PROTECCIÓN DE DATOS EN LA EMPRESA

CEA Confederación de Empresarios de Andalucía
CEAT Andalucía
Federación Andaluza de Autónomos
Servicio Andaluz de Empleo
Consejería de Empleo

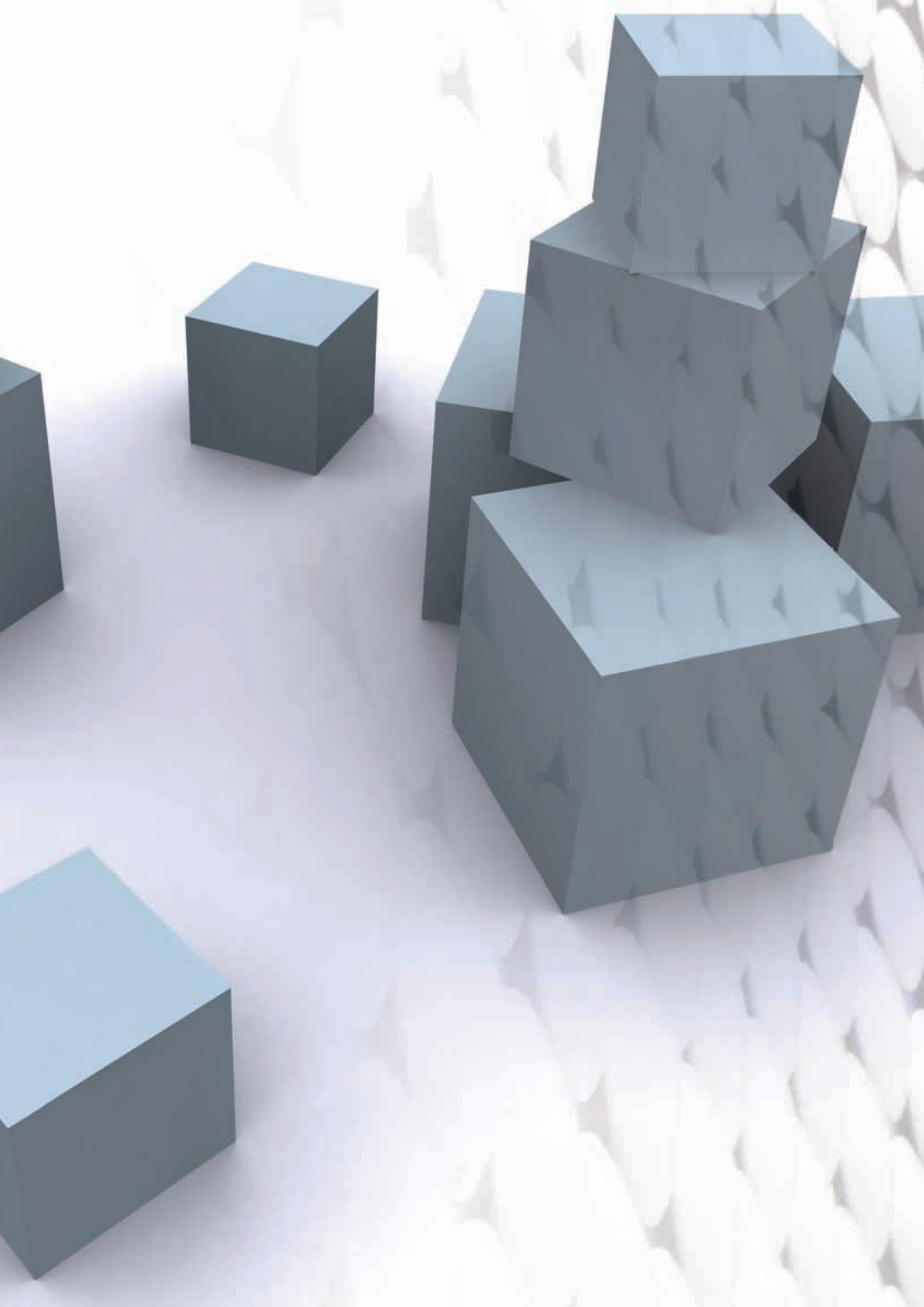
Imagen: Photoxpress

© Maksim Pasko
© Sergey Tokarev
© Yurok Aleksandrovich
© Dinostock
© Stèphan Szeremeta
© e-pyton
© Jan Will
© Dinostock
© Dinostock
© Unclesam

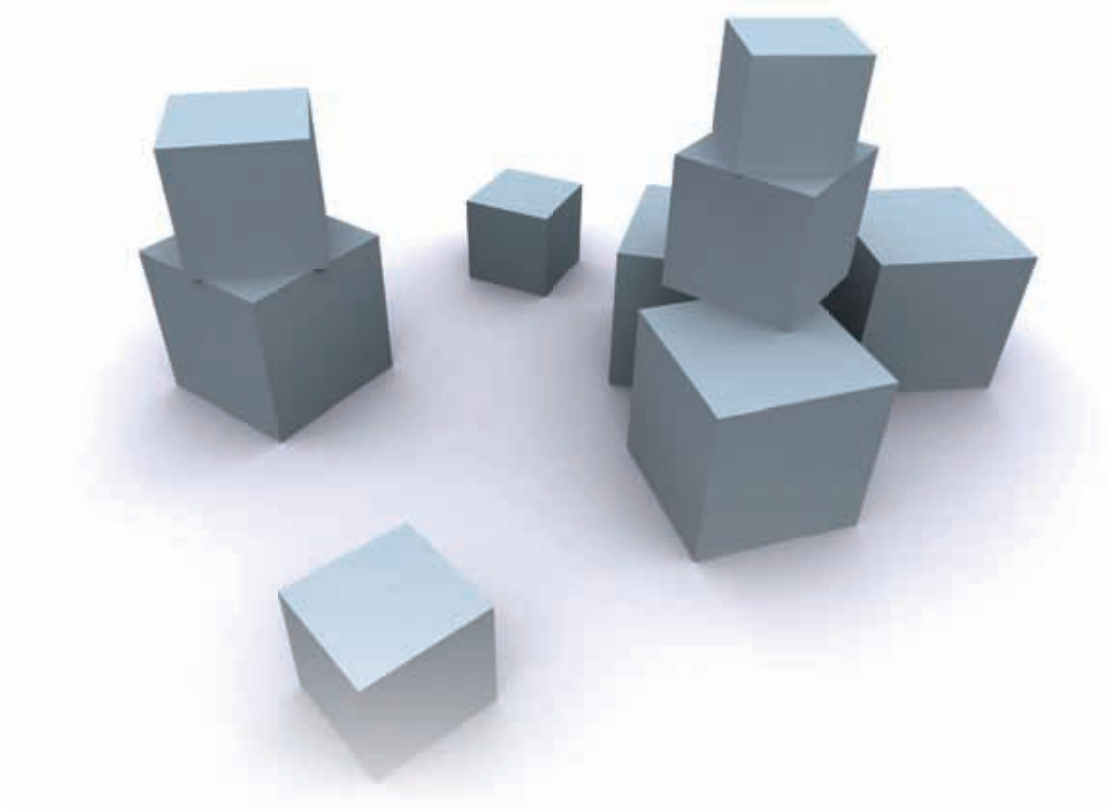
© Supertrooper
© Mykola Velychko
© Saskia Massink
© Dinostock
© EMILLENNIUM
© T. Tulic
© PaulPaladin
© Araraadt
© Dinostock
© Orlando Florin Rosu

© Dinostock
© Aloysius Patrimonio
© Stephen Orsillo
© Paul Moore
© MVit
© Dmitry Goygel-Sokol
© Chester F
© Nicemonkey
© Sophie
© Dinostock

© Dinostock
© Mariolina
© Ivan Hafizov
© .shock
© Valentin Mosichev
© Julien Tromeur
© Paul Moore
© Blaine Stiger



Unidad 0
Introducción



UNIDAD DIDÁCTICA 0 // INTRODUCCIÓN

1. DICOTOMÍA ENTRE EL DERECHO A LA INTIMIDAD Y EL DERECHO A LA INFORMACIÓN EN EL DERECHO ESPAÑOL

Una cuestión muy polémica y de máxima actualidad es la delimitación de los límites entre el derecho a la intimidad y el derecho a la información.

Ambos derechos están comprendidos entre los derechos fundamentales y libertades públicas que gozan de la máxima protección constitucional (arts. 18.1 y 20.1.d. de la Constitución, respectivamente).

Podemos definir la intimidad como la «parte más reservada o más particular de los pensamientos y afectos o asuntos interiores de una persona, familia o colectividad», entendiendo «interior» como aquello que sólo se siente en la conciencia, y por «lo particular» como lo propio y privativo. En definitiva, es una esfera de la persona ajena a la vida socio-política organizada, cuyo conocimiento por terceros no afecta a las necesidades propias de una sociedad democrática. En la Exposición de motivos de la derogada LORTAD, se afirma que la intimidad «protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos...-». Incorporando un nuevo concepto, «la privacidad», que supone para el legislador un alcance mayor de intrusión en la vida personal.

Por otro lado, los derechos de expresión y de información están limitados por el imperativo constitucional de respeto a los demás derechos fundamentales, por los preceptos de las leyes que los desarrollan y, especialmente, en el derecho al honor, a la intimidad... (Art. 20.4 CE).

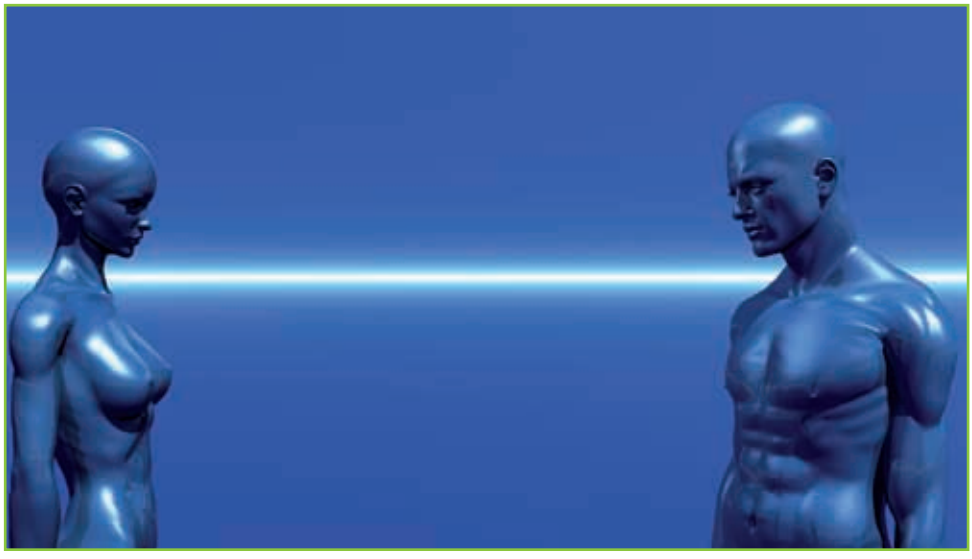
Por supuesto que la diferenciación entre «personas públicas» de «personas privadas» y la notoriedad o no de los datos personales, darán una protección diferenciada que no puede tener el mismo alcance para todos. La Jurisprudencia imperante del Tribunal Constitucional y del Tribunal Supremo va en esa dirección.

2. LA PROTECCIÓN DE LOS DATOS PERSONALES EN LA CONSTITUCIÓN

El artículo 18.4 de la Constitución Española de 1978 establece 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»*.

Ése es, necesariamente, nuestro punto de arranque para considerar si tal protección se cumple o no se cumple, o se cumple mal respecto a la automatización de la información sobre datos personales y/o familiares, y sobre la utilización de los datos informatizados por parte de los poderes públicos.

En consecuencia, consideraremos primero el soporte constitucional de la protección y el alcance de dicha protección, para después considerar la protección establecida en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal (LOPD), que, como venimos repitiendo, sustituye a la LO 5/1992, de 29 de octubre (LORTAD), tanto en lo que se refiere a las Administraciones Públicas y la protección de los derechos personales frente a los ficheros de titularidad pública, como los de titularidad privada.

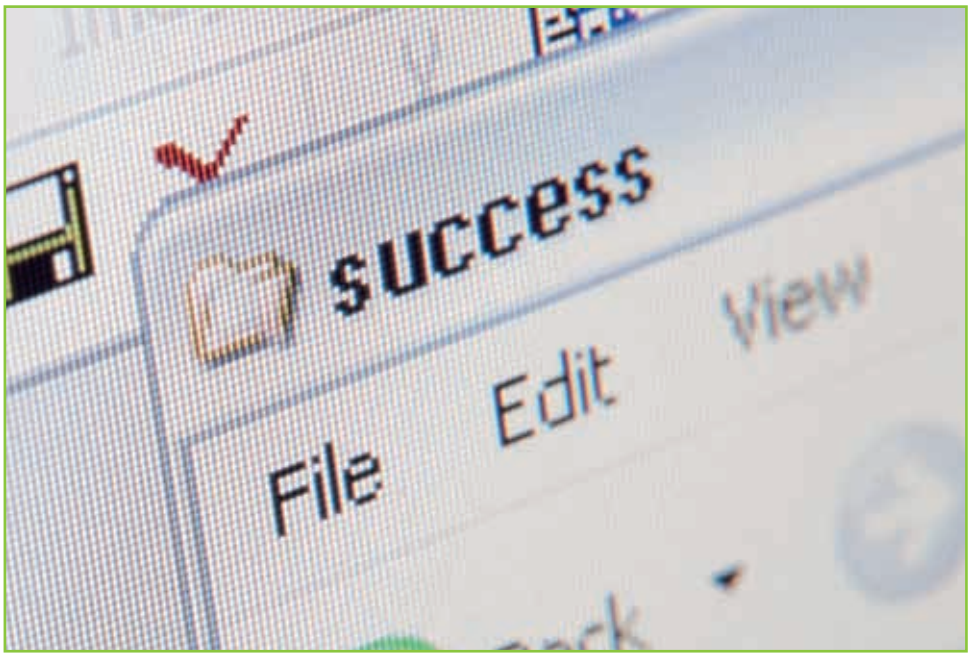


2.1. ALCANCE PROTECTOR DEL ART. 18.4

Por una parte, el art. 18.4 de la Constitución española consagra el principio de 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»*. Los principios de tutela que consagra sólo son aplicables al «ciudadano», es decir, al español. La posible protección de extranjeros vendrá dada en virtud de acuerdos de reciprocidad o de Convenios internacionales, respecto a los ciudadanos de los Estados que los suscriban y acepten. Más adelante haremos referencia al Convenio 108 del Consejo de Europa y al Convenio de Schengen, ambos ratificados por España.

En cumplimiento de lo que dispone el art. 18.4 de la CE, pero también de los compromisos internacionales contraídos por España, con los dos Convenios citados, se promulga la LO 5/1992 (LORTAD), recientemente sustituida por la LO 15/1999 (LOPD), de Protección de Datos de Carácter Personal, que estudiaremos especialmente.

Pero también la Constitución Española, en su Título IV dedicado al Gobierno y Administración, en el art. 105 b), prevé otra garantía de los ciudadanos según la cual, por Ley, se regulará el acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas. Aquí nada se dice de informática, pero queda implícito que ese derecho que se reconoce a los ciudadanos de acceso a archivos y registros no excluye, en principio, soporte alguno que pueda contenerlos. Por consiguiente, también hay que aplicarlo respecto a archivos y registros realizados en soporte automatizado o no de datos personales.



También en la LORTAD y su sucesora, la LOPD, vemos la aplicabilidad de este principio constitucional como Ley que hace ejercitable el derecho constitucional de acceso a tales datos.

La Constitución establece un derecho de protección frente al uso de la informática y, por su propia ubicación en el texto constitucional, constituye un derecho fundamental específicamente protegido.

El contenido de ese derecho o libertad es concretado particularmente referido al **derecho al honor** (personal y familiar) y a la **intimidad personal y familiar** de los ciudadanos (no de las personas jurídicas), respecto al tratamiento informático. Supone una garantía específica de tales derechos, que son reconocidos como tales en el mismo art. 18 de la CE, punto 1.

La insistencia constitucional para la protección de este derecho se manifiesta también en el enunciado del art. 20.4 de la CE, que pone límites a la libertad de expresión y de información, también derechos fundamentales, al establecer que *«estas libertades tienen su límite en el respeto a los derechos reconocidos en este título (Título 1 «De los derechos y deberes fundamentales», arts. 10 a 55 de la CE), en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia»* (LO 1/1982, de 5 de mayo, de protección civil del honor, la intimidad la propia imagen, y su corrección por la LO 3/1985).

Es, pues, un derecho fundamental de libertad, para ejercer cualquier derecho, frente a los obstáculos o intrusiones que puedan producirse con la utilización de la información autocrática (Sentencia del TC de 20 de julio de 1993). Se trata, pues, de **un derecho fundamental del ciudadano consistente en la libertad de ejercicio de todos los derechos frente a la informática.**

ASPECTOS A RECORDAR

- Es la Constitución española la que enmarca la protección de datos personales, al encuadrarla entre los derechos y libertades fundamentales.
- La Ley Orgánica de Protección de Datos (que deroga a la antigua LORTAD), y su reglamentación normativa posterior, viene desarrollar ese principio de la C.E.

