsable del fichero deberá declarar un domicilio a efectos de notificaciones en el procedimiento.

Artículo 131. Especialidades en la notificación de ficheros de titularidad pública.

1. Cuando se trate de la notificación de ficheros de titularidad pública, deberá acompañarse a la notificación una copia de la norma o acuerdo de creación, modificación o supresión del fichero a que hace referencia el artículo 52 del presente reglamento.

Cuando el diario oficial en el que se encuentre publicada la citada norma o acuerdo sea accesible a través de Internet, bastará con indicar en la notificación la dirección electrónica que permita su concreta localización.

2. Recibida la notificación, si la misma no contuviera la información preceptiva o se advirtieran defectos formales, el Registro General de Protección de Datos requerirá al responsable del fichero para que complete o subsane la notificación. El plazo para la subsanación o mejora de la solicitud será de tres meses, en el caso de que se precise la modificación de la norma o acuerdo de creación del fichero.

Artículo 132. Acuerdo de inscripción o cancelación.

Si la notificación referida a la creación, modificación o supresión del fichero contuviera la información preceptiva y se cumplieran las restantes exigencias legales, el Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, acordará, respectivamente, la inscripción del fichero, asignando al mismo el correspondiente código de inscripción, la modificación de la inscripción del fichero o la cancelación de la inscripción correspondiente.

Artículo 133. Improcedencia o denegación de la inscripción.

El Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, dictará resolución denegando la inscripción, modificación o cancelación cuando de los documentos aportados por el responsable del fichero se desprenda que la notificación no resulta conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre.

La resolución será debidamente motivada, con indicación expresa de las causas que impiden la inscripción, modificación o cancelación.

Artículo 134. Duración del procedimiento y efectos de la falta de resolución expresa.

1. El plazo máximo para dictar y notificar resolución acerca de la inscripción, modificación o cancelación será de un mes.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, se entenderá inscrito, modificado o cancelado el fichero a todos los efectos.

SECCIÓN 2.ª PROCEDIMIENTO DE CANCELACIÓN DE OFICIO DE FICHEROS INSCRITOS

Artículo 135. Iniciación del procedimiento.

El procedimiento de cancelación de oficio de los ficheros inscritos en el Registro General de Protección de Datos se iniciará siempre de oficio, bien por propia iniciativa o en virtud de denuncia, por acuerdo del Director de la Agencia Española de Protección de Datos.

Artículo 136. Terminación del expediente.

La resolución, previa audiencia del interesado, acordará haber lugar o no a la cancelación del fichero.

Si la resolución acordase la cancelación del fichero, se dará traslado de la misma al Registro General de Protección de Datos, para que proceda a la cancelación.

SECCIÓN 1.ª PROCEDIMIENTO DE AUTORIZACIÓN DE TRANSFERENCIAS INTERNACIONALES DE DATOS

Artículo 137. Iniciación del procedimiento.

1. El procedimiento para la obtención de la autorización para las transferencias internacionales de datos a países terceros a las que se refiere el artículo 33 de la Ley Orgánica 15/1999, de 13 de diciembre, y el artículo 70 de este reglamento se iniciará siempre a solicitud del exportador que pretenda llevar a cabo la transferencia.

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

a) 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.
b) La transferencia o transferencias respecto de las que se solicita la autorización, con indicación de la finalidad que la justifica.
c) 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.

Si la autorización se pretendiera fundar en lo dispuesto en el apartado 4 del artículo 70, deberán aportarse las normas o reglas adoptadas en relación con el tratamiento de los datos en el seno del grupo, así como la documentación que acredite su carácter vinculante y su eficacia dentro del grupo. Igualmente deberá aportarse la documentación que acredite la posibilidad de que el afectado o la Agencia Española de Protección de Datos puedan exigir la responsabilidad que corresponda en caso de perjuicio del afectado o vulneración de las normas de protección de datos por parte de cualquier empresa importadora.

Artículo 138. Instrucción del procedimiento.

1. Cuando el Director de la Agencia Española de Protección de Datos acuerde, conforme a lo dispuesto en el artículo 86.1 de la Ley 30/1992, de 26 de noviembre, la apertura de un período de información pública, el plazo para la formulación de alegaciones será de diez días a contar desde la publicación en el «Boletín Oficial del Estado» del anuncio previsto en dicha Ley.

2. No será posible el acceso a la información del expediente en que concurran las circunstancias establecidas en el artículo 37.5 de la Ley 30/1992, de 26 de noviembre.

3. Transcurrido el plazo previsto en el apartado 1, en caso de que se hubieran formulado alegaciones, se dará traslado de las mismas al solicitante de la autorización, a fin de que en el plazo de diez días alegue lo que estime procedente.