Unidad 1

Marco General de la Protección de Datos

UNIDAD DIDÁCTICA 1 // MARCO GENERAL DE LA PROTECCIÓN DE DATOS

1. MARCO NORMATIVO

El marco normativo regulador de los derechos de los ciudadanos a la protección de sus datos personales tiene una **múltiple vertiente geográfica y una rica evolución temporal**.

1.1. ÁMBITO INTERNACIONAL

Acuerdo de Schengen

El Convenio de aplicación del Acuerdo de Schengen, de 14 de junio de 1985, relativo a la supresión gradual de los controles en las fronteras comunes, de 19 de junio de 1990, en su artículo 118 especifica las medidas que cada uno de los países firmantes del Convenio se compromete a adoptar en la parte nacional del Sistema de Información de Schengen:

- Control en la entrada a las instalaciones.
- Control en los soportes de datos.
- Control en la entrada de datos.
- Control de la utilización.
- Control de acceso.

- Verificación de la transmisión
- Auditoría del tratamiento
- Control del transporte

Deberá garantizarse la seguridad de los datos transmitidos a servicios situados fuera de su territorio debiéndose comunicar las medidas adoptadas a la autoridad de control.

1.2. UNIÓN EUROPEA

Convenio 108 del Consejo de Europa

Aparte de las referencias a las medidas de seguridad que se hacen en la Memoria Explicativa del Convenio, el artículo 7 de éste se dedica a la seguridad de los datos.

«Se tomarán las medidas de seguridad apropiadas para la protección de los datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.».

- 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.

- Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (DOCE L178 de 17 de julio de 2000). (Directiva comercio electrónico).

- Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Esta Directiva deroga la Directiva 97/66 del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

1.3. ESPAÑA

- Constitución Española.

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD).

- 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, (LORTAD) (BOE núm. 147 de 21 de junio de 1994). (Reglamento).

- 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 (BOE núm. 151 de 25 de junio de 1999). (Reglamento de Seguridad).

- Instrucción 1/2000, de 1 de diciembre, de la Agencia Española de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos (BOE núm. 301 de 16 de diciembre de 2000). (Instrucción).

- Sentencia 292/2000 del Tribunal Constitucional, donde se declararon inconstitucionales varios preceptos de la LOPD.

ASPECTOS A RECORDAR

Destacan:

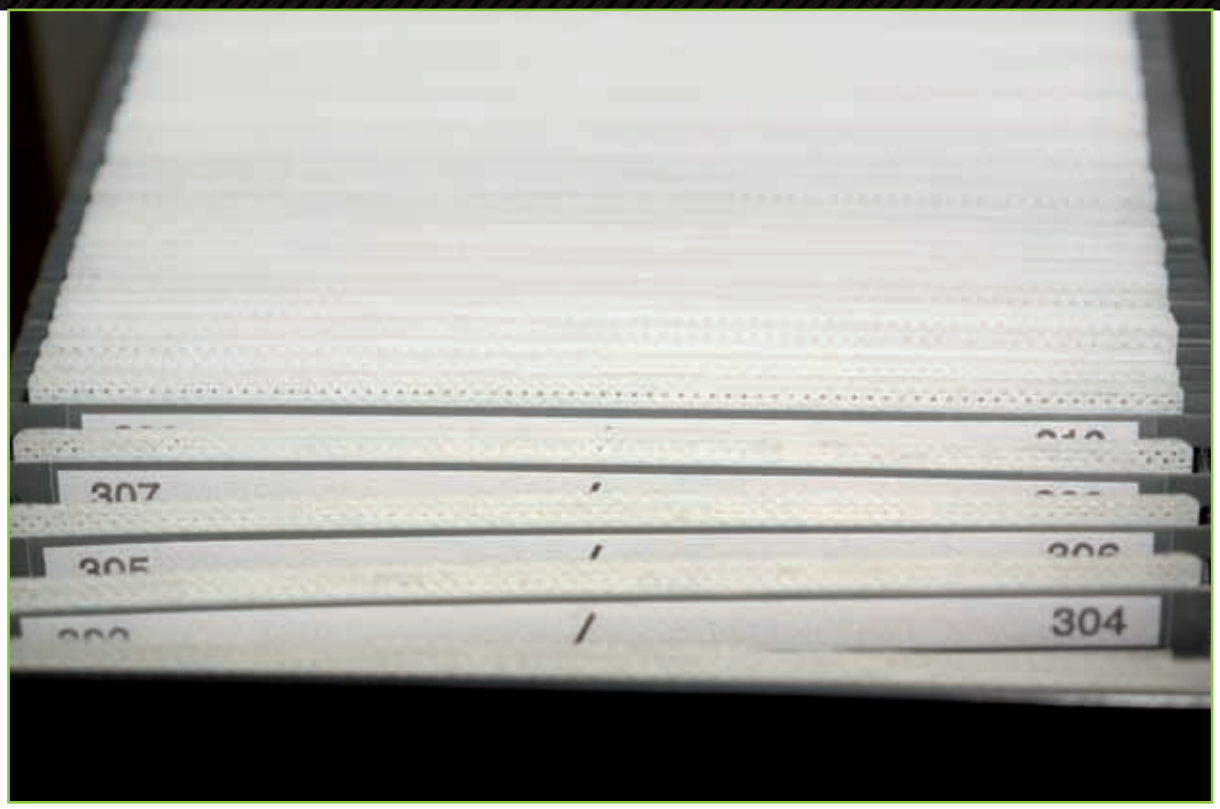
- Internacional: Schengen.
- U.E.: Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002.
- España: LOPD y su Reglamento de medidas de seguridad, acompañados por los reglamentos de creación de las Agencias de Protección de Datos.

2. LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS (LOPD)

2.1. ÁMBITO DE APLICACIÓN

2.1.1 Ámbito subjetivo: ¿A quién alcanza el carácter de dato personal?

El artículo 1 de la LOPD dispone literalmente que *"la presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y, especialmente, de su honor e intimidad personal y familiar"*, ostentando, en consecuencia, la condición de comerciante (es el caso de los profesionales liberales cuyas actividades están expresamente excluidas del ámbito de aplicación de la Ley Básica 3/1993 en su artículo 6) y, los segundos, cuando no fuera posible diferenciar su actividad mercantil de la propia actividad privada. En estos dos casos deberán aplicarse



siempre las garantías de la Ley Orgánica 15/1999, dada la naturaleza fundamental del derecho a proteger. Ello exigirá siempre ir analizando caso por caso para hallar, en cada supuesto concreto, el límite fronterizo donde resulte afectado el derecho fundamental a la protección de datos de los interesados, personas físicas o, por el contrario, aquél no resulte amenazado por incidir tan sólo en la esfera de la actividad comercial o empresarial, teniendo en todo caso presente que, en caso de duda, la solución deberá siempre adoptarse a favor de la protección de los derechos individuales.

Todo esto se complementa con lo dispuesto por la AEPD en respuesta a una consulta sobre la aplicación de la Ley a ficheros que contienen datos relacionados con empresarios individuales (Memoria 1999), según la cual: *"Al propio tiempo se ha venido indicando por la Agencia que los datos referidos a empresarios individuales no pueden entenderse amparados en la LORTAD en el ejercicio de su actividad mercantil, dado que su objeto consiste en la protección de la intimidad personal y familiar de las personas físicas, siendo así que no puede entenderse que las empresas gocen de la citada intimidad. Por tanto, no puede ser aplicable a esas personas la protección consagrada por la LORTAD, ni siquiera cuando su actividad se identifique plenamente con la de una persona física determinada, habida cuenta que el ámbito personal que se protege debe ser considerado como distinto del empresarial"*.

No obstante, debe tenerse en cuenta que la nueva Ley Orgánica 15/1999 extiende su manto protector más allá de la mera protección del derecho a la intimidad personal y familiar para consagrar el denominado derecho a la **autodeterminación informativa**, por lo que es objeto de la Ley **la protección de cualesquiera derechos fundamentales y libertades públicas de las personas físicas frente al tratamiento de sus datos de carácter personal**. Ello supone que, si bien los empresarios individuales, en el ejercicio de su actividad mercantil, pueden carecer de un derecho a la intimidad personal y familiar, sin embargo, el tratamiento de los datos referidos

a los mismos podrá suponer una vulneración de otros derechos que les atribuye la Constitución (por ejemplo, el tratamiento de los datos relacionados con pertenencia de un empresario a una determinada asociación puede vulnerar el derecho de asociación, consagrado por el artículo 22 de la Constitución).

Así pues, sin perjuicio de que sea preciso realizar un análisis en cada caso concreto, el punto de partida lo constituye sin duda la premisa de que **sólo y exclusivamente los datos de carácter personal de personas físicas son objeto de protección por la LOPD**.

2.1.2. Ámbito objetivo: ¿Qué es un dato de carácter personal?

Dispone el artículo 2 de la LOPD que *"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 use posterior de estos datos por los sectores público y privado"*. Definiendo posteriormente dato de carácter personal como *«cualquier información concerniente a personas físicas identificadas o identificables»*.

Por otro lado, vemos que el concepto de dato de carácter personal no puede ser más amplio, previsión de la Ley que nos parece meritoria, pues su amplitud facilita su adaptación a la constante evolución de la informática. Esa amplitud se ve, además, ratificada por lo ya dispuesto en el artículo 1.4 del Real Decreto 1332/1994, de 20 de junio, al identificarlo como *"toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier tipo susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable"*. Esa extensión conceptual debe evidenciarnos la intención del legislador por adoptar un concepto de dato de carácter personal en el que quepan no sólo nombres, apellidos, número de afiliación,... sino también imágenes, sonidos y voces, con la única limitación de que estos datos resulten suficientes para identificar a su titular. No se discrimina, por tanto, información alguna; cualquier detalle o pormenor de una persona física que permita identificarla tiene la categoría de dato de carácter personal.

2.2. ESTRUCTURA

2.2.1. Estructura normativa

La LOPD está estructurada en **7 títulos y varias Disposiciones Adicionales, Transitorias y Finales.**

La estructura de la citada norma es, pues, la que sigue:

- TÍTULO I: Disposiciones generales.
- TÍTULO II: Principios de la Protección de Datos.
- TÍTULO III: Derechos de las personas.

- TÍTULO IV: Disposiciones Sectoriales.
  - CAPÍTULO I: Ficheros de titularidad pública.
  - CAPÍTULO II: Ficheros de titularidad privada.
- TÍTULO V: Movimiento internacional de datos.
- TÍTULO VI: Agencia de Protección de Datos.
- TÍTULO VII: Infracciones y sanciones.
  - DISPOSICIONES ADICIONALES.
  - DISPOSICIONES TRANSITORIAS.
  - DISPOSICIÓN DEROGATORIA.
  - DISPOSICIONES FINALES.

La Ley, al igual que su Reglamento de Medidas de Seguridad, se encuentra en los Anexos.

2.2.2. Estructura lógica y análisis

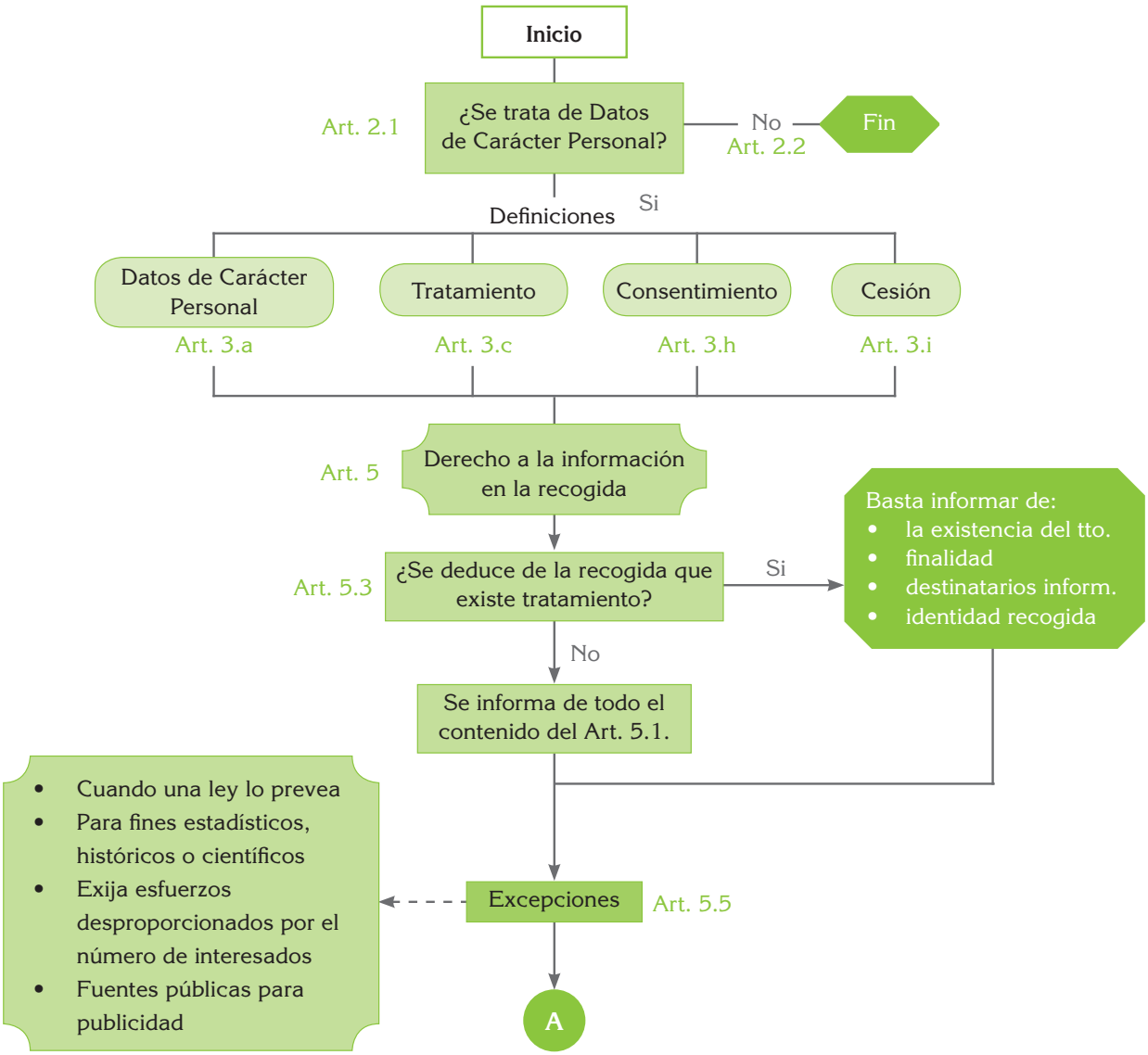
Para este análisis se procede a representar los aspectos significativos de la L.O. de forma gráfica y secuencial utilizando para ello un diagrama de flujo o esquema, tal que sea de una mayor facilidad el seguimiento de cada uno de los preceptos claves en este estudio, indicando al lado de cada elemento gráfico el artículo al que hace referencia.