Artículo 139. Actos posteriores a la resolución.

1. 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 Registro General de Protección de Datos inscribirá de oficio la autorización de transferencia internacional.

2. En todo caso, se dará traslado de la resolución de autorización o denegación de la autorización de la transferencia internacional de datos al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26.3 de la Directiva 95/46/CE.

Artículo 140. Duración del procedimiento y efectos de la falta de resolución expresa.

1. 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.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, se entenderá autorizada la transferencia internacional de datos.

SECCIÓN 2.ª PROCEDIMIENTO DE SUSPENSIÓN TEMPORAL DE TRANSFERENCIAS INTERNACIONALES DE DATOS

Artículo 141. Iniciación.

1. En los supuestos contemplados en el artículo 69 y en el apartado 3 del artículo 70, el Director de la Agencia Española de Protección de Datos podrá acordar la suspensión temporal de una transferencia internacional de datos.

2. En tales supuestos, el Director dictará acuerdo de inicio referido a la suspensión temporal de la transferencia.

El acuerdo deberá ser motivado y fundarse en los supuestos previstos en este reglamento.

Artículo 142. Instrucción y resolución.

1. Se dará traslado del acuerdo al exportador, a fin de que en el plazo de quince días formule lo que a su derecho convenga.

2. Recibidas las alegaciones o cumplido el plazo señalado, el Director dictará resolución acordando, en su caso, la suspensión temporal de la transferencia internacional de datos.

Artículo 143. Actos posteriores a la resolución.

1. El Director de la Agencia Española de Protección de Datos dará traslado de la resolución al Registro General de Protección de Datos, a fin de que la misma se haga constar en el registro.

El Registro General de Protección de Datos inscribirá de oficio la suspensión temporal de la transferencia internacional.

2. En todo caso, se dará traslado de la resolución al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26.3 de la Directiva 95/46/CE.

Artículo 144. Levantamiento de la suspensión temporal.

1. La suspensión se levantará tan pronto como cesen las causas que la hubieran justificado, mediante resolución del Director de la Agencia Española de Protección de Datos, del que se dará traslado al exportador.

2. El Director de la Agencia Española de Protección de Datos dará traslado de la resolución al Registro General de Protección de Datos, a fin de que la misma se haga constar en el Registro.

El Registro General de Protección de Datos hará constar de oficio el levantamiento de la suspensión temporal de la transferencia internacional.

3. El acuerdo será notificado al exportador y al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26. 3 de la Directiva 95/46/CE.

CAPÍTULO VI. Procedimiento de inscripción de códigos tipo

Artículo 145. Iniciación del procedimiento.

1. El procedimiento para la inscripción en el Registro General de Protección de Datos de los códigos tipo se iniciará siempre a solicitud de la entidad, órgano o asociación promotora del código tipo.

2. La solicitud, que deberá reunir los requisitos legalmente establecidos, habrá de acompañarse de los siguientes documentos:

a) Acreditación de la representación que concurra en la persona que presente la solicitud.
b) Contenido del acuerdo, convenio o decisión por la que se aprueba, en el ámbito correspondiente el contenido del código tipo presentado.
c) En caso de que el código tipo proceda de un acuerdo sectorial o una decisión de empresa certificación referida a la adopción del acuerdo y legitimación del órgano que lo adoptó.
d) En el supuesto contemplado en la letra anterior, copia de los estatutos de la asociación, organización sectorial o entidad en cuyo marco haya sido aprobado el código.
e) En caso de códigos tipo presentados por asociaciones u organizaciones de carácter sectorial, documentación relativa a su representatividad en el sector.
f) En caso de códigos tipo basados en decisiones de empresa, descripción de los tratamientos a los que se refiere el código tipo.
g) Código tipo sometido a la Agencia Española de Protección de Datos.

Artículo 146. Análisis de los aspectos sustantivos del código tipo.

1. Durante los treinta días siguientes a la notificación o subsanación de los defectos el Registro General de Protección de Datos podrá convocar a los solicitantes, a fin de obtener aclaraciones o precisiones relativas al contenido sustantivo del código tipo.

2. Transcurrido el plazo señalado en el apartado anterior, el Registro General de Protección de Datos elaborará un informe sobre las características del proyecto de código tipo.

3. La documentación presentada y el informe del Registro serán remitidos al Gabinete Jurídico, a fin de que por el mismo se informe acerca del cumplimiento de los requisitos establecidos en el Título VII de este Reglamento.

Artículo 147. Información pública.

1. Cuando el Director de la Agencia Española de Protección de Datos acuerde, conforme a lo dispuesto en el artículo 86.1 de la Ley 30/1992, de 26 de noviembre, la apertura de un período de información pública, el plazo para la formulación de alegaciones será de diez días a contar desde la publicación en el «Boletín Oficial del Estado» del anuncio previsto en dicha ley.