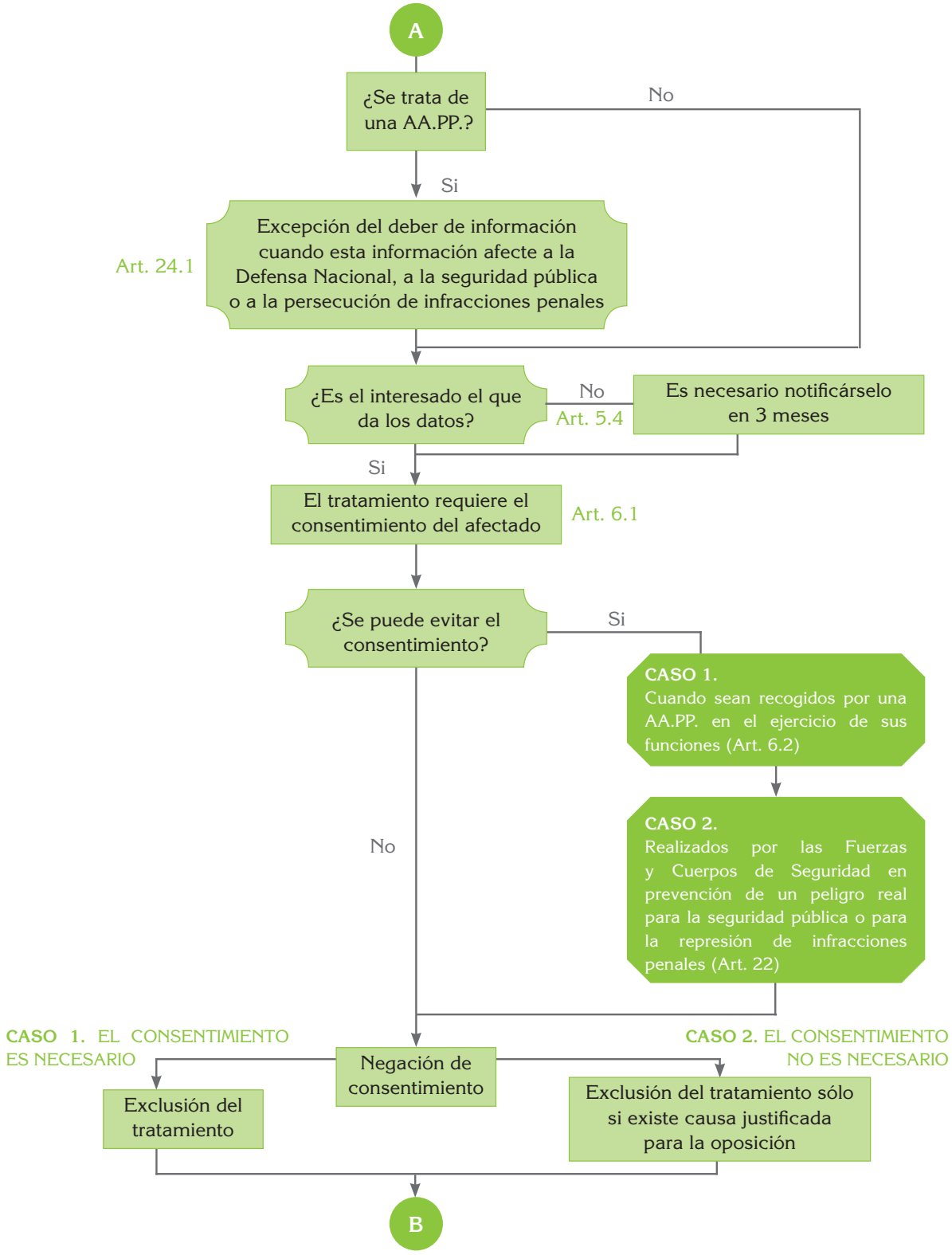
A priori, es necesario resaltar los siguientes aspectos de esta LOP 15/1999:

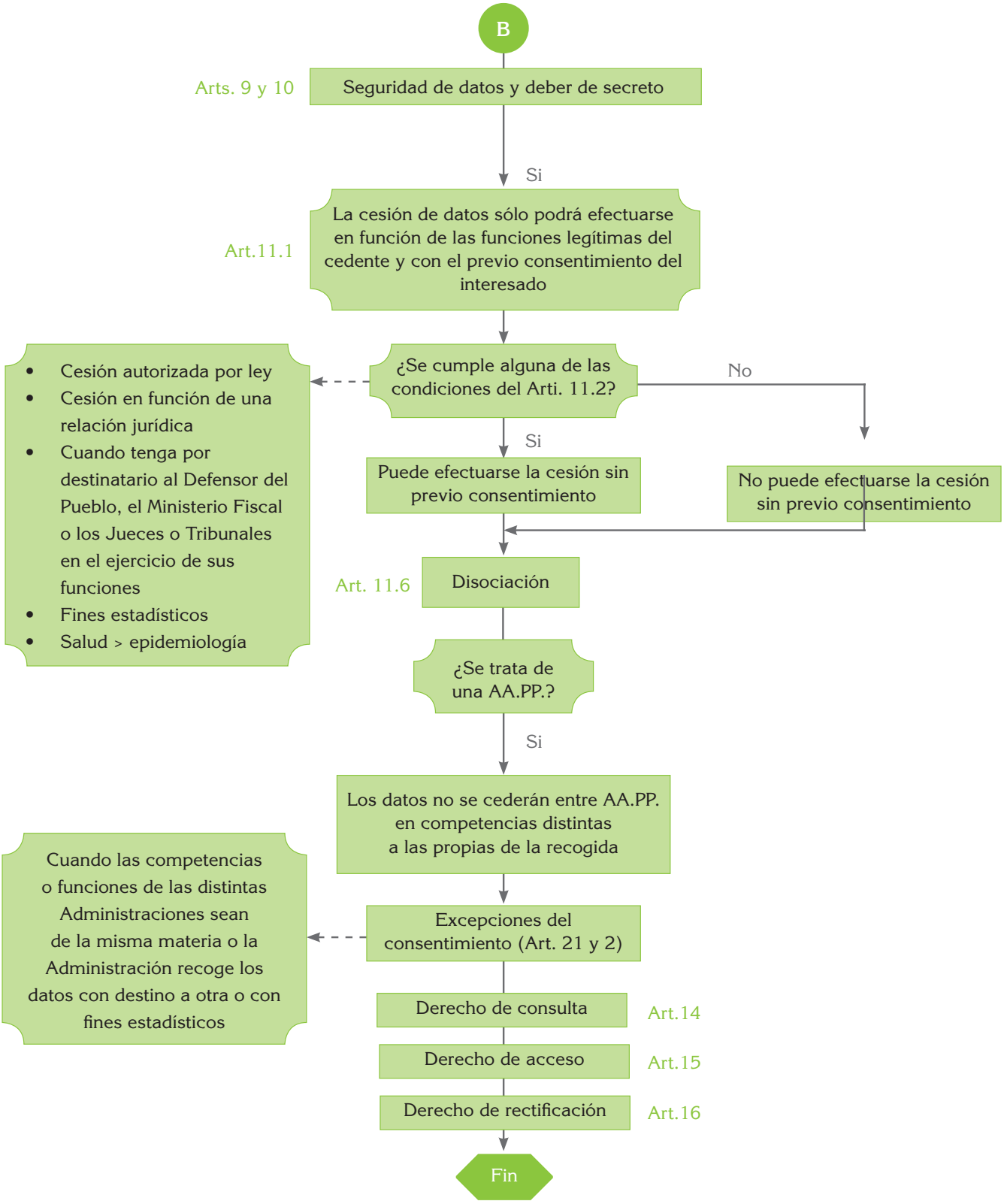
- Conceptos generales de *"dato de carácter personal"*, *"tratamiento de datos"*, *"comunicación o cesión de datos"*, *"consentimiento"*, etc.
- El derecho a la información de todo ciudadano a conocer la existencia de un fichero y / o tratamiento de los datos que se le requieren, así como las excepciones a este derecho.
- El consentimiento que ha de prestarse por cada afectado para que sus datos se graben en ese fichero o se les añada al tratamiento indicado, así como las excepciones a dicho consentimiento.
- La cesión de datos entre dos entidades o dos AA.PP., donde ha de preverse un consentimiento por parte del interesado para que pueda hacerse legítimamente, exceptuándose éste en algunos casos puntuales indicados en la LOPD.
- El derecho de acceso, rectificación y cancelación que todo ciudadano puede ejercitar sobre los datos de carácter personal relativos a su persona que sean sometidos a tratamiento por parte de entidades, organismos, empresas o administraciones, salvo en determinados casos en los cuales estos derechos se encuentran limitados.

Estos puntos se irán tratando en este Manual en el orden lógico ya planteado.

A continuación se indica el esquema explicativo de estos conceptos:




A
¿Se trata de una AA.PP.?
No
Si
Art. 24.1
Excepción del deber de información cuando esta información afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales
¿Es el interesado el que da los datos?
No
Art. 5.4
Es necesario notificárselo en 3 meses
Si
El tratamiento requiere el consentimiento del afectado
Art. 6.1
¿Se puede evitar el consentimiento?
Si
CASO 1.
Cuando sean recogidos por una AA.PP. en el ejercicio de sus funciones (Art. 6.2)
CASO 2.
Realizados por las Fuerzas y Cuerpos de Seguridad en prevención de un peligro real para la seguridad pública o para la represión de infracciones penales (Art. 22)
No
CASO 1. EL CONSENTIMIENTO ES NECESARIO
Negación de consentimiento
CASO 2. EL CONSENTIMIENTO NO ES NECESARIO
Exclusión del tratamiento
Exclusión del tratamiento sólo si existe causa justificada para la oposición
B


B
Arts. 9 y 10
Seguridad de datos y deber de secreto
Si
Art.11.1
La cesión de datos sólo podrá efectuarse en función de las funciones legítimas del cedente y con el previo consentimiento del interesado
¿Se cumple alguna de las condiciones del Arti. 11.2?
Cesión autorizada por ley
Cesión en función de una relación jurídica
Cuando tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales en el ejercicio de sus funciones
Fines estadísticos
Salud > epidemiología
No
Si
Puede efectuarse la cesión sin previo consentimiento
No puede efectuarse la cesión sin previo consentimiento
Art. 11.6
Disociación
¿Se trata de una AA.PP.?
Si
Los datos no se cederán entre AA.PP. en competencias distintas a las propias de la recogida
Cuando las competencias o funciones de las distintas Administraciones sean de la misma materia o la Administración recoge los datos con destino a otra o con fines estadísticos
Excepciones del consentimiento (Art. 21 y 2)
Derecho de consulta
Art.14
Derecho de acceso
Art.15
Derecho de rectificación
Art.16
Fin

ASPECTOS A RECORDAR

- Delimitación del ámbito de la LOPD a personas físicas.
- Exclusión de personas jurídicas.
- Caso particular: autónomos y empresarios individuales.
- Amplitud del concepto de Dato Personal.
- Secuencia lógica de obtención de datos, cesiones y consentimientos.

3. CONCEPTOS

3.1. DATOS DE CARACTER PERSONAL

Cualquier información concerniente a personas físicas, identificadas o identificables.

Dentro de esta categoría hay que distinguir:

A. Datos especialmente protegidos

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. 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 precisara siempre el previo consentimiento del afectado.

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.

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.

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.

No obstante, lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal relativos a la salud, 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.

B. Datos relativos a la salud

Son datos especialmente protegidos por su importancia personal.

Sin perjuicio de lo que se dispone en el articulo 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.

3.2. FICHERO

Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

3.3. 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.

3.4. RESPONSABLE DEL FICHERO O TRATAMIENTO

Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y use del tratamiento.

3.5. AFECTADO O INTERESADO

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

3.6. DISOCIACIÓN

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

3.7. ENCARGADO DEL TRATAMIENTO

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

3.8. CONSENTIMIENTO DEL INTERESADO

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

3.9. CESIÓN O COMUNICACIÓN DE DATOS

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

3.10. 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.

3.11. SISTEMA DE INFORMACIÓN

Conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

3.12. USUARIO

Una persona física que utiliza con fines privados o comerciales un servicio de comunicaciones electrónicas disponible para el público, sin que necesariamente se haya abonado ha dicho servicio (Directiva sobre la privacidad y las comunicaciones electrónicas).

Sujeto o proceso autorizado para acceder a datos o recursos.

3.13. DOCUMENTO DE SEGURIDAD

Documento de obligado cumplimiento donde se llevarán todos los registros oportunos en materia de Protección de Datos. Cada documento es distinto según el nivel de seguridad que se deba adoptar. Dicho documento deberá estar siempre disponible por si se lo requiere la Agencia de Protección de Datos, y no ha de estar inscrito: lo que se inscribe es el fichero -nos referimos a los datos que sobre el fichero se le pidan-, no el documento. Por cada fichero debe de existir un Documento de Seguridad, sin embargo, pensamos que es más flexible agrupar los de los ficheros según el nivel de seguridad de estos y realizar un Documento de Seguridad para cada uno de ellos (por ejemplo, un Documento de Seguridad para todos los ficheros que contengan Medidas de Seguridad de nivel básica).

El documento está compuesto de **dos partes**: **un texto explicativo** donde redactaremos las obligaciones del personal, obligaciones generales, medidas a adoptar, y un **libro de registros** donde llevaremos los registros oportunos. La Ley advierte que ha de ser el Responsable del Fichero (en nivel básico) o el Responsable de Seguridad quien proceda a la cumplimentación.

4. AGENTES DE CONTROL Y FUNCIONES

4.1. AGENCIA GENERAL DE PROTECCIÓN DE DATOS

En un principio su denominación era Agencia de Protección de Datos pero la Ley 62/2003, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social le cambió la denominación a esta que posee en la actualidad.

4.1.1. Normativa regente

Le son de aplicación:

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (Título VI con rango de ley ordinaria).
- Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.
- Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en defecto de ambas.

4.1.2. Naturaleza

Ente de Derecho Público con personalidad jurídica propia y plena capacidad pública y privada, que actúa con independencia de las Administraciones Públicas en el ejercicio de sus funciones y que se relaciona con el Gobierno a través del Ministerio de Justicia.

4.1.3. Régimen Jurídico

- Régimen General (Excluida de la LOFAGE).
- Ejercicio competencias / Ley 30/1992, de 26 de noviembre.
- Régimen Patrimonial / Derecho Privado.
- Contratación / Derecho Privado.
- Régimen Personal / Funcionarios de las Administraciones Públicas y personal contratado según la naturaleza de las funciones.
- Régimen Presupuestario: Presupuesto integrado, con la debida independencia, en los Presupuestos Generales del Estado.
  - Control Externo: Tribunal de Cuentas.
  - Control Interno: IGAE.

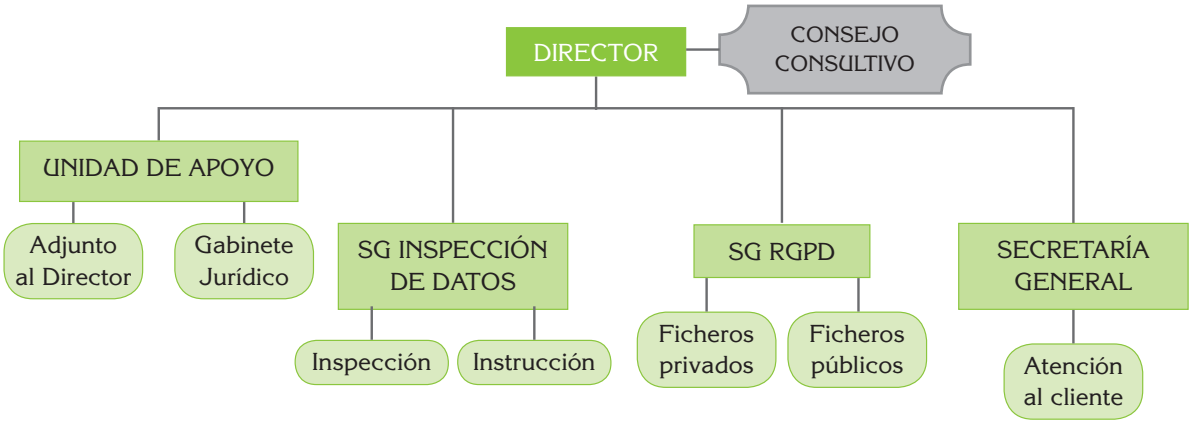
4.1.4. Funciones

Vienen reguladas en el artículo 37 de la LORD y se pueden clasificar en:

- **General:**
  - Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.
  - En relación con los afectados:
  - Atender a sus peticiones y reclamaciones.
  - Información de los derechos reconocidos en la Ley.
  - Promover campañas de difusión a través de los medios.
- **En relación con quienes tratan datos:**
  - Emitir autorizaciones previstas en la Ley.
  - Requerir medidas de corrección.
  - Ordenar, en caso de ilegalidad, el cese en el tratamiento y la cancelación de los datos.
  - Ejercer la potestad sancionadora.
  - Recabar ayuda e información que precise.
  - Autorizar las transferencias internacionales de datos.
- **En la elaboración de normas:**
  - Informar los Proyectos de normas de desarrollo de la LOPD.
  - Informar los Proyectos de normas que incidan en materias de protección de datos.
  - Dictar instrucciones y recomendaciones de adecuación de los tratamientos a la LORD.
  - Dictar recomendaciones en materia de seguridad y control de acceso a los ficheros.
- **En materia de telecomunicaciones:**
  - Tutelar los derechos y garantías de los abonados y usuarios en el ámbito de las comunicaciones electrónicas, incluyendo el envío de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico o medios de comunicación electrónica equivalente.

- **Otras funciones:**
  - Velar por la publicidad en los tratamientos publicando anualmente una lista de los mismos.
  - Cooperación Internacional.
  - Representación de España en los foros internacionales en la materia.
  - Control y observancia de lo dispuesto en la Ley reguladora de la Función Estadística.
  - Elaboración de una Memoria Anual, presentada por conducto del Ministro de Justicia a las Cortes.

4.1.5. Estructura



4.2. AGENCIAS DE COMUNIDADES AUTONÓMICAS

La creación de Agencias Autonómicas de Protección de Datos estaba prevista ya en el artículo 40 de la derogada LORTAD. La LORD, en el artículo 41, regula la creación de estos órganos de control:

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 0 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.».

Sus competencias se centran sobre los ficheros de datos de carácter personal creados o gestionados por la Administración de su ámbito territorial.

Al amparo de la LORTAD sólo se creó la Agencia de Protección de Datos de la Comunidad de Madrid mediante la Ley 13/1995, de 21 de abril, de regulación del uso de la informática en el tratamiento de datos personales por la Comunidad de Madrid, derogada por la vigente Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid.

Recientemente, y ya bajo la vigencia de la LOPD, se han creado dos nuevas agencias: la Agencia Catalana de Protección de Datos, en virtud de la Ley 2002, de 19 de abril, de creación de la Agencia Catalana de Protección de Datos, y la Agencia Vasca de Protección de Datos por 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.