2. No será posible el acceso a la información del expediente en que concurran las circunstancias establecidas en el artículo 37.5 de la Ley 30/1992, de 26 de noviembre.

Artículo 148. Mejora del código tipo.

Si durante la tramitación del procedimiento resultase necesaria la aportación de nuevos documentos o la modificación del código tipo presentado, la Agencia Española de Protección de Datos podrá requerir al solicitante, a fin de que en el plazo de treinta días introduzca las modificaciones que sean precisas, remitiendo el texto resultante a la Agencia Española de Protección de Datos.

Se declarará la suspensión del procedimiento en tanto el solicitante no dé cumplimiento al requerimiento.

Artículo 149. Trámite de audiencia.

En caso de que durante el trámite previsto en el artículo 148 se hubieran formulado alegaciones, se dará traslado de las mismas al solicitante de la autorización, a fin de que en el plazo de diez días alegue lo que estime procedente.

Artículo 150. Resolución.

1. Cumplidos los términos establecidos en los artículos precedentes, el Director de la Agencia resolverá sobre la procedencia o improcedencia de la inscripción del código tipo en el Registro General de Protección de Datos.

2. Cuando el Director de la Agencia Española de Protección de Datos resuelva autorizar la inscripción del código tipo, se dará traslado de la resolución al Registro General de Protección de Datos, a fin de proceder a su inscripción.

Artículo 151. Duración del procedimiento y efectos de la falta de resolución expresa.

1. El plazo máximo para dictar y notificar resolución será de seis meses, a contar desde la fecha de entrada de la solicitud en la Agencia Española de Protección de Datos.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el solicitante podrá considerar estimada su solicitud.

Artículo 152. Publicación de los códigos tipo por la Agencia Española de Protección de Datos.

La Agencia Española de Protección de Datos dará publicidad al contenido de los códigos tipo inscritos en el Registro General de Protección de Datos, utilizando para ello, con carácter preferente, medios electrónicos o telemáticos.

CAPÍTULO VII. Otros procedimientos tramitados por la agencia española de protección de datos

SECCIÓN 1.ª PROCEDIMIENTO DE EXENCIÓN DEL DEBER DE INFORMACIÓN AL INTERESADO

Artículo 153. Iniciación del procedimiento.

1. El procedimiento para obtener de la Agencia Española de Protección de Datos la exención del deber de informar al interesado acerca del tratamiento de sus datos de carácter personal cuando resulte imposible o exija esfuerzos desproporcionados, prevista en el apartado 5 del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, se iniciará siempre a petición del responsable que pretenda obtener la aplicación de la exención.

2. En el escrito de solicitud, además de los requisitos recogidos en el artículo 70 de la Ley 30/1992, de 26 de noviembre, el responsable deberá:

a) Identificar claramente el tratamiento de datos al que pretende aplicarse la exención del deber de informar.
b) Motivar expresamente las causas en que fundamenta la imposibilidad o el carácter desproporcionado del esfuerzo que implicaría el cumplimiento del deber de informar.
c) Exponer detalladamente las medidas compensatorias que propone realizar en caso de exoneración del cumplimiento del deber de informar.
d) Aportar una cláusula informativa que, mediante su difusión, en los términos que se indiquen en la solicitud, permita compensar la exención del deber de informar.

Artículo 154. Propuesta de nuevas medidas compensatorias.

1. Si la Agencia Española de Protección de Datos considerase insuficientes las medidas compensatorias propuestas por el solicitante, podrá acordar la adopción de medidas complementarias o sustitutivas a las propuestas por aquél en su solicitud.

2. Del acuerdo se dará traslado al solicitante, a fin de que exponga lo que a su derecho convenga en el plazo de quince días.

Artículo 155. Terminación del procedimiento.

Concluidos los trámites previstos en los artículos precedentes, el Director de la Agencia dictará resolución, concediendo o denegando la exención del deber de informar. La resolución podrá imponer la adopción de las medidas complementarias a las que se refiere el artículo anterior.

Artículo 156. Duración del procedimiento y efectos de la falta de resolución expresa.

1. El plazo máximo para dictar y notificar resolución en el procedimiento será de seis meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud del responsable del fichero.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su solicitud por silencio administrativo positivo.

SECCIÓN 2.ª PROCEDIMIENTO PARA LA AUTORIZACIÓN DE CONSERVACIÓN DE DATOS PARA FINES HISTÓRICOS, ESTADÍSTICOS O CIENTÍFICOS

Artículo 157. Iniciación del procedimiento.