Unidad 2

Tratamiento de Datos en la Empresa

UNIDAD DIDACTICA 2 // TRATAMIENTO DE DATOS EN LA EMPRESA

En esta Unidad vamos a estudiar los distintos aspectos de la LOPD con respecto al **tratamiento de datos** que, recordemos, se definía como: *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.*

1. AGENTES INVOLUCRADOS EN EL TRATAMIENTO DE DATOS

La protección de los datos de carácter personal trae consigo la aparición de una serie de figuras que inciden en menor o mayor medida en el tratamiento de los datos. Estas figuras son las siguientes: **responsable del fichero** o **responsable del tratamiento, titular de fichero, encargado del tratamiento, responsable del mantenimiento** y **encargado del mantenimiento, responsable propietario del fichero, responsable de seguridad, afectado** o **interesado** y **usuario**.

Vamos a definir a continuación dichas figuras para después enumerar sus principales funciones y obligaciones y, en su caso, derechos.

1.1. RESPONSABLE DEL TRATAMIENTO O DEL FICHERO

1.1.1. Definición

El artículo 3.d) de la LOPD lo define como *«persona física o jurídica, de naturaleza pública a privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento»*.

La LOPD introdujo cierta confusión al denominar una misma figura de dos formas diferentes y emplear en unos artículos *«responsable del fichero»* y en otros *«responsable del tratamiento»*, con lo que hubo quien entendió erróneamente que se trataba de dos figuras diferentes cuando en realidad era la misma figura con dos nombres distintos.

Las funciones y obligaciones del responsable del fichero, según los niveles de seguridad de los ficheros a los que nos referiremos en un capitulo posterior, son las siguientes:

1.1.2. Funciones

Nivel básico

- Decidir sobre la finalidad, contenido y uso del tratamiento (art. 3.d Ley).
- Autorizar la ejecución del tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero (art. 6 Reg. Seguridad).
- Elaborar el Documento de Seguridad (art. 8.1 Reg. Seguridad).
- Adoptar las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así coma las con secuencias a que daría lugar su incumplimiento (art. 9.2 Reg. Seguridad).
- Se encargará de que exista una relación actualizada de usuarios que tengan acceso autorizado al Sistema de Información (art. 11.1 Reg. Seguridad).
- Establecer los procedimientos de identificación y autentificación para dicho acceso (art. 11.1 Reg. Seguridad).
- Establecer mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados (art. 12.2 Reg. Seguridad).
- Establecer los criterios con que el personal autorizado para ello concede, altere o suprima el acceso a los ficheros que contengan datos de carácter personal y recursos (art. 12.4 Reg. Seguridad).
- Será quien, únicamente, pueda autorizar la salida, fuera de los locales en que esté ubicado el fichero, de soportes informáticos que contengan datos de carácter personal (art. 13.2 Reg. Seguridad).
- Verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y recuperación de datos (art. 14.1 Reg. Seguridad).
- Resolver sobre la petición de acceso en el plazo de un mes a contar desde la recepción de la solicitud (art. 12.3 Reg. Desarrollo).

- Resolver sobre la petición de rectificación o cancelación en el plaza de diez días a partir de la recepción de la solicitud (art. 15.2 Reg. Desarrollo modificado por el artículo 16.1 de la Ley).
- Proceder al bloqueo de los datos en los casos en que, siendo procedente su cancelación, no sea posible su extinción física, tanto por razones técnicas como por causa del procedimiento o soporte utilizado (art. 16 Reg. Desarrollo).
- Formular las alegaciones que considere pertinentes cuando la Agencia Española de Protección de Datos le de traslado de la reclamación de un afectado (art. 17.3 Reg. Desarrollo).

Nivel medio

- Designar uno o varios responsables de seguridad (art. 16 Reg. Seguridad).

1.1.3. Obligaciones

Nivel básico

- Excluirá del tratamiento los datos relativos al afectado que ejercite su derecho de oposición (art. 6.4 Ley).
- Adoptará 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 (art. 9 Ley).
- Estará obligado al secreto profesional y al deber de custodia, respecto de los datos de carácter personal de la instalación (art. 10 Ley).
- Hará efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días (art. 16.1 Ley).
- Si los datos rectificados o cancelados hubieran sido comunicados previamente, deberá notificar la rectificación o cancelación efectuada a quien se haya comunicado, en el caso de que se mantenga el tratamiento para este último, que deberá proceder a la rectificación o cancelación, en su caso (art. 16.4 Ley).
- En el momento en que se efectúe la primera cesión de datos, deberá informarse a los afectados (art. 27.1 Ley).

Nivel medio

- Adoptará las medidas correctoras adecuadas según las deficiencias detectadas en la auditoría (art. 17.3 Reg. Seguridad).
- 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 (art. 18.1 Reg. Seguridad).
- Autorizará por escrito la ejecución de los procedimientos de recuperación de datos (art. 21.2 Reg. Seguridad).

En muchos de estos casos podrá existir delegación de la función, pero en ningún supuesto, de la responsabilidad que, en cualquier caso, corresponde al responsable del fichero.

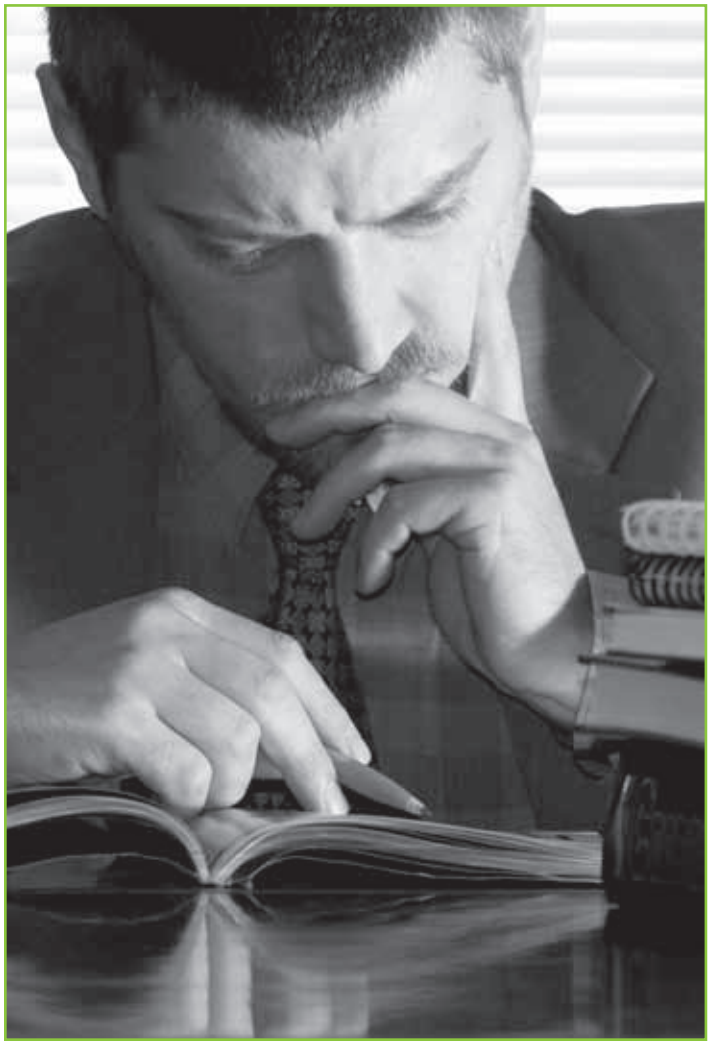
1.2. TITULAR DEL FICHERO

Esta figura sólo es contemplada en la normativa española de protección de datos en el artículo 10 de la LOPD al referirse al deber de secreto que deben guardar *«quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal»*.

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 aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo».

En este caso se diferencia titular del fichero y responsable del fichero.



1.3. ENCARGADO DEL TRATAMIENTO

1.3.1. Definición

El artículo 3.g) de la LOPD lo define como *«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»*.

Esta figura creó en su momento gran polémica debido a la interpretación que se diese a la parte de la definición que especifica: «por cuenta del responsable del tratamiento».

Se podría entender que el encargado del tratamiento fuera un empleado u organismo interno: Jefe o Departamento de Informática que realizaba el tratamiento por cuenta del responsable del fichero o tratamiento. Pero es un tercero externo con el que, según el artículo 12 de la Ley había que formalizar un contrato al que nos referiremos más adelante y que, a raíz de ello, contraería una serie de obligaciones que deben venir claramente especificadas en aquel.

1.3.2. Funciones

Realizar, por cuenta del responsable del fichero, los tratamientos que figuran en el contrato formalizado.

1.3.3. Obligaciones

- Tratará los datos conforme a las instrucciones del responsable del tratamiento.
- No los aplicará o utilizará con fin distinto al que figura en el contrato.
- No los comunicará, ni siquiera para su conservación, a otras personas.
- Deberá destruir o devolver al responsable del tratamiento los datos de carácter personal una vez cumplida la prestación contractual.
- Deberá destruir o devolver al responsable del tratamiento cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.
- Implantará las medidas de seguridad que correspondan según el nivel de seguridad de los ficheros.

Cobra especial importancia esta figura, dados los numerosos casos de subcontratación que se producen tanto en el sector privado como en el público.

DOCTRINA DE LA AEPD. ACLARACIONES SOBRE LA FIGURA DEL ENCARGADO DEL TRATAMIENTO

Se han recibido reiteradas consultas referidas al supuesto específico en que las actividades de una determinada empresa que implican un tratamiento automatizado de datos de carácter personal (nóminas, contabilidad, etc,) son efectuadas por una entidad asesora, sin que para la empresa se realice un tratamiento efectivo de dichos datos. En particular, se ha planteado a quien corresponderá el cumplimiento de las obligaciones reguladas por la LOPD.

De lo establecido en la mencionada Ley debe señalarse que las obligaciones que la misma impone, en particular la de proceder a la notificación del fichero a la Agencia Española de Protección de Datos, habrán de cumplirse por parte de quien ostente la condición de responsable del fichero, definido por el articulo 3.d) de la Ley como *"persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento"*.

Por tanto, la solución a la cuestión planteada deberá basarse en el hecho de si la empresa por cuya cuenta se procede al tratamiento de los datos decide sobre la finalidad y el modo en que se procederá a dicho tratamiento, con independencia de que por la misma se efectúen las operaciones que supongan la incorporación de los datos al fichero.

En concreto, en el caso en que la empresa facilite los datos a la gestoría, precisamente con la finalidad de que por la misma se desarrollen las debidas actividades de tratamiento de los datos (por lo que será la cliente quien decida sobre la finalidad y use de la información), aquella tendrá

la condición de responsable del fichero y deberá notificar su existencia al Registro General de Protección de Datos.

Dado que en este caso nos encontraremos ante un supuesto en que la gestoría tendrá la condición de encargado del tratamiento, la relación entre ambas entidades deberá someterse a lo dispuesto en el artículo 12 de la Ley, siendo de destacar las siguientes cuestiones:

- En lo que atañe a los requisitos formales de este tipo de contratos, el articulo 12.2 impone que *"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"*.
- Por lo que respecta al periodo de conservación de los datos, el artículo 12.3 establece que *"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"*, habiendo desaparecido la posibilidad de conservar los datos durante un periodo máximo de cinco años, que preveía el artículo 27.2 de la LORTAD.
- En lo referente a la cesión de los datos, de lo establecido en el artículo 12.2 se desprende que no procederá esa cesión, de forma que los datos habrán de ser entregados única y exclusivamente al responsable del fichero. Ello impide, a nuestro juicio, la posibilidad de proceder a una subcontratación de este tipo de servicios por parte del encargado del tratamiento, debiendo siempre el responsable ser parte en la relación jurídica, ya que cualquier transmisión de los datos a un tercero que no corresponda al responsable del fichero habrá de ser considerada cesión.
- En cuanto a las medidas de seguridad que hayan de ser adoptadas por quienes realicen trabajos de tratamiento de datos por cuenta de tercero, habrán de ser, en principio, las mismas que las impuestas al responsable del fichero, tal y como se desprende de lo previsto en los artículos 9 y 12.2 de la Ley Orgánica.
- Por último, según el artículo 12.4, *"en el caso de que el encargado de 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"*, siendo, en consecuencia, de aplicación el régimen sancionador establecido en los artículos 43 y siguientes de la Ley, sujetando el primero de ellos al encargado del tratamiento a dicho régimen.

1.4. RESPONSABLE DEL MANTENIMIENTO

La LOPD no define en ninguno de sus artículos esta figura y tan sólo se refiere a ella en el artículo 28, referido a los datos incluidos en las fuentes de acceso público.

Articulo 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 profesionales a que se refiere el artículo 3.1 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. ».

No se prevé ninguna sanción para el caso de que las entidades responsables del mantenimiento no cumplan lo solicitado por el colegiado. Por todo ello nos inclinamos a considerar que los responsables del mantenimiento son en realidad los responsables del fichero aunque igualmente en este caso el incumplimiento de la solicitud de un colegiado para que se indique que sus datos no pueden utilizarse para fines de publicidad o prospección comercial, dentro del ámbito de la LOPD, quedaría impune.

1.5. ENCARGADO DEL MANTENIMIENTO

Nos encontramos con una figura similar a la anterior por lo que sólo transcribiremos lo que al respecto dice el artículo 28.

"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."

1.6. RESPONSABLE PROPIETARIO DEL FICHERO

1.6.1. Definición

Esta figura no aparece en ninguna de las normas españolas sobre protección de datos de carácter personal y, por consiguiente, carece de algún tipo de responsabilidad ante la Agencia Española de Protección de Datos o ante las Agencias Autonómicas.

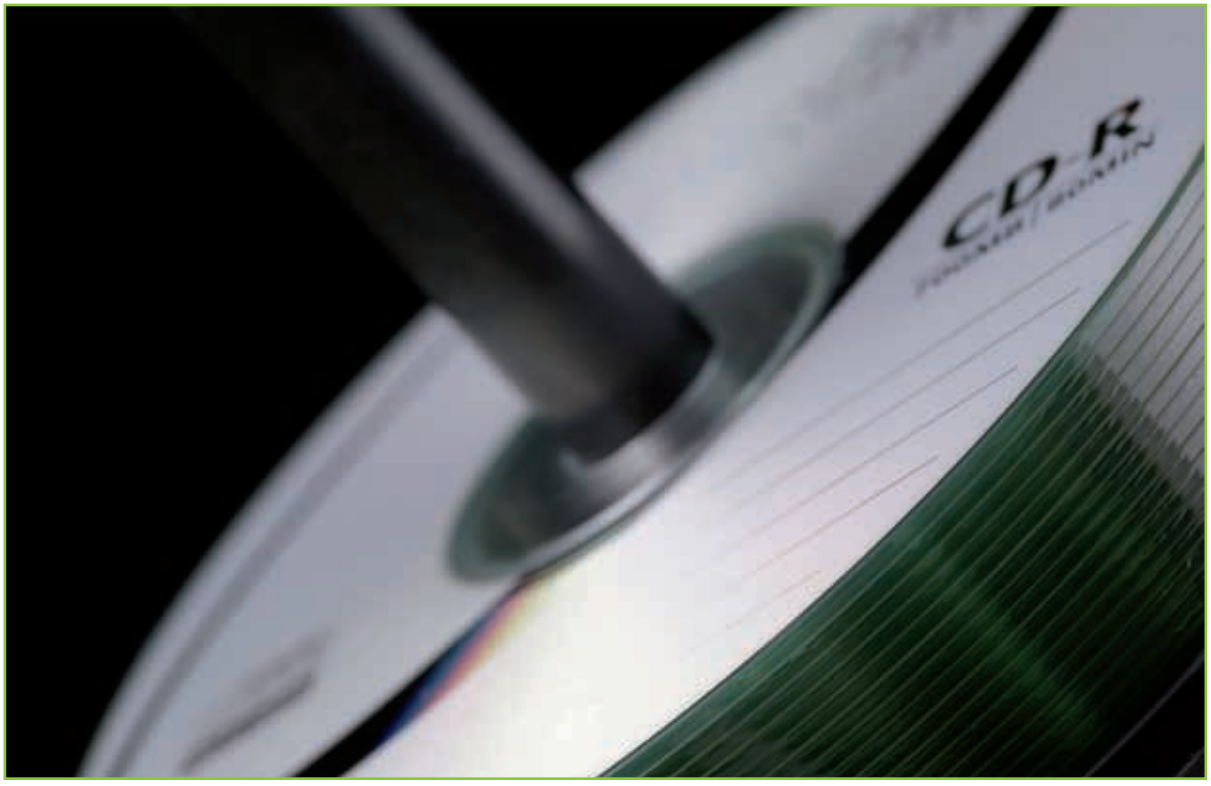
Su responsabilidad, tanto personal como profesional dentro de la organización, vendrá dada por el tipo de organización de que se trate.

El responsable propietario del ficheros será quien cree el fichero, lo mantenga y disponga las medidas de seguridad que considere necesarias, fije las normas para establecer las autorizaciones de acceso, y en definitiva, realice o pida al Departamento de Sistemas de Información que haga todo lo necesario para el buen use de su fichero, siendo el repetido Departamento de Sistemas

de Información el que facilite las herramientas necesarias para el tratamiento, pero habiéndose liberado de la responsabilidad directa sobre los datos y los ficheros aunque tenga la que le corresponde como custodio de los mismos.