1. El procedimiento para obtener de la Agencia Española de Protección de Datos la declaración de la concurrencia en un determinado tratamiento de datos de valores históricos, científicos o estadísticos, a los efectos previstos en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento, se iniciará siempre a petición del responsable que pretenda obtener la declaración.

2. En el escrito de solicitud, el responsable deberá:

a) Identificar claramente el tratamiento de datos al que pretende aplicarse la excepción.
b) Motivar expresamente las causas que justificarían la declaración.
c) Exponer detalladamente las medidas que el responsable del fichero se propone implantar para garantizar el derecho de los ciudadanos.

3. La solicitud deberá acompañarse de cuantos documentos o pruebas sean necesarios para justificar la existencia de los valores históricos, científicos o estadísticos que fundamentarían la declaración de la Agencia.

Artículo 158. Duración del procedimiento y efectos de la falta de resolución expresa.

1. El plazo máximo para dictar y notificar resolución en el procedimiento será de tres meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud del responsable del fichero.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su solicitud.

Disposición adicional única. Productos de software.

Los productos de software destinados al tratamiento automatizado de datos personales deberán incluir en su descripción técnica el nivel de seguridad, básico, medio o alto, que permitan alcanzar de acuerdo con lo establecido en el título VIII de este reglamento.

Disposición final única. Aplicación supletoria.

En lo no establecido en el capítulo III del título IX serán de aplicación a los procedimientos sancionadores tramitados por la Agencia Española de Protección de Datos las disposiciones contenidas en el Reglamento del Procedimiento para el ejercicio de la potestad sancionadora, aprobado por Real Decreto 1398/1993, de 4 de agosto.

12.3. Instrucción 1/1998, de 19 de enero, de la AEPD, relativa al ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición

La Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal dedica los artículos 14 y siguientes a los derechos de acceso, rectificación y cancelación de los datos de carácter personal contenidos en ficheros automatizados. Dichos derechos se configuran como uno de los ejes fundamentales sobre los que se articula la protección del honor, la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos, en desarrollo de lo dispuesto en el artículo 18.4 de la Constitución Española.

El ejercicio de los derechos de acceso, rectificación y cancelación aparece regulado no sólo en la Ley Orgánica 5/1992, sino también en el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos procedimentales de la citada Ley.

Al amparo de lo dispuesto en el artículo 36.c) de la Ley Orgánica 5/92 que atribuye al Director de la Agencia la función de "Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos automatizados a los principios de la presente Ley", se ha elaborado la presente Instrucción.

Esta Instrucción tiene por objeto aclarar las disposiciones relativas a los derechos de acceso, rectificación y cancelación, ya que las actuaciones practicadas por esta Agencia han puesto de manifiesto que en su aplicación se presentan problemas interpretativos y que es necesario precisar el ejercicio de estos derechos en relación con algunos ficheros que presentan características especiales. Para ello, la Instrucción recoge la regulación de dichos derechos de acuerdo con la Ley Orgánica 5/1992 y el Real Decreto 1332/1994, de 20 de junio, y realiza una interpretación unitaria de los preceptos teniendo en cuenta la totalidad de principios legales.

En las normas primera, segunda y tercera se detallan los requisitos que deben cumplirse en el ejercicio de los derechos de acceso, rectificación y cancelación con carácter general. Sin embargo, las particularidades que presentan los ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito y los ficheros con fines de publicidad exigen tratarlos de un modo especial en las normas cuarta y quinta, respectivamente.

Norma Primera. Requisitos Generales

1.- Los derechos de acceso a los ficheros automatizados, así como los de rectificación y cancelación de datos son personalísimos, y serán ejercidos por el afectado frente al responsable del fichero por lo que será necesario que el afectado acredite su identidad frente a dicho responsable. Estos derechos se ejercerán sin otras limitaciones que las que prevén la Ley Orgánica 5/1992 y el Real Decreto 1332/1994, de 20 de junio.

Podrá, no obstante, actuar el representante legal del afectado cuando éste se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de los mismos, en cuyo caso será necesario que el representante legal acredite tal condición.

2.- La Ley configura los derechos de acceso, rectificación y cancelación como derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

3.- El ejercicio de los derechos deberá llevarse a cabo mediante solicitud dirigida al responsable del fichero, que contendrá:

- Nombre, apellidos del interesado y fotocopia del DNI del interesado y, en los casos que excepcionalmente se admita, de la persona que lo represente, así como el documento acreditativo de tal representación. La fotocopia del DNI podrá ser sustituida siempre que se acredite la identidad por cualquier otro medio válido en derecho.

- Petición en que se concreta la solicitud.

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

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

- El interesado deberá utilizar cualquier medio que permita acreditar el envío y la recepción de la solicitud.

4.- El responsable del fichero deberá contestar la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado en sus ficheros, debiendo utilizar cualquier medio que permita acreditar el envío y la recepción.

En el caso de que la solicitud no reúna los requisitos especificados en el apartado tercero, el responsable del fichero deberá solicitar la subsanación de los mismos.

5.- El responsable del fichero deberá adoptar las medidas oportunas para garantizar que todas 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.

Norma Segunda. Derecho de Acceso

1.- El afectado tiene derecho a solicitar y obtener información de sus datos de carácter personal incluidos en ficheros automatizados.

2.- Al ejercitar el derecho de acceso, el afectado podrá optar por uno o varios de los siguientes sistemas de consulta del fichero, siempre que la configuración o implantación material del fichero lo permita:

a) Visualización en pantalla

b) Escrito, copia o fotocopia remitida por correo

c) Telecopia

d) Cualquier otro procedimiento que sea adecuado a la configuración e implantación material del fichero, ofrecido por el responsable del mismo.

3.- El responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes, a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición de acceso, ésta podrá entenderse desestimada a los efectos de la interposición de la reclamación prevista en el artículo 17.1 de la Ley Orgánica 5/1992.

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

4.- Si la resolución fuera estimatoria, el acceso se hará efectivo en el plazo de los diez días siguientes a la notificación de aquella.

5.- El responsable del fichero podrá denegar el acceso a los datos de carácter personal cuando el derecho se haya ejercitado en un intervalo inferior a doce meses y no se acredite un interés legítimo al efecto, así como cuando la solicitud sea formulada por persona distinta del afectado.

Tratándose de ficheros de titularidad pública se podrá denegar el acceso en los supuestos de los artículos 21.1 y 21.2 de la Ley Orgánica 5/1992, en los que se establecen excepciones relativas a los ficheros de las Fuerzas y Cuerpos de Seguridad del Estado y a los ficheros de la Hacienda Pública y del artículo 22 de la Ley Orgánica 5/1992.

6.- La información que se proporcione, cualquiera que sea el soporte en que fuere facilitada, se dará en forma legible e inteligible, previa transcripción en claro de los datos del fichero, en su caso, y comprenderá todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático, así como 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.

En el caso de que los datos provengan de fuentes diversas, deberán especificarse las mismas identificando la información que proviene de cada una de ellas.

Norma Tercera. Derechos de Rectificación y Cancelación.

1.- Si los datos de carácter personal del afectado son inexactos o incompletos, inadecuados o excesivos, podrá éste solicitar del responsable del fichero la rectificación o, en su caso, la cancelación de los mismos.

2.- Los derechos de rectificación y cancelación se harán efectivos por el responsable del fichero dentro de los cinco días siguientes al de la recepción de la solicitud. Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá notificar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que éste, a su vez, la lleve a cabo en su fichero.

3.- La solicitud de rectificación deberá indicar el dato que es erróneo y la corrección que debe realizarse y deberá ir acompañada de la documentación justificativa de la rectificación solicitada, salvo que la misma dependa exclusivamente del consentimiento del interesado.

4.- En la solicitud de cancelación, el interesado deberá indicar si revoca el consentimiento otorgado, en los casos en que la revocación proceda, o si, por el contrario, se trata de un dato erróneo o inexacto, en cuyo caso deberá acompañar la documentación justificativa.

5.- La cancelación no procederá cuando pudiese causar un perjuicio a intereses legítimos del afectado o de terceros o cuando existiese una obligación de conservar los datos.

6.- Si solicitada la rectificación o cancelación, el responsable del fichero considera que no procede atender la solicitud del afectado, se lo comunicará motivadamente dentro del plazo de los cinco días siguientes al de la recepción de la misma, a fin de que por éste se pueda hacer uso de la reclamación prevista en el artículo 17.1 de la Ley Orgánica 5/1992.

7.- Transcurrido el plazo de cinco días sin que de forma expresa se responda a la solicitud de rectificación o cancelación, ésta podrá entenderse desestimada a los efectos de la interposición de la reclamación que corresponda.

8.- La cancelación exige el borrado físico de los datos, sin que sea suficiente a estos efectos una marca lógica o el mantenimiento de otro fichero alternativo en el que se registren las bajas producidas.

9.- En los casos en que, siendo procedente la cancelación de los datos, no sea posible su extinción física, tanto por razones técnicas como por causa del procedimiento o soporte utilizado, el responsable del fichero procederá al bloqueo de los datos, con el fin de impedir su ulterior proceso o utilización.

Se exceptúa, no obstante, el supuesto en el que se demuestre que los datos han sido recogidos o registrados por medios fraudulentos, desleales o ilícitos, en cuyo caso la cancelación de los mismos comportará siempre la destrucción del soporte en el que aquéllos figuren.