1.6.2. Funciones

- Determinará quién puede acceder a los datos de carácter personal y que sean necesarios para la función que realice.
- Autorizará la realización de nuevos formularios de recogida de datos dentro de su Servicio o Unidad de forma que lleven incorporada la leyenda informativa, la cual tendrá que ser elaborada por la Asesoría Jurídica.
- Informará de la necesidad de creación de nuevos ficheros, con anterioridad a la misma, para poder desarrollar las funciones del Servicio o Unidad, de cara a que la Asesoría Jurídica ponga en marcha, en su caso, el procedimiento pare inscribirlo en la AEPD y solicitar el consentimiento si fuese necesario.
- Informará de la necesidad de realizar nuevas cesiones de datos de carácter personal para que la Asesoría Jurídica pudiese evaluar si es necesario el consentimiento.
- Informará en el caso de actuar la empresa como cesionario de datos de carácter personal para que la Asesoría Jurídica evalúe, en función del origen de la información, su legalidad.
- Estará al tanto del tratamiento de datos especialmente protegidos, en su caso, o la necesidad de añadir nuevos para poner en marcha los procedimientos pertinentes.



1.6.3. Obligaciones

- Velará porque se concedan y revoquen oportunamente las autorizaciones para acceder a los datos de los cuales es responsable.
- Guardará secreto de la información de carácter personal que conozca en el desempeño de su función aún después de haber abandonado la empresa (art. 10 Ley).

1.7. RESPONSABLE DE SEGURIDAD

1.7.1. Definición

Esta figura no aparece en el articulado de la LOPD pero sí en el Reglamento de medidas de seguridad, por lo que hemos de acudir a éste para averiguar sus funciones.

Según el artículo 16 del Reglamento, referido a los ficheros de nivel de seguridad medio y alto, será quien se encargará de coordinar y controlar las medidas definidas en el Documento de Seguridad.

No supondrá esta designación una delegación de responsabilidad que siempre corresponde al responsable fichero salvo la excepción del artículo 12 de la LOPD que puede incumbir al encargado del tratamiento.

1.7.2. Funciones

Nivel medio

- Coordinar y controlar las medidas de seguridad definidas en el Documento de Seguridad (art. 16 Reg. Seguridad).
- Analizar los informes de auditoría (art. 17.3 Reg. Seguridad).

Nivel alto

- Controlar los mecanismos que permiten el control de accesos (art. 24.3 Reg. Seguridad).

1.7.3. Obligaciones

Nivel medio

- Elevar al responsable del fichero las conclusiones del análisis del informe de auditoría (art. 17.3 Reg. Seguridad).
- Guardar secreto de los datos de carácter personal que pueda conocer, así como sobre controles y posibles debilidades, incluso después de haber causado baja en la entidad (art. 10 Ley).

Nivel alto

- Revisar periódicamente la información de control registrada (art. 24.5 Reg. Seguridad).
- Mensualmente elaborará un informe de las revisiones efectuadas (art. 24.5 Reg. Seguridad).
- Conocer la normativa interna en materia de seguridad, y especialmente la referente a protección de datos de carácter personal.
- Conocer las consecuencias que se pudieran derivar y las responsabilidades en que se pudiera incurrir en caso de incumplimiento de la normativa, que podrían derivar en sanciones.

Se trata de una figura muy interesante que debía estar presente en todas las organizaciones aunque no tuviesen datos de carácter personal ni ficheros de nivel medio y alto.

1.8. AFECTADO O INTERESADO

Según el artículo 3.e) de la LOPD es: *«persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo»*.

Este apartado c), al definir tratamiento de datos, dice lo siguiente: *«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»*.

Esta figura cobra especial importancia, pues nos va a determinar quiénes van a ser objeto de protección en la LOPD y quiénes no van a estar amparados por ellas, como ya se comentó en la UD.I.

Con respecto a la citada polémica con los datos del empresario individual, y dada la dificultad que existe muchas veces Para determinar qué datos inciden en la esfera de la actividad privada del comerciante o profesional y cuáles inciden en la esfera de la actividad comercial o profesional lo aconsejable es que, ante la duda, el responsable del fichero notifique la creación del fichero que contenga dichos datos.

1.9. USUARIO

1.9.1. Definición

Según el artículo 2.2 del Reglamento de medidas de seguridad es: *«Sujeto o proceso autorizado pare acceder a datos o recursos»*.

Este personal en el primer caso, que suele estar unido al responsable del fichero por algún tipo de relación laboral, debe estar debidamente clasificado de tal forma que cada uno solo puede acceder a la información que precise pare el trabajo que está desarrollando y a ninguna más.

Aparte de este tipo de usuario que mantiene una determinada relación laboral, existe otro que cobra especial importancia con la incorporación al ámbito de aplicación de la LOPD de los ficheros de partidos políticos, sindicatos y comunidades religiosas. Se trata de aquellos afiliados o fieles que sin ningún tipo de relación jurídica y de forma gratuita colaboran con dichas instituciones, para lo cual tienen acceso a los ficheros de aquellos, cuyos datos suelen ser de nivel alto.

Entendemos que con dicho tipo de usuario se debe formalizar el correspondiente documento que les asimile a los encargados del tratamiento y que, por tanto, sean responsables de sus actos administrativamente con independencia de la sanción penal que les pudiese corresponder en el caso de incurrir en un delito.

Las funciones y obligaciones que vienen a continuación, afectarán a cada uno en función de su puesto de trabajo.

1.9.2. Funciones

- Accederá a los datos de carácter personal a los que esté autorizado, necesarios para la función que realice.
- Realizará funciones propias del puesto de trabajo.

1.9.3. Obligaciones

- Guardar secreto de la información de carácter personal que conozca en el desempeño de su función aún después de haber abandonado el Ayuntamiento (art. 10 Ley).
- Conocer la normativa interna en materia de seguridad, y especialmente la referente a protección de datos de carácter personal. Dicha normativa puede consistir en: normas, procedimientos, reglas y estándares, así como posibles guías.
- Cumplir lo dispuesto en la normativa interna vigente en cada momento.
- Conocer las consecuencias que se pudieran derivar y las responsabilidades en que pudiera incurrir en caso de incumplimiento de la normativa, que podrían derivar en sanciones.
- No intentar saltar los mecanismos y dispositivos de seguridad, evitar cualquier intento de acceso no autorizado a datos o recursos, informar de posibles debilidades en los controles, y no poner en peligro la disponibilidad de los datos, ni la confidencialidad o integridad de los mismos.
- Usar de forma adecuada, según la normativa, los mecanismos de identificación y autenticación ante los sistemas de información, tanto sean contraseñas como sistemas más avanzados: biométricos u otros, y en ambos casos mediante acceso local o a través de redes de comunicaciones, cuando esté así previsto. En el caso de contraseña: cumplir lo recogido en la normativa, especialmente en cuanto a asignación, sintaxis, distribución,

custodia y almacenamiento de las mismas, así como el cambio con la periodicidad que se determine.

- No utilizar el correo electrónico u otros medios de comunicación interna o con el exterior para transmitir mensajes que contengan o lleven adjuntos datos de carácter personal que por sus características, volumen o destinatarios puedan poner en peligro la confidencialidad o la integridad de los datos.
- No realizar transferencias de ficheros con datos de carácter personal entre sistemas o descargas en equipos salvo en los casos expresamente autorizados, y protegiendo después los contenidos para evitar su difusión o copias no autorizadas.
- Dirigir a impresoras protegidas los listados que contengan datos de carácter personal que requieran protección, y recogerlos con celeridad para evitar su difusión, copia o sustracción.
- No sacar equipos o soportes de las instalaciones sin la autorización necesaria, y en todo caso con los controles que se hayan establecido.
- Proteger los datos personales responsabilidad del tratamiento que excepcionalmente tuvieran que almacenarse o usarse fuera del lugar de trabajo: en el propio domicilio o en otras instalaciones alternativas tanto en sistemas fijos como en portátiles.
- Salir de los ordenadores personales o terminales cuando vaya a estar ausente de su puesto durante un tiempo superior al fijado en los procedimientos para cada caso, de modo que el sistema le pida alguna clave.
- Entregar cuando se le requiera por sus superiores jerárquicos, y especialmente cuando vaya a causar baja en el Ayuntamiento, las llaves, claves, tarjetas de identificación, material, documentación, equipos, contraseñas y cuantos activos sean propiedad de aquél.

ASPECTOS A RECORDAR

- Las máximas responsabilidades del responsable del fichero tratamiento.
- La necesidad de un contrato entre responsable y encargado de tratamiento.
- La importancia de contar con un responsable de seguridad en la empresa.
- Las obligaciones de los titulares y de los usuarios.
- Las funciones y responsabilidades del mantenimiento.

2. PRINCIPIOS DEL TRATAMIENTO DE DATOS

Principios Generales del Derecho son los conceptos básicos en que se funda y orienta el sistema jurídico, cuyo contenido influye en la elaboración del derecho positivo, los principios de una ley serán, por tanto, los conceptos básicos en los que se funda y orienta dicha ley.

Así, la ley se funda en unos conceptos básicos que son los principios de los que emanan una serie de derechos para los unos, algunos de los cuales comportan a su vez una serie de obligaciones y para poder ser ejercidos dichos derechos es preciso disponer de los procedimientos correspondientes.

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal se basa en unos principios que figuran en los artículos 4 al 12, ambos inclusive, de la Ley, de los que emanan una serie de derechos, artículos 13 a 1,4 1,), que se pueden ejercer siguiendo los procedimientos que se desarrollan en el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinadas aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los datos de carácter personal.

Los principios de la protección de datos son los siguientes:

2.1 PRINCIPIO DE INFORMACIÓN

El Derecho de información en la recogida de datos está regulado en el artículo 5. En primer lugar, detalla el contenido de la información que se ha de facilitar:

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

- De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de estos y de los destinatarios de la información.

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

Dichas advertencias deberán figurar de forma claramente legible en los cuestionarios u otros impresos cuando este sea el sistema de recogida de la información.

No será necesario informar del carácter obligatorio o facultativo de las respuestas, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos o de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición si el contenido de ello se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

Si los datos de carácter personal no hubiesen sido recabados del interesado, se deberá informar al mismo por el responsable del fichero en el plazo de tres meses siguientes al momento del registro de los datos de forma expresa, precisa inequívoca, a menos que ya hubiera sido informado con anterioridad de:

- Contenido del tratamiento.
- Procedencia de los datos.
- Existencia de un fichero o tratamiento de datos de carácter personal.
- Finalidad de la recogida de los datos.
- Destinatarios de la información.

- Posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- Identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Se exceptúa de la obligación de cumplir con lo anterior en los siguientes casos:

- Una ley lo prevea.
- El tratamiento tenga fines históricos, estadísticos o científicos.
- Cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados.
- Cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial.

Analicemos a continuación cómo se recoge la información:

1. **De forma oral:**
   - *Ventanilla o mesa de atención al público.*
     Sera suficiente con que en la sala existan unos carteles en los que se informe claramente a los ciudadanos de las advertencias anteriormente expuestas.
   - *Atención telefónica.*

2. **De forma escrita:**
   - *Cuestionarios o impresos.*
     En los impresos o cuestionarios deberá figurar una leyenda en la que figure la debida información.
   - *Contratos.*
     En el contrato deberán figurar las advertencias correspondientes.
   - *Web.*

Cuando los datos se recaben en una web en Internet en la misma web deberá figurar una leyenda en la que consten las advertencias correspondientes de forma que se pueda demostrar que quien introduce sus datos ha leído la leyenda.

DOCTRINA DE LA AEPD SOBRE EL PROCEDIMIENTO PARA LA EXENCIÓN DEL DEBER DE INFORMAR (ARTÍCULO 5.4 LOPD)

Se recibió en la Agenda Española de Protección de Datos un escrito en que se solicitaba que por el Director de la Agenda Española de Protección de Datos se resuelva sobre la procedencia de aplicar a la entidad solicitante la excepción al deber de información a los afectados, contemplada en el artículo 5.4 de la LOPD, al suponer dicha notificación *"un esfuerzo desproporcionado en consideración al número de interesados"*.

El artículo 5.5 de la Ley dispone que *"no será de aplicación lo dispuesto en el apartado anterior (referido al deber de información a los afectados cuando los datos no sean recabados de los mismos) cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados,*

a criterio de la Agenda 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".

De ello se desprende que la apreciación de la excepción indicada sólo será posible a través de un acto administrativo de la Agenda en que se decida acerca de la procedencia o improcedencia de la excepción alegada en cada caso concreto. Dicho acto implicará la tramitación del correspondiente procedimiento administrativo, con todas las garantías establecidas en la Ley 30/1992, de 26 de noviembre, de Régimen Juridico de las Administraciones Públicas y del Procedimiento Administrativo Común, y que habrá de someterse a las reglas previstas en su Título VI, dada la aplicación supletoria de la misma prevista por el artículo 35.2 de la Ley Orgánica 15/1999.

Se tratará en todo caso de un procedimiento iniciado por la propia solicitud del interesado, de modo que no será necesaria la adopción de un acuerdo de iniciación de oficio.

En la tramitación del procedimiento deberá requerirse al solicitante para que acredite efectivamente la desproporcionalidad del esfuerzo que conllevaría la práctica de la notificación. En particular, la Ley Orgánica 15/1999 establece como criterios que habrán de ser ponderados por la Agencia para valorar si procede o no aplicar la excepción del artículo 5.4 la antigüedad de los datos, el número de afectados y las medidas compensatorias que se adopten por el responsable del tratamiento.

Por ello, sería necesario que en la fase probatoria se cuantificara realmente el coste que conllevaría la notificación a los afectados y que, durante esta misma fase, se solicitará la expresión del modo en que se adoptarán, en su caso, las medidas compensatorias adecuadas.

Por otra parte, es necesario resaltar que de lo dispuesto en el artículo 5.4 se desprende que la facultad de decisión de esta Agencia se limitará a determinar si, dadas las circunstancias del caso (y, en particular, las previstas en la propia norma) la notificación implicaría un esfuerzo desproporcionado.

En consecuencia, a tenor de la norma no se desprende que sea la Agencia Española de Protección de Datos la que haya de resolver sobre las medidas compensatorias que hayan de adoptarse, sino únicamente sobre la suficiencia de las medidas que se hayan propuesto. Por esta razón, no parece que la Resolución pueda aprobar o no la medida propuesta, sino, simplemente, declarar si es posible aplicar la excepción a la vista de tal medida.

Por este motivo en caso de que se considere que la medida no fuera suficiente, esta circunstancia debería quedar claramente expresada en la propuesta de Resolución, en la que, además, podría señalarse (a fin de garantizar la debida celeridad de procedimiento, impuesta por el artículo 75 de la Ley 30/1992) cual sería el criterio de la Agencia para delimitar las medidas compensatorias que, en su caso, pudieran ser suficientes para estimar la solicitud planteada, a fin de que el interesado pudiera, en el trámite de audiencia concedido por el artículo 84 de la Ley

30/1992 aclarar, si lo estima necesario, las medidas compensatorias propuestas o, si procede, proponer nuevas medidas.

Finalmente, la Resolución del procedimiento debería ser dictada por el Director de la Agencia Española de Protección de Datos dado que, pese a que el artículo 12 del Estatuto de la Agencia Española de Protección de Datos no incluye referencia alguna a este procedimiento, si cabría apreciar su competencia en virtud de la función de Dirección y Representación de la Agencia atribuida por el artículo 36.1 de la Ley Orgánica 15/1999, siendo dicha Resolución susceptible de recurso contencioso-administrativo ante la Audiencia Nacional, de conformidad con lo establecido en el apartado 5 la Disposici6n Adicional cuarta de la Ley 29/1998, de 13 de Julio, reguladora de la Jurisdicción Contencioso Administrativo.

2.2. PRINCIPIO DE CONSENTIMIENTO

Consentimiento, según el artículo 3.h) de la LOPD, es: *«toda manifestación de voluntad, libre, inequívoca, especifica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen»*.

El consentimiento será necesario, en principio, salvo las excepciones establecidas, para el simple tratamiento de los datos y para la cesión o comunicación de los mismos.

Especial importancia tiene el consentimiento en el caso de los datos especialmente protegidos.

El consentimiento puede ser expreso, de forma oral o escrita, tácita y presunto.

La LOPD, a través de su articulado, especialmente el artículo 7 referido a los datos especialmente protegidos, explicita la existencia de un consentimiento escrito en unos casos, y de un consentimiento expreso en otros.

En el artículo 6, al hablar del consentimiento en general, así como en el artículo 11, al referirse a la comunicación de datos, se regula el consentimiento sin más, lo que da pie a la existencia de un tercer tipo de consentimiento que puede ser el tácito o el presunto. A continuación analizaremos cada uno de ellos para ver, en definitiva, cuáles van a ser los permitidos siguiendo el criterio de la Agencia Española de Protección de Datos.

No hemos de olvidar, antes de seguir, la importancia que tiene la opción elegida, tanto en el momento de la información al afectado como en el momento del consentimiento a la hora de probar los hechos. Siempre será más fácil la prueba escrita que cualquier otro tipo de prueba.

Consentimiento expreso

Es el que se manifiesta mediante un acto positivo o declarativo de voluntad. Puede ser de forma oral o escrita. En cualquier caso, como hemos dicho anteriormente, para probar que se ha

emitido, más difícil en el primer caso, deberá utilizarse uno de los medios de prueba admitidos por el derecho.

Consentimiento tácito

Es el que se produce cuando pudiendo manifestar un acto de voluntad contrario, éste no se lleva a cabo, es decir, cuando el silencio se presume como un acto de aceptación.

Respecto a la validez de este tipo de consentimiento, con independencia de lo dicho anteriormente, nos remitimos a la doctrina dada por la Agencia Española de Protección de Datos.

Finalmente y respecto de la forma de solicitar el consentimiento se ha señalado que la LOPD solo habla de necesidad de consentimiento expreso y por escrito en el artículo 7 que regula los datos especialmente protegidos, es decir aquellos datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias, o bien aquellos que hagan referencia al origen racial, a la salud y a la vida sexual.

Es por ello que si el legislador hubiera considerado que el consentimiento hubiera de ser siempre expreso no habría distinguido entre diversas clases de supuestos o modalidades para prestarlo. En este sentido se informó que el Tribunal Supremo, en varias sentencias, interpreta que: fuera de los casos en que la Ley exige una declaración expresa, el consentimiento en los negocios jurídicos puede ser prestado en forma tácita.

Por tanto, el consentimiento tácito para la cesión de datos puede ser válido siempre que no se trate de datos especialmente protegidos.

No obstante, correspondería a la entidad que ha solicitado su consentimiento la prueba de que lo ha obtenido en ese caso concreto.

Asimismo, la Agencia Española de Protección de Datos a diversas consultas sobre los caracteres del consentimiento ha contestado lo siguiente:

"... de las características del consentimiento no se infiere su carácter expreso en todo caso, razón por la cual en aquellos supuestos en que el legislador ha pretendido que el consentimiento deba revestir ese carácter lo ha indicado expresamente; así sucede en el caso de tratamiento de datos especialmente protegidos

indicando el artículo 7.2) la necesidad de consentimiento expreso y escrito para el tratamiento de los datos de ideología, religión, creencias y afiliación sindical, y el artículo 7.3) la necesidad de consentimiento expreso aunque no necesariamente escrito para el tratamiento de los datos relacionados con la salud, el origen racial y /a vida sexual."

Por tanto, el consentimiento podía ser tácito en el tratamiento de datos que no sean especialmente protegidos (artículo 7.2 y 7.3 de la Ley Orgánica 15/1999), si bien para que ese consentimiento tácito pueda ser considerado inequívoco será preciso otorgar al afectado un plazo prudencial para que pueda claramente tener conocimiento de que su omisión de oponerse al tratamiento implica un consentimiento al mismo.

Consentimiento presunto

Es el que no se deduce ni de una declaración ni de un acto de silencio positivo, sino de un comportamiento o conducta que implica aceptación de un determinado compromiso u obligación.

La Agencia Española de Protección de Datos no considera válido el consentimiento presunto y así lo manifiesta en la contestación que da sobre los caracteres del consentimiento al definir como habrá de ser éste:

- **Libre**, lo que supone que el mismo deberá haber sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por el Código Civil.
- **Específico**, es decir, referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento, tal y como impone el artículo 4.2 de la Ley Orgánica 15/1999.
- **Informado**, es decir, que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que el mismo se produce. Precisamente para ello el artículo 5.1 de la Ley Orgánica impone el deber de informar a los interesados de una serie de extremos que en el mismo se contienen.
- **Inequívoco**, lo que implica que no resulta admisible deducir el consentimiento de los meros actos realizados por el afectado (consentimiento presunto), siendo preciso que exista expresamente una acción u omisión que implique la existencia de consentimiento.

Excepciones al consentimiento

Según el artículo 6 de la LOPD, no será necesario el consentimiento inequívoco del afectado en los siguientes casos:

- Una ley disponga otra cosa.
- Se recoja 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 de negocios, 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 LOPD.

- 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.

Las excepciones al consentimiento en el caso de cesiones o comunicaciones de datos las veremos más adelante.

Una ocasión idónea para solicitar el consentimiento, cuando éste es necesario, será el momento en el que se recaban los datos que es también cuando se debe informar al interesado por lo que nos remitimos a la dicho en el caso del principio de información. Recordando siempre los problemas de prueba cuando no se trata de un consentimiento expreso y por escrito.

ASPECTOS A RECORDAR

- Consentimientos expresos, tácitos y presuntos.
- ¿Es válido el presunto?
- La no necesidad de consentimiento no es lo mismo que el tácito.
- Excepciones recogidas en la LOPD.
- Derechos del interesado.

2.3. PRINCIPIO DE CALIDAD

En el artículo 4 de la LOPD se exponen una serie de subprincipios que integran el principio de calidad. Son estos:

- Pertinencia
- Finalidad
- Exactitud
- Cancelación
- Lealtad

2.3.1. Principio de pertinencia (Artículo 4.1)

«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.».

No se pueden recoger todos los datos que queramos como se hacía en los primeros tiempos de la informática allá por los años sesenta en que se recopilaban los datos, no porque se necesitase en aquellos momentos sino por si se podían necesitar en el futuro dadas las carencias tecnológicas que había.

En el artículo figuran tres exigencias: que sean adecuados, pertinentes y no excesivos.

- **Adecuado** se define como: *«que se ajusta a las necesidades o características de alguien o algo»*.
- **Pertinente** es *«adecuado u oportuno»*.
- Por último, **no excesivo** significa *«que no excede del límite de lo normal, razonable o proporcionado»*.

Vemos, pues, que según los significados de las exigencias, estas vienen a ser redundantes.

Han de ser ajustados a las necesidades o características de las finalidades, adecuados y no exceder del límite de lo normal, razonable y proporcionado.

Las finalidades con las que se relacionan estas exigencias a su vez han de ser determinadas, explícitas y legítimas.

Explícita, que es clara o precisa y **legítima**, que es conforme a la ley o basada en ella.

Por lo tanto, las finalidades tienen que ser precisas, claras y conformes a la ley.

2.3.2. Principio de finalidad (Artículo 4.2)

«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 estos con fines históricos, estadísticos o científicos.».

La derogada LORTAD decía que los datos no podrían usarse para finalidades distintas, en tanto que la LOPD habla de finalidades incompatibles.

Ha existido cierta polémica sobre si actualmente se ha hecho más o menos restrictiva la condición.

Distinto, según el diccionario que estamos consultando, significa *«no igual»*, mientras que **incompatible** es que *«no puede estar o coexistir sin impedimento»*.

Seguimos entendiendo, como ya dijimos en su momento, que el cambio de la palabra distinta por incompatible abre un amplio abanico de posibilidades de uso.

Con la nueva redacción, muchas compañías que poseen grandes bases de datos de clientes podrán utilizar éstas para otros fines distintos de aquellos para los que los datos fueron recogidos aunque, por supuesto, no deben ser incompatibles con éstos.

2.3.3. Principio de exactitud

Según el artículo 4.3: *«Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.»*.

En este artículo se ha producido un cambio que, en un principio, puede parecer intrascendente y que, sin embargo, ha levantado gran polémica y tiene gran ascendencia.

La modificación ha consistido en cambiar la palabra real por actual. **Real** significa que *«tiene existencia verdadera»*, mientras **actual** significa *«de ahora, de este momento o del momento a que se hace referencia»*.

Este cambio ha influido en la consideración de la Agencia Española de Protección de Datos a la hora de contemplar el saldo cero en los ficheros de cumplimiento e incumplimiento de obligaciones dinerarias.

Antes permitía que pudiese existir un registro con un deudor y saldo cero resultado del pago de la deuda existente anteriormente y a partir de la entrada en vigor de la LOPD estima que esto no es posible debiendo el responsable del fichero cancelar el dato.

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

2.3.4. Principio de cancelación

Los puntos 5 y 6 del artículo 4 están referidos a la cancelación de los datos:

« Art. 4.5. 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 periodo 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 integro determinados datos.

« Art.4. 6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.»

Más adelante, al referimos a los derechos de las personas, ampliaremos este punto.

2.3.5. Principio de lealtad

En el artículo 4.7 se prohibe la recogida de datos por medios fraudulentos, desleales o ilícitos.

ASPECTOS A RECORDAR

- Las finalidades tienen que ser precisas, claras y conformes a la Ley.
- Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.
- Sean exactos los datos de carácter personal.
- Se cancelarán cuando hayan dejado de ser relevantes.
- Se almacenarán de forma que guarden el derecho de acceso.
- Se prohibe la recogida de datos por medios fraudulentos, desleales o ilícitos.

3. OBTENCIÓN, RECOGIDA Y MODIFICACIÓN DE DATOS

3.1. CLAVES

3.1.1. Principio de calidad de los datos

El principio de calidad de los datos está enunciado en el artículo 4 de la LOPD, según el cual *"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"*.

En virtud de este principio, el responsable del fichero no está autorizado a tratar datos personales que no sean necesarios para cumplir las finalidades del fichero, ni siquiera contando con el consentimiento del interesado. Existen numerosos casos en la práctica en los que el responsable del fichero incumple el principio de calidad de los datos exigidos por la Ley, y de ellos ha quedado constancia en las Memorias de la Agenda. No obstante, un caso recurrente, y al que la Agencia Española de Protección de datos da importancia por la indefensión a la que se ha sometido al interesado, es el de las recabaciones de datos que se llevan a cabo por los departamentos de recursos humanos de algunas empresas.

Si una compañia solicita de sus trabajadores la cumplimentación de un formulario en el que se solicitan distintos datos personales, entre los cuales figura el nivel de estudios, titulaciones, aficiones, etc., ¿se cumple en este caso el principio de calidad de los datos?. ¿Son los datos solicitados a los empleados adecuados, pertinentes y no excesivos?

Una empresa podía obtener y tratar todos aquellos datos de sus empleados que sean necesarios para el mantenimiento de la relación laboral. En este sentido, tal y come viene señalando la Agencia Española de Protección de Datos, una empresa podía conocer el nivel de estudios de sus trabajadores, dado que dicho dato, en principio, no cabe considerarlo come excesivo, pues permite al departamento de recursos humanos valorar el nivel de conocimientos y preparación de sus empleados de cara a posibles promociones internas.

No así los datos referentes a sus aficiones, pues tales datos no parecen adecuados para el normal desenvolvimiento de la relación laboral.

3.1.2. Derecho de información por parte del interesado

No obstante, las limitaciones que el principio de calidad de los datos impone al responsable del fichero a la hora de su recabación, el legislador garantiza la adecuación del tratamiento a los principios legales a través de las obligaciones de información que se imponen a aquel. En efecto, en el momento de la obtención de los datos del interesado, será requisito para la validez del consentimiento que éste preste el tratamiento de sus datos, que de modo previo e inequívoco se le advierta de los siguientes extremos:

- De la existencia de un fichero automatizado.
- De la finalidad del mismo.
- De los destinatarios de la información.
- Del carácter obligatorio o facultativo de sus respuestas a las preguntas planteadas.
- De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
- De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- De la identidad y dirección del responsable del fichero.

En el supuesto de que en la recogida se utilicen cuestionarios u otros impresos, esta información debe figurar de forma claramente legible. En esos casos no bastará la comunicación verbal de las citadas advertencias.

El interesado deberá dar su consentimiento inequívoco, salvo que la propia Ley establezca otra cosa o concurra alguno de los supuestos previstos por la propia Ley en virtud de los cuales no se requerirá el consentimiento del interesado para el tratamiento de sus datos (art. 6.1) y que ya estudiamos:

- Cuando los datos se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias.
- Cuando los datos se refieran a los planes de un contrato o precontrato de una relación de negocios, 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 y resulte necesario para la prevención o diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, cuando

los tratamientos se realicen por personal sanitario sujeto a una obligación de secreto profesional.

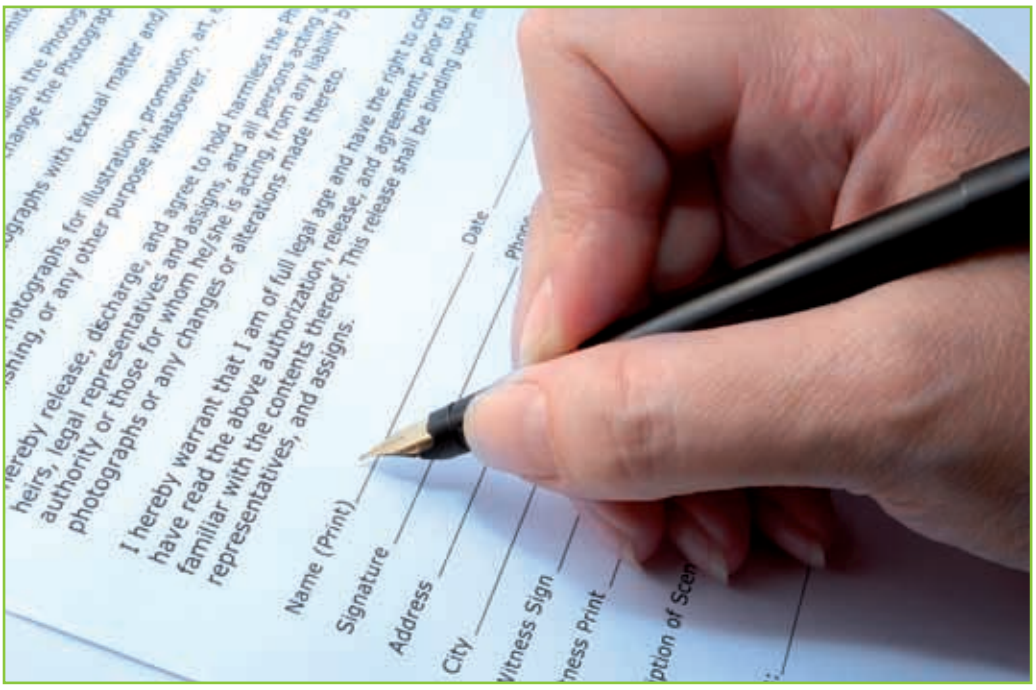
- Cuando los datos figuren en fuentes accesibles al público y el tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos.

El consentimiento se podrá otorgar en cualquiera de las formas admisibles en derecho. De este modo, puede ser: tácito o expreso; Además, el consentimiento prestado por el interesado podría ser revocado por éste cuando exista causa justificada, si bien no se le atribuyen efectos retroactivos a su revocación.

3.1.3. Tratamiento adecuado a la finalidad del fichero

Por último, la LOPD propone el uso de los datos para otra finalidad que no sea aquella para lo que fueron recabados. *"Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubiesen sido recogidos. No se considerará incompatible el tratamiento posterior de esos datos con fines históricos, estadísticos o científicos"*.

Por tanto, no se procederá a recabar datos de carácter personal cuyo conocimiento por parte del responsable del fichero no esté justificado en función de la finalidad de la cual el usuario no haya sido previamente informado. Para que los datos sean utilizados con una finalidad distinta a la puesta en conocimiento del interesado en el momento de su recabación, deberá obtenerse de nuevo su consentimiento.



ASPECTOS A RECORDAR

La salvaguardia conjunta del principio de calidad, principio de finalidad y el derecho de información, rigen las obligaciones y excepciones de las obtenciones de datos.

3.2. TITULARIDAD DE LOS FICHEROS

3.2.1. Privada

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 establecidas para la protección de las personas por la Ley Orgánica 15/1999.

Notificación e inscripción registral

- Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia Española de Protección de Datos.
- Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.
- Deberán comunicarse a la Agencia Española de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.
- El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles. En caso contrario podría pedir que se completen los datos que falten o se proceda a su subsanación.
- Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia Española de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos.

3.2.2. Pública

Creación, modificación o supresión

La creación, modificación o supresión de los ficheros de las Administraciones Públicas sólo podrán hacerse por medio de disposición general publicada en el "BOE" o Diario Oficial correspondiente.

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

- La finalidad del fichero y los usos previstos para el mismo.
- Las personas o colectivos sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos.
- El procedimiento de recogida de los datos de carácter personal.
- La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
- Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.
- Los órganos de las Administraciones responsables del fichero.
- Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

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

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.

3.2.3. Caso especial: Ficheros de las Fuerzas y Cuerpos de Seguridad

- 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 Ley Orgánica 15/1999.
- 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.

- 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 de la Ley Orgánica 15/1999, 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.
- Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento. A estos efectos, se considerara 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.

4. COMUNICACIONES Y CESIONES DE DATOS PERSONALES

Cesión o comunicación de datos según el artículo 3.i) es *«toda revelación de datos realizada a una persona distinta del interesado»*.

En la LORTAD se utilizaba el término cesión y en la LOPD se emplea el término comunicación excepto en el artículo 27, *«Comunicación de la cesión de datos»*.