Norma Cuarta. Ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito.

1.- El ejercicio de los derechos de acceso, rectificación y cancelación en el caso de los ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito se rige por las normas anteriores de la presente Instrucción, sin perjuicio de lo señalado en los apartados siguientes.

2.- El responsable de un fichero de prestación de servicios de solvencia patrimonial y crédito con datos obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el afectado o con su consentimiento, estará obligado a satisfacer, en cualquier caso, los derechos de acceso, rectificación y cancelación. Las personas y entidades a las que se presta el servicio únicamente estarán obligadas a comunicar al afectado aquellos datos relativos al mismo a los que ellas tengan acceso y a comunicar la identidad del responsable del fichero común para que pueda completar el ejercicio de sus derechos.

3.- El responsable del fichero común en el que se traten automatizadamente datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés, ante una solicitud de ejercicio del derecho de acceso, deberá comunicar al afectado todos los datos relativos al mismo que obren en el fichero. Cualquier otra entidad participante en el sistema, ante tal solicitud, deberá comunicar al afectado todos los datos relativos al mismo a los que ella pueda acceder, así como la identidad del responsable del fichero común para que pueda completar el ejercicio de su derecho de acceso.

Si la solicitud del ejercicio de los derechos de rectificación o cancelación de datos se dirige al responsable del fichero común, éste tomará las medidas oportunas para trasladar dicha solicitud a la entidad que haya facilitado los datos, para que ésta la resuelva. En el caso de que el responsable del fichero común no haya recibido contestación por parte de la entidad en el plazo de cinco días, procederá a la rectificación o cancelación cautelar de los mismos.

Si la solicitud del ejercicio de los derechos de rectificación o cancelación de datos se dirige a cualquier otra entidad participante en el sistema y hace referencia a datos que dicha entidad haya facilitado al fichero común, procederá a la rectificación o cancelación de los mismos en sus ficheros y a notificarlo al responsable del fichero común en el plazo de cinco días. Si la solicitud hace referencia a datos que la entidad no hubiera facilitado al fichero común, dicha entidad informará al afectado sobre este hecho, proporcionándole, además, la identidad del responsable del fichero común para que pueda completar el ejercicio de sus derechos.

4.- En los ficheros de prestación de servicios de información de solvencia patrimonial y crédito, cualquiera que sea el origen de los datos, cuando el afectado lo solicite el responsable del fichero común deberá cumplir la obligación establecida en el artículo 28.2 de la Ley Orgánica 5/1992 de 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.

Norma Quinta. Ficheros con fines de publicidad.

1.- El responsable del fichero que presta el servicio de publicidad estará obligado a satisfacer los derechos de acceso, rectificación y cancelación. La entidad beneficiaria de la publicidad estará obligada a indicar al afectado la identidad del responsable del fichero del que provienen los datos. A tal efecto, se entenderá suficiente que dicha información se haga constar en la campaña publicitaria.

2.- Cuando el interesado manifieste su deseo de no recibir publicidad, y no ejerza expresamente el derecho de cancelación el responsable del fichero podrá conservar los mínimos datos imprescindibles para identificarlo y adoptar las medidas necesarias que eviten el envío de publicidad.

Disposición Final.-

La presente Instrucción entrará en vigor a los 20 días de su publicación en el Boletín Oficial del Estado.

Madrid, 19 de enero de 1998

EL DIRECTOR DE LA AGENCIA, Fd.: Juan José Martín-Casallo López

12.4. Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras

El incremento que últimamente están experimentando las instalaciones de sistemas de cámaras y videocámaras con fines de vigilancia ha generado numerosas dudas en lo relativo al tratamiento de las imágenes que ello implica.

Además es un sector que ofrece múltiples medios de tratar datos personales como pueden ser los circuitos cerrados de televisión, grabación por dispositivos «webcam», digitalización de imágenes o instalación de cámaras en el lugar de trabajo. Precisamente la última Conferencia Internacional de Autoridades de Protección de Datos, celebrada en Londres los pasados días 1 a 3 de noviembre de este año, ha girado en torno a la necesidad de adecuar la videovigilancia a las exigencias del derecho fundamental a la protección de datos. Todo esto hace necesario que, en ejercicio de la competencia que le atribuye el artículo 37.1.c) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, la Agencia Española de Protección de Datos dicte una Instrucción para adecuar los tratamientos de imágenes con fines de vigilancia a los principios de dicha Ley Orgánica y garantizar los derechos de las personas cuyas imágenes son tratadas por medio de tales procedimientos.