Dada la definición que se da en el articulo 3.i), parece que coincide más con el término comunicación que con el de cesión.

La comunicación de datos se contempla en los artículos 11 y 21, este último dedicado específicamente a la comunicación de datos entre las Administraciones Públicas.

La comunicación de datos, como hemos dicho anteriormente, es uno de los principios básicos de la protección de datos.

Según éste, los datos de carácter personal objeto de tratamiento, para ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, precisan del consentimiento del interesado.

En el artículo figuran una serie de excepciones al mismo:

- Cuando la comunicación está exceptuada en una Ley.
- Cuando se trate de datos recogidos de fuentes accesibles al público.
- Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
- Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal, los Jueces, 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.
- Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
- 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.

Si la información que se le facilita al interesado respecto a la comunicación de sus datos a un tercero no le permite conocer la finalidad a que se destinarán sus datos o el tipo de actividad de aquel a quien se pretenden comunicar, el consentimiento que autorice dicha comunicación será nulo.

En cualquier caso, el consentimiento de la comunicación de datos es revocable.

El cesionario, por el sólo hecho de recibir los datos, se obliga a la observancia de las disposiciones de la LOPD.

Si antes de la comunicación se disocian los datos, no será aplicable nada de lo expuesto anteriormente, pues los datos pierden su característica de datos de carácter personal.

El artículo 21 referido a la comunicación de datos entre las Administraciones Públicas también fue objeto del Recurso de Inconstitucionalidad 1.463/2000, promovido por el Defensor del Pueblo ante el TO y que este considera en su Sentencia 292/2000, de 30 de noviembre, eliminando el párrafo del punto 1 del artículo: *«cuando la comunicación hubiera sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso»*, lo que ha obligado a muchos organismos a tener que modificar la notificación de ficheros efectuada a la Agencia Española de Protección de Datos con anterioridad.

ASPECTOS A RECORDAR

- Sometimiento a la finalidad de los datos y a las funciones del cesionario y cedente.
- Consentimientos informados y consentimientos viciados.
- Excepciones al consentimiento.
- Revocación del consentimiento.

5. TRATAMIENTO POR CUENTA DE UN TERCERO

5.1. CONCEPTO

La figura del tratamiento por cuenta de tercero es distinta a la de la comunicación (aunque pueda en ocasiones llegar a confundirse), y está regulada por el artículo 12 de la LOPD. Se trata de un acceso a los datos que se realiza por un tercero, denominado encargado de tratamiento, cuando dicho acceso es necesario para la prestación de un servicio al responsable del fichero. Únicamente se considera encargado del tratamiento a la persona, ya sea física o jurídica, que trata datos por cuenta del responsable del fichero.

5.2. REQUISITOS

La realización del tratamiento por cuenta de tercero deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y las disposiciones por las que se rige. El encargado del tratamiento únicamente podrá tratar los datos conforme a las instrucciones del responsable del fichero y deberá comprometerse a no aplicarlos o utilizarlos con fines distintos al que figure en el contrato. Además, no los podrá comunicar, ni siquiera para su conservación, a terceras personas.

De esto último se deduce la prohibición de subcontratación por parte de los encargados de tratamiento de los servicios que le han sido encomendados por el responsable del fichero. En caso de que para un determinado tratamiento sea necesaria la concurrencia de varios encargados (por ejemplo, en los casos de servicios de alojamiento de sitios web en los que proveedores, distintos del principal, ofrecen a éste servicios de respaldo o ponen a su disposición un servidor espejo), el responsable deberá suscribir un acuerdo en los términos previstos en la Ley con cada uno de ellos. Es decir, habrá tantos encargados de tratamiento como servicios se presten al responsable.

5.3. DISTINCIÓN RESPONSABLE Y ENCARGADO DEL TRATAMIENTO

En ocasiones es difícil distinguir la figura del responsable del tratamiento o responsable del fichero de la del encargado del tratamiento. La cuestión radica principalmente en el hecho de si

la organización por cuya cuenta se procede al tratamiento de los datos decide sobre la finalidad y el modo en que se procederá a dicho tratamiento, con independencia de que por la misma se efectúen las operaciones que supongan la incorporación de los datos al fichero.

En concreto, y siguiendo el ejemplo del apartado anterior, en el que una empresa, responsable del fichero con los datos personales de sus empleados, encarga a otra compañía la gestión de sus nóminas, en caso de que la empresa facilite los datos a la gestoría precisamente con la finalidad de que por la misma se desarrollen las debidas actividades de tratamiento de los datos, será aquella quien decida sobre la finalidad y use de la información y tendrá, por tanto, la condición de responsable del fichero. A la hora de dilucidar quién es el responsable, no es tan relevante el tratamiento concreto que se hace de los datos como la persona que decide sobre la finalidad del fichero.

6. TRANSFERENCIAS INTERNACIONALES DE DATOS

6.1. CONCEPTO

Transferencia internacional de datos es toda transmisión de los mismos fuera de territorio español.

La transferencia internacional de datos no es una figura distinta de la comunicación de datos o del tratamiento de datos por cuenta de tercero. De hecho, la gran mayoría de transferencias internacionales de datos se materializan a través de alguna de las figuras citadas.

La prohibición de transferencias internacionales como principio general

El principio general contemplado en el artículo 33 de la LOPD es la prohibición de transferencias temporales o definitivas de datos de carácter personal con destino a países que no proporcionan un nivel de protección equiparable al que presta la LOPD. Cabe, sin embargo, realizar transferencias de datos a países que no ofrezcan tal nivel de protección, siempre que se observen las disposiciones aplicables y se obtenga autorización previa por parte del director de la Agencia Española de Protección de Datos, quien la otorgará si se ofrecen garantías adecuadas en el caso concreto de que se trate.

En cuanto al carácter adecuado del nivel de protección del país de destino, se evaluará por la Agencia Española de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o tipo 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 y el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en dichos países.

6.2. EXCEPCIONES

La norma contemplada en el artículo 33 de la LOPD tiene una serie de excepciones, reguladas en el artículo 34. Esta disposición exceptúa la aplicación de la prohibición prevista en el artículo 33 en los siguientes supuestos:

- Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.
- Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.
- Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico o la gestión de servicios sanitarios.
- Cuando se refiera a transferencias dinerarias conforme a su legislación específica.
- Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.
- 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.
- Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable de un fichero y un tercero.
- 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.
- Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- Cuando la transferencia se efectúe, a petición de una persona con interés legítimo, desde un registro público y aquella sea acorde con la finalidad del mismo.

- 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.

Hasta mediados del 2003, la Comisión Europea había declarado a Suiza, Hungría, Canadá y Argentina países dotados de un régimen que garantiza un nivel de protección adecuado.

La Comisión también ha declarado un nivel de protección adecuado con respecto a Estados Unidos, aunque este constituye un caso en que el legislador europeo ha demostrado su creatividad. En efecto, Estados Unidos carece de una legislación federal que, al modo de las legislaciones nacionales europeas, tenga por objeto la protección de datos de carácter personal. Dada esta falta de regulación legal, Estados Unidos nunca hubiese podido ser declarada como estado con un nivel de protección adecuado.

Estados Unidos se rige, en numerosos ámbitos, por el principio de autorregulación, en virtud del cual son las propias empresas las que adoptan sus propios códigos de conductas o se acogen a códigos de conductas sectoriales, respecto de los cuales el Estado carece de facultad fiscalizadora o de control alguno. Para suplir esta laguna, se ha creado una figura *sui generis* en el panorama legislativo internacional, los Principios de Puerto Seguro, un sistema que trata de casar la autorregulación americana con los principios legales europeos.

Los Principios de Puerto Seguro aprobados por el Departamento de Comercio de Estados Unidos, se corresponden casi literalmente con los principios que inspiran la Directiva 95/46/CE. Las empresas estadounidenses se podrán acoger voluntariamente a estos principios, obligándose a respetarlos y a colaborar con las autoridades europeas de protección de datos personales, lo que hace posible que esas entidades acrediten un nivel de protección adecuado. Con ello, las transferencias con destino a estas empresas "certificadas" según los Principios de Puerto Seguro, se equiparan a efectos legales con aquellas llevadas a cabo con destino a países respecto de los que se haya declarado un nivel de protección adecuado.

ASPECTOS A RECORDAR

En general, las Transferencias Internacionales de Datos (TIE) están prohibidas.

7. LA CANCELACIÓN DE DATOS

La LOPD establece que los datos de carácter personal deberán ser cancelados a propia iniciativa del responsable del fichero cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la que fueron recabados o registrados.

Los datos, en todo caso, no podrán ser conservados de forma que permitan la identificación al interesado durante un periodo superior al necesario para los fines para los que los mismos se registraron.

Estamos, por tanto, no ante una facultad del responsable del fichero sino ante una obligación. Tan pronto como los datos personales hayan dejado de servir para la finalidad para la que se recabaron y respecto de la cual el interesado prestó su consentimiento, deberá procederse a su cancelación.

La cancelación de los datos debe llevarse a cabo a través de su bloqueo, conservándose únicamente a disposición de las Administraciones Públicas, jueces y tribunales para la atención de posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción que la Ley prevea para éstas.

A su vez, puede ser el propio interesado el que pida su cancelación de datos. ejerciendo para ello uno de sus derechos recogido en la LOPD y que estudiaremos en la siguiente Unidad, si bien, este derecho tiene sus excepciones como podremos observar.

DOCTRINA DE LA AEPD SOBRE EL BLOQUEO DE DATOS

Se planteó el alcance de la excepción o suspensión de la obligación de cancelación de datos que implica el bloqueo de los mismos, así como la conciliación del artículo 16.3 de la LOPD con la normativa reglamentaria de desarrollo dictada al amparo de la LORTAD y que regulaba la cancelación, concluyéndose la subsistencia de éstas en una interpretación coordinada con aquella disposición, y entrándose a analizar el supuesto del bloqueo de datos.

Así, el artículo 16.1 del Real Decreto 1332/1994, de 20 de junio, hace también referencia al bloqueo de datos, disponiendo que *"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"*, con la excepción prevista en su párrafo segundo, según la cual *"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 aquellos figuren"*.

Por otro lado, el apartado 8 de la Norma Tercera de la Instrucción 1/1998, de 19 de enero, de la Agencia Española de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación, dispone que *"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"*, añadiendo el apartado 9 de la misma Norma que *"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".

Las citadas previsiones fueron dictadas al amparo de lo establecido en la Ley Orgánica 5/1992, que no contenía previsión alguna en relación con el bloqueo de los datos de carácter personal, limitándose a reflejar esta obligación de cancelar, sin delimitar en qué consistía, efectivamente, la obligación de cancelación. Así, el artículo 15.2 de la derogada Ley se limitaba a señalar que *"los datos de carácter personal que resulten inexactos o incompletos serán rectificados y cancelados en su caso"*, añadiendo el artículo 15.4 que *"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"*, y el artículo 15.5 que *"los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del fichero y el afectado"*.

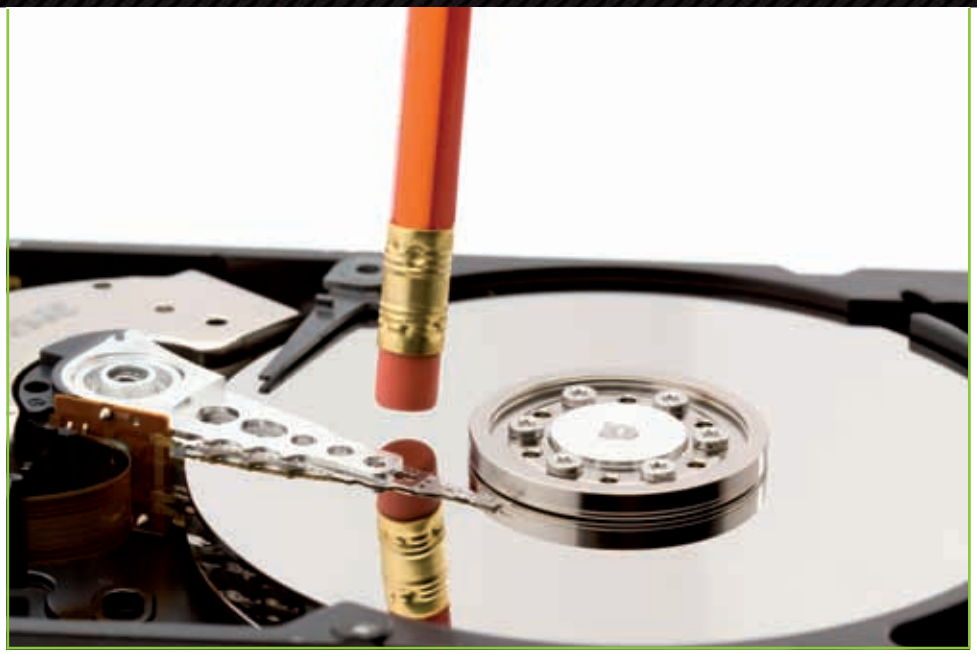
Sin embargo, la nueva Ley Orgánica 15/1999 sí viene a hacer una referencia expresa al bloqueo de los datos de carácter personal en su artículo 16.3, al establecer que *"la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, jueces y tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión"*.

Este precepto, a su vez, se complementa con la previsión contenida en el artículo 16.5 que siguiendo lo ya apuntado por la LORTAD, indica que *"los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado"*.

Del análisis conjunto de las dos normas últimamente citadas se desprende claramente que existirán determinados supuestos en que la cancelación o bien no podrá tener lugar, dada la obligación de conservación impuesta por la Ley, o bien deberá suponer una fase previa de bloqueo de los datos que, produciendo unos efectos similares al borrado físico de los mismos, salvo en determinadas circunstancias, no implicará automáticamente ese borrado.

Asi, el artículo 16.3 viene a reconocer, en consonancia con lo ya previsto en el artículo 15.5 de la LORTAD y 16.5 de la nueva Ley, que existirán determinados supuestos en los que la propia relación jurídica que vincula al afectado con el responsable del fichero y que determina, en definitiva, el tratamiento del dato de carácter personal cuya cancelación se pretende, así como las obligaciones de cada índole que pudieran derivarse de la citada relación jurídica y que aparecen impuestas por la Ley impedirá que la cancelación se materialice de forma inmediata en un borrado físico de los datos.

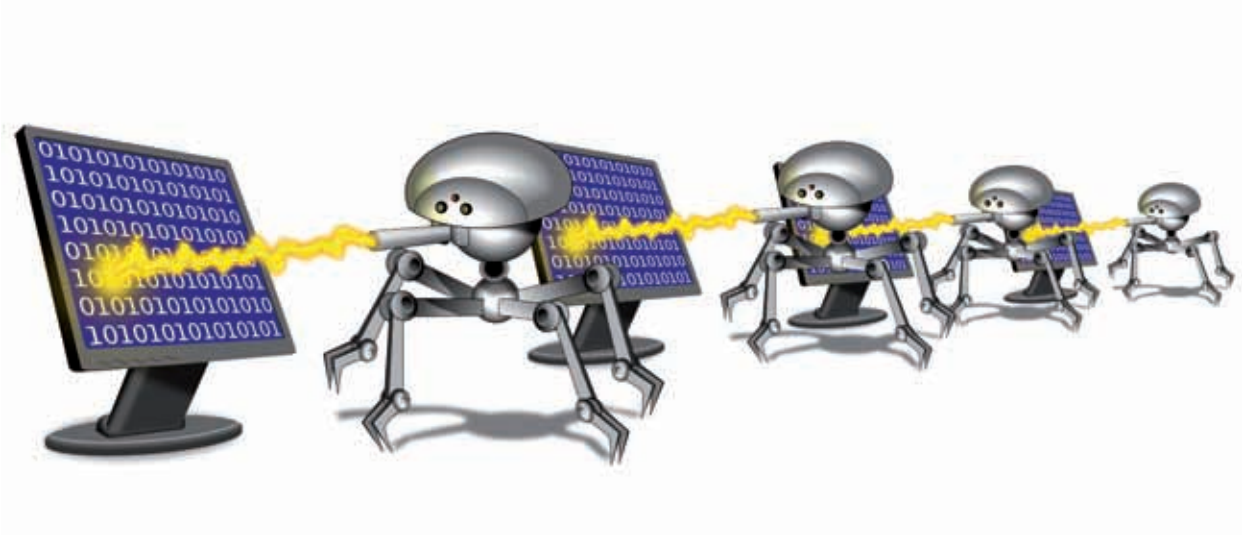
Por el contrario, el responsable del fichero estará obligado, bien por el contenido de aquella relación jurídica, bien por lo establecido en una norma imperativa, al mantenimiento del dato, si bien sometido a determinadas condiciones que aseguren y garanticen el derecho del afectado



a la protección de sus datos de carácter personal, no pudiendo disponer de tales datos en la misma medida en que podría hacerlo en caso de que no procediera (de oficio -por haber dejado de ser necesarios para el cumplimiento de la finalidad del fichero- o a solicitud del afectado) la cancelación de los mismos.