El marco en que se mueve la presente Instrucción es claro. La seguridad y la vigilancia, elementos presentes en la sociedad actual, no son incompatibles con el derecho fundamental a la protección de la imagen como dato personal, lo que en consecuencia exige respetar la normativa existente en materia de protección de datos, para de esta manera mantener la confianza de la ciudadanía en el sistema democrático.

Las imágenes se consideran un dato de carácter personal, en virtud de lo establecido en el artículo 3 de la Ley Orgánica 15/1999 y el artículo 1.4 del Real Decreto 1322/1994 de 20 de junio, que considera como dato de carácter personal la información gráfica o fotográfica.

En relación con la instalación de sistemas de videocámaras, será necesario ponderar los bienes jurídicos protegidos.

Por tanto, toda instalación deberá respetar el principio de proporcionalidad, lo que en definitiva supone, siempre que resulte posible, adoptar otros medios menos intrusivos a la intimidad de las personas, con el fin de prevenir interferencias injustificadas en los derechos y libertades fundamentales.

En consecuencia, el uso de cámaras o videocámaras no debe suponer el medio inicial para llevar a cabo funciones de vigilancia por lo que, desde un punto de vista objetivo, la utilización de estos sistemas debe ser proporcional al fin perseguido, que en todo caso deberá ser legítimo.

En cuanto a la proporcionalidad, pese a ser un concepto jurídico indeterminado, la Sentencia del Tribunal Constitucional 207/1996 determina que se trata de «una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad, y más en particular de las medidas restrictivas de derechos fundamentales adoptadas en el curso de un proceso penal viene determinada por la estricta observancia del principio de proporcionalidad.

En este sentido, hemos destacado que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones:

«si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)».

Asimismo la proporcionalidad es un elemento fundamental en todos los ámbitos en los que se instalen sistemas de videovigilancia, dado que son numerosos los supuestos en los que la vulneración del mencionado principio puede llegar a generar situaciones abusivas, tales como la instalación de sistemas de vigilancia en espacios comunes, o aseos del lugar de trabajo. Por todo ello se trata de evitar la vigilancia omnipresente, con el fin de impedir la vulnerabilidad de la persona.

Se excluyen de la presente Instrucción los datos personales grabados para uso o finalidad doméstica de conformidad con lo establecido en el artículo 2 a) de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, si bien en el sentido estricto señalado por el Tribunal de Justicia de las Comunidades Europeas en la Sentencia de 6 de noviembre de 2003, asunto Lindqvist, que al interpretar la excepción prevista en el artículo 3 apartado 2 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, indica que únicamente contempla «las actividades que se inscriben en el marco de la vida privada o familiar de los particulares» y no otras distintas. En la misma línea se pronuncia el Dictamen 4/2004, adoptado por el Grupo de Trabajo creado por el Artículo 29 de la Directiva 95/46/CE, con fecha 25 de noviembre de 2002.

Además, la Instrucción tampoco se aplicará al tratamiento de imágenes cuando éstas se utilizan para el ejercicio de sus funciones por parte de las Fuerzas y Cuerpos de Seguridad, que está cubierto por normas específicas, aunque estos tratamientos también deberán cumplir las garantías establecidas por la Ley Orgánica 15/1999.

Por otro lado, la Instrucción pretende adecuar los tratamientos a los criterios marcados por la jurisprudencia del Tribunal Constitucional al considerar que el tratamiento de datos personales no exige la conservación de los mismos, sino que basta su recogida o grabación. En el mismo sentido se han pronunciado las legislaciones que sobre esta materia han adoptado los distintos Estados miembros de la Unión Europea, cumpliendo así el mandato contenido en la Directiva 95/46/CE.

Por último, las plenas garantías de protección de los datos personales, así como las peculiaridades de su tratamiento exige una regulación concreta evitando la aplicación de un conjunto de reglas abstractas y dispersas.

Por ello, a la hora de regular la legitimación del tratamiento de imágenes, la Agencia Española de Protección de Datos, entiende que es requisito esencial la aplicación íntegra del artículo 6.1 y 2 y del artículo 11.1 y 2 de la LOPD, sin perjuicio del estricto cumplimiento de los requisitos que para la instalación de cámaras o videocámaras de vigilancia vengan exigidos por la legislación vigente. Asimismo se regula el contenido del deber de información previsto en el artículo 5 de la misma Ley Orgánica, así como el ejercicio de los derechos a que se refieren los artículos 15 y siguientes de la citada Ley Orgánica. Por descontado, la creación de un fichero de videovigilancia exige su previa notificación a la Agencia Española de Protección de Datos, para la inscripción en su Registro General.

En su virtud, de conformidad con lo dispuesto en el artículo 37.1.c) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, dispongo:

Artículo 1. Ámbito objetivo.

1. La presente Instrucción se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras.

El tratamiento objeto de esta Instrucción comprende la grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas.

Se considerará identificable una persona cuando su identidad pueda determinarse mediante los tratamientos a los que se refiere la presente instrucción, sin que ello requiera plazos o actividades desproporcionados.

Las referencias contenidas en esta Instrucción a videocámaras y cámaras se entenderán hechas también a cualquier medio técnico análogo y, en general, a cualquier sistema que permita los tratamientos previstos en la misma.

2. El tratamiento de los datos personales procedentes de las imágenes obtenidas mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad se regirá por las disposiciones sobre la materia.

3. No se considera objeto de regulación de esta Instrucción el tratamiento de imágenes en el ámbito personal y doméstico, entendiéndose por tal el realizado por una persona física en el marco de una actividad exclusivamente privada o familiar.

Artículo 2. Legitimación.

1. Sólo será posible el tratamiento de los datos objeto de la presente instrucción, cuando se encuentre amparado por lo dispuesto en el artículo 6.1 y 2 y el artículo 11.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. Sin perjuicio de lo establecido en el apartado anterior la instalación de cámaras y videocámaras deberá respetar en todo caso los requisitos exigidos por la legislación vigente en la materia.

Artículo 3. Información.

Los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de La Ley Orgánica 15/1999, de 13 de diciembre. A tal fin deberán:

a) Colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados y

b) Tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999.

El contenido y el diseño del distintivo informativo se ajustará a lo previsto en el Anexo de esta Instrucción.

Artículo 4. Principios de calidad, proporcionalidad y finalidad del tratamiento.

1. De conformidad con el artículo 4 de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras.

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

3. Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida.

Artículo 5. Derechos de las personas.

1. Para el ejercicio de los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, el/la afectado/a deberá remitir al responsable del tratamiento solicitud en la que hará constar su identidad junto con una imagen actualizada. El ejercicio de estos derechos se llevará a cabo de conformidad con lo dispuesto en la citada Ley Orgánica y su normativa de desarrollo.

2. El responsable podrá facilitar el derecho de acceso mediante escrito certificado en el que, con la mayor precisión posible y sin afectar a derechos de terceros, se especifiquen los datos que han sido objeto de tratamiento.

3. El/la interesado/a al que se deniegue total o parcialmente el ejercicio de los derechos señalados en el párrafo anterior, podrá reclamar su tutela ante el Director de la Agencia Española de Protección de Datos.

Artículo 6. Cancelación.

Los datos serán cancelados en el plazo máximo de un mes desde su captación.

Artículo 7. Notificación de ficheros.

1. La persona o entidad que prevea la creación de ficheros de videovigilancia deberá notificarlo previamente a la Agencia Española de Protección de Datos, para su inscripción en el Registro General de la misma.

Tratándose de ficheros de titularidad pública deberá estarse a lo establecido en el artículo 20 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. A estos efectos, no se considerará fichero el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real.

Articulo 8. Seguridad y Secreto.

El responsable deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

Asimismo cualquier persona que por razón del ejercicio de sus funciones tenga acceso a los datos deberá de observar la debida reserva, confidencialidad y sigilo en relación con las mismas.

El responsable deberá informar a las personas con acceso a los datos del deber de secreto a que se refiere el apartado anterior.

Disposición transitoria.

Los responsables de ficheros de videovigilancia ya inscritos en el Registro General de la Agencia Española de Protección de Datos deberán adoptar las medidas previstas en el artículo 3, letra a), y en el artículo 4.3 de esta Instrucción en el plazo máximo de tres mes desde su entrada en vigor.

Disposición final.

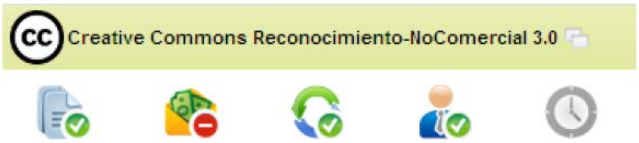
La presente Instrucción entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Madrid, 8 de noviembre de 2006.–El Director de la Agencia Española de Protección de Datos, José Luis Piñar Mañas.

Anexo.

1. El distintivo informativo a que se refiere el artículo 3.a) de la presente Instrucción deberá de incluir una referencia a la «LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS», incluirá una mención a la finalidad para la que se tratan los datos («ZONA VIDEOVIGILADA»), y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

2. El modelo a que se refiere el apartado anterior, está disponible en la página web de la Agencia Española de Protección de Datos, www.agpd.es, de donde podrá ser descargado, especificando los datos del responsable.



ALCATRAZ SOLUTIONS
902 169 121
www.lopdgest.com

CSA
947 256 250
www.csa.es