En cuanto a las causas que podrán motivar la conservación del dato, sujeto a su previo bloqueo, y al margen de la relación jurídica con el afectado, a la que se refiere el artículo 16.5 de la Ley Orgánica 15/1999, éstas deberán fundarse en lo dispuesto *"en las disposiciones aplicables"* o a la *"atención de las posibles responsabilidades nacidas del tratamiento"*, tal y como prevé la meritada Ley.

En este sentido, debe recordarse en relación con el mantenimiento del dato bloqueado, en cuanto supone una excepción al borrado físico del mismo que, en definitiva, es el fin último de la cancelación (tal y como prevé el propio artículo 16.3, al indicar que *"cumplido el citado plazo deberá procederse a la supresión"*), que ha de tenerse en cuenta que la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, viene a imponer, expresamente, el principio de reserva de Ley en cuanto a las limitaciones al derecho fundamental de protección de datos de carácter personal, de forma que cualquier limitación a ese derecho (como sería la derivada del artículo 16.3 de la Ley) deberá constar en una disposición con rango de Ley para que el bloqueo de los datos pueda considerarse lícitamente efectuado. Así, a título de ejemplo, podría considerarse que el bloqueo habrá de efectuarse durante los plazos de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento, en los términos previstos por la legislación civil o mercantil que resulte de aplicación, así como el plazo de cuatro años de prescripción de las deudas tributarias, en cuanto los datos puedan revestir trascendencia fiscal (habida cuenta de la obligación de conservación que impone el artículo 111 de la Ley General Tributarias y el plazo legal de prescripción de cuatro años previsto en el artículo 24 de la Ley de Derechos y Garantías de los Contribuyentes).



En consecuencia, cabe entender que la cancelación no supone automáticamente, en todo caso, un borrado o supresión físico de los datos, sino que puede determinar, en caso de que así lo establezca una norma con rango de Ley o se desprenda de la propia relación jurídica, que vincula al responsable del fichero con el afectado (y que motiva el propio tratamiento), el bloqueo de los datos sometidos a tratamiento. Por este motivo, y con las peculiaridades que se han venido indicando, ha de considerarse que lo establecido en el Real Decreto 1332/1994 y en el apartado 8 de la Norma Tercera de la Instrucción 1/1998, debe interpretarse de forma armonizada con la citada disposición, no existiendo una obligación terminante de borrado físico en todos los casos.

Unidad 3

Derechos de los Titulares de los Datos durante el Tratamiento

UNIDAD DIDACTICA 3 // DERECHOS DE LOS TITULARES DE LOS DATOS DURANTE EL TRATAMIENTO

1. DERECHO DE INFORMACIÓN EN LA RECOGIDA DE DATOS

Basado en el Artículo 5 de la LOPD:

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

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

ASPECTOS A RECORDAR

- Tenemos el derecho a que en todo momento, pero principalmente en la obtención, se nos informe de que estamos proporcionando datos para un fichero. No puede haber duda en la forma de esta información.
- Es posible, como vimos, exceptuar parte de este derecho, pero nunca de la existencia del tratamiento.

2. DERECHO DE CONSULTA

El Registro General de Protección de Datos será de consulta pública y gratuita. Cualquier persona tiene derecho a consultar en dicho Registro:

- Existencia de tratamientos de datos de carácter personal.
- Sus finalidades.
- La identidad del responsable del tratamiento.

En el Registro General de Protección de Datos de la AEPD existen dos tipos de ficheros: ficheros de titularidad pública y ficheros de titularidad privada.

Se puede acceder a los mismos a través de Internet en la web de la AEPD.

Los datos que facilita el Registro en el caso de un fichero de titularidad municipal son los siguientes:

- Tipo de Administración.
- Responsable del fichero.
- Nombre del fichero.
- Descripción.
- Dirección de acceso.
- Finalidad.
- Disposición general.
- Fecha.

Ejemplo

Búsqueda de ficheros de Titularidad Pública: RESULTADO DETALLADO.
Tipo de administración: ADMINISTRACION LOCAL.
Responsable del fichero: AYUNTAMIENTO DE MADRID. ÁREA DE MEDIO AMBIENTE.
DEPARTAMENTO DE CONTAMINACIÓN ATMOSFÉRICA.
NEGOCIADO DE TRAMITACION DE SANCIONES.

Nombre del fichero: SANCIONES.
Descripción: TRAMITACIÓN.
Dirección de acceso: C/ BARCELO, 6, 28004 MADRID.
Finalidad: CONTROL DE LAS DENUNCIAS POR EMISIÓN DE HUMOS Y RUIDOS EN VIRTUD DEL CUMPLIMIENTO DE LA ORDENANZA GENERAL DE PROTECCIÓN DEL MEDIO AMBIENTE URBANO, EN LO QUE SE REFIERE A VEHÍCULOS.
Disposición General: BOLETÍN OFICIAL DE LA COMUNIDAD AUTONOMA N.° 1
Fecha: 02-01-1997
Fuente: web AEPD.

ASPECTOS A RECORDAR

- En caso de desearlo podemos consultar la existencia y finalidad de un tratamiento y el responsable. De ahí la importancia de que estén recogidos en la AEPD, que es quien (incluso via web) nos puede dar esa información.
- Los datos en sí no están accesibles en la AEPD. Para eso están otros derechos como el de consulta.

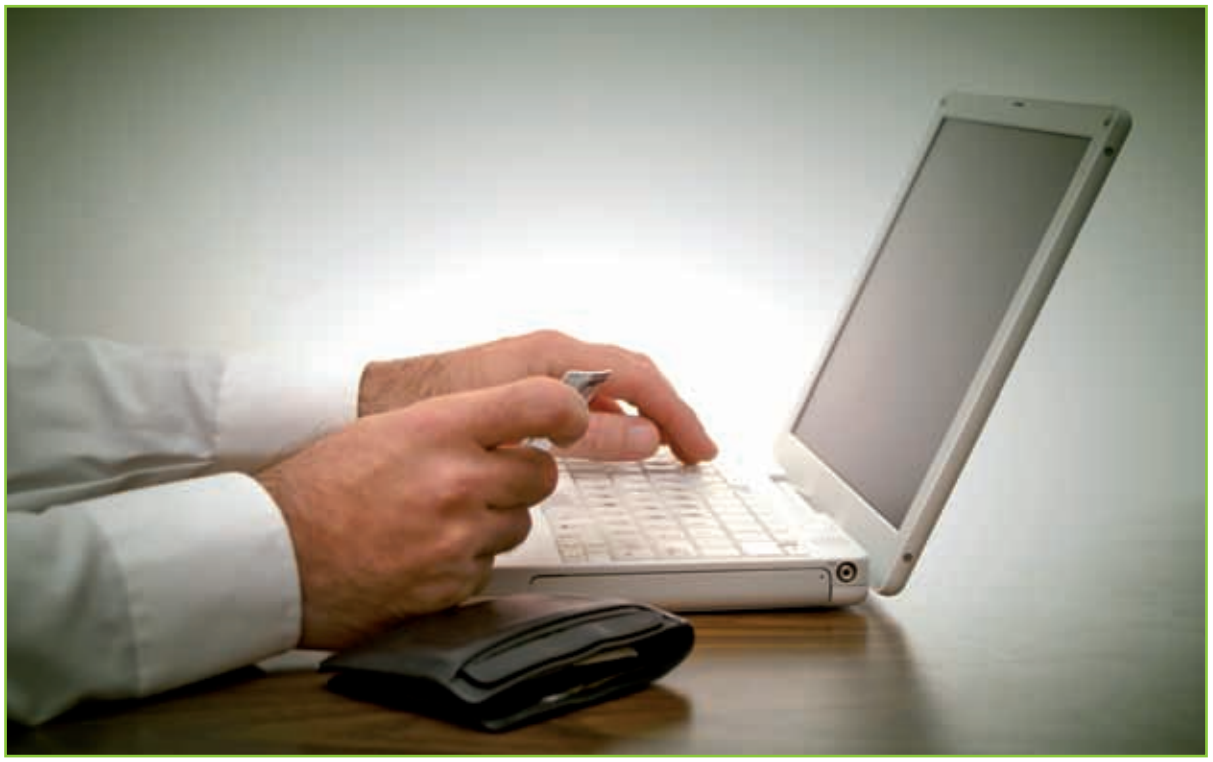
3. DERECHO DE ACCESO

El derecho de acceso viene regulado en el artículo 15 de la LOPD, desarrollado en el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de datos de carácter personal (artículos 11 a 14), subsistente según la disposición transitoria tercera de la LOPD en cuanto no se oponga a la misma y aclarado en la Instrucción 1/1998, de 19 de enero, de la AEPD relativa al ejercicio de los derechos de acceso, rectificación y cancelación.

Este derecho, así como los de rectificación, cancelación y oposición a los que nos referiremos en los puntos siguientes son personalísimos, por lo que el afectado, en el caso de querer ejercer sus derechos, deberá acreditar su identidad.

Cuando el afectado se encuentre en situatión de incapacidad o minoría de edad, podría actuar el representante legal, siempre que acredite su condición.

Para ejercer sus derechos, el afectado deberá realizarlo mediante solicitud al responsable del fichero que deberá contener:



- Nombre y apellidos del interesado.
- Fotocopia de su documento de identidad o de otro documento que acredite su identidad. Cuando exista representante legal, deberá también acompañar fotocopia de su documento nacional de identidad así como del documento acreditativo de tal representación.
- 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 afectado deberá utilizar cualquier medio que permita acreditar el envío y la recepción de la solicitud.

El responsable del fichero deberá contestar dicha solicitud aún en el caso de que no figuren datos personales del afectado en sus ficheros, debiendo utilizar cualquier medio que permita acreditar el envio y la recepción. Si la petición no reuniese los requisitos referidos anteriormente, el responsable del fichero deberá solicitar la subsanación de aquellos.

Según la norma primera, apartado 5 de la Instrucción:

«*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.*».

Esta recomendación es un tanto peligrosa dada la complejidad del tema. Parece muy difícil que todo el personal que accede a estos datos, que en una institución puede ser todo el mundo, tenga los conocimientos necesarios para resolver una incidencia de este tipo.

Creemos que es mejor centralizar en una unidad determinada de la empresa la resolución de todas las incidencias que tengan algo que ver con los datos de carácter personal.

Los requisitos y las actuaciones que hemos examinado hasta ahora afectan tanto al **derecho de acceso** como al de **rectificación** y **cancelación**.

Cuando el afectado ejercite el derecho de acceso, puede optar por alguno de los sistemas de consulta de ficheros que indicamos a continuación, siempre que la configuración del fichero lo permita:

- Visualización en pantalla.
- Escrito, copia o fotocopia remitida por correo.
- Telecopia.
- Cualquier otro procedimiento que ofrezca el responsable del fichero.

Y la información que se facilite debe reunir las siguientes condiciones:

a. Legible e inteligible.
b. Comprensión de todos los datos del afectado que existan en la base.
c. Origen de los datos.
d. Cesionarios de dichos datos.
e. Especificación de concretos usos y finalidades para los que se almacenaron los datos.

Si los datos provienen de diferentes orígenes, deberán especificarse identificando la información que tiene su origen en cada uno de ellos.

El derecho de acceso sólo podrá ser ejercido en intervalos, no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes (art. 15.3 LOPD).

Los responsables de los ficheros de titularidad pública podrán denegar el acceso en los supuestos siguientes:

Articulo 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 a régimen general de la presente Ley.

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 estarán 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.

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 73, 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.

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.

Articulo 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...

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.

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.».

ASPECTOS A RECORDAR

- Derecho personalísimo: por lo que hay que acreditar personalidad o representación legal.
- No se pide a la AEPD, sino al responsable del tratamiento.
- Se accede al dato en si.
- Solicitud con acuse de recibo.
- Plazo de solicitud: no inferior a 12 meses, salvo fuerza mayor.
- Exclusiones como los de las Fuerzas y Cuerpos de Seguridad del Estado.

4. DERECHO DE RECTIFICACIÓN Y CANCELACIÓN

En principio nos remitimos a lo que figura en el punto anterior respecto a los requisitos generales para el ejercicio del derecho.

La Norma Tercera de la Instrucción 1/1998, de 19 de enero, de la AEPD a la que nos estamos refiriendo especifica el procedimiento correspondiente para ejercicio de los derechos de rectificación y cancelación.

Cuando los datos de carácter personal de un afectado o interesado que figuren en un fichero o tratamiento sean inexactos o incompletos, este podría solicitar del responsable del fichero su rectificación o, en su caso, su cancelación.

El plazo para hacer efectivos estos derechos, en un principio, era de cinco días. Lo que se demostró en la práctica que era un plazo muy corto por lo que fue ampliado a **diez días**.

Este plazo se contará **a partir del día siguiente al de la recepción**.

En el caso de que los datos hubiesen sido cedidos, el responsable del fichero dispondría de idéntico plazo para comunicárselo al cesionario que deberá efectuar la rectificación o la cancelación, en su caso, en su fichero.

La solicitud de rectificación deberá incluir lo siguiente:

- Dato que es erróneo.
- Corrección que deba realizarse.
- Documentación justificativa de la rectificación solicitada.

Esta última no será necesaria en el caso de que la rectificación dependa exclusivamente del consentimiento del interesado.

La solicitud de cancelación deberá incluir:

- Si revoca el consentimiento otorgado en los casos en que la revocación proceda.
- Que se trate de un dato erróneo o inexacto en cuyo caso deberá acompañar la documentación justificativa.

«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» (articulo 16.3 LOPD).

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, subsistente en cuanto no se oponga a la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, en virtud de la disposición transitoria tercera de la misma, en su artículo 1 define bloqueo de datos como: *«la identificación y reserva de datos con el fin de impedir su tratamiento»*.

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.

ASPECTOS A RECORDAR

- Existe una solicitud formal de que hay un plazo de 10 días desde la recepción.
- Si están cedidos, el responsable tiene el mismo plazo para cambiarlos ante el encargado del tratamiento.
- Las opciones son rectificar el dato o cancelarlo, salvo los casos excluidos en la Ley.
- En caso de cancelación puede, bien revocarse el consentimiento, bien cancelarlo por erróneo.
- En ese caso hay que demostrar el error.

5. DERECHO DE OPOSICIÓN

En la LORTAD no aparece de forma explícita este derecho; sin embargo, **de forma implícita**, podemos considerar que lo está en el artículo 29.2 cuando reconoce el derecho de los afectados *«a conocer el origen de sus datos de carácter personal así como a ser dados de baja de forma inmediata del fichero automatizado, cancelándose las informaciones que sobre ellos figuren en aquel, con su simple solicitud»*.

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, en su Considerando 25, contempla entre los derechos otorgados a las personas cuyos datos de carácter personal sean objeto de tratamiento, la posibilidad de oponerse a su tratamiento en determinadas circunstancias.

Asimismo, en el Considerando 45 se dice: *«que cuando se pudiera efectuar lícitamente un tratamiento de datos por razones de interés público o del ejercicio de la Autoridad Pública, o en interés legítimo de una persona física, cualquier persona deberá, sin embargo, tener derecho a oponerse a que los datos que le conciernan sean objeto de un tratamiento, en virtud de motivos fundados y legítimos relativos a su situación concreta; los Estados miembros tienen, no obstante, la posibilidad de establecer disposiciones nacionales contrarias»*.

El artículo 14 de la Directiva está dedicado a este derecho.

Artículo 14. Derecho de oposición del interesado

«Los Estados miembros reconocerán al interesado el derecho a:

a. *Oponerse, al menos en los casos contemplados en las letras e) y f) del artículo 75, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos;*
b. *Oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección; o ser informado antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de estos a efectos de prospección, y a que se le ofrezca expresamente el derecho de oponerse, sin gastos, a dicha comunicación o utilización.*

Los Estados miembros adoptarán todas las medidas necesarias para garantizar que los interesados conozcan la existencia del derecho a que se refiere el párrafo primero de la letra b)».

Por otro lado, al igual que la LORTAD, la LOPD no dedica un artículo específico a este derecho pues el artículo 176, *«Procedimiento de oposición, acceso, rectificación o cancelación»,* nos remite a la vía reglamentaria para el desarrollo de estos procedimientos.

Dado que, a pesar del tiempo transcurrido, a la hora de redactar estas líneas no se ha efectuado ningún desarrollo reglamentario y siguen subsistentes los anteriores reglamentos en virtud de la Disposición Transitoria Tercera de la LOPD, no está del todo claro que pueda ejercer el afectado este derecho.

Lo que sí queda claro en el mencionado artículo es que no se exigirá contraprestación alguna por el ejercicio del mismo.

A través de la LOPD vemos que en diferentes artículos se menciona la posibilidad de ejercer este derecho.

Así, en el artículo 6.4, al referirse a los casos en los que no sea necesario consentimiento del interesado para el tratamiento de sus datos de carácter personal, y mientras una ley no disponga lo contrario, éste podrá oponerse a su tratamiento, siempre que existan motivos fundados y legítimos relativos a una concreta situación personal. El responsable del fichero deberá excluir esos datos del tratamiento.

El artículo 18, referido a la tutela de los derechos, en su punto 2 contempla el derecho de oposición entre los derechos que deben ser tutelados por la AEPD.

Por último, en el artículo 30, que contempla los tratamientos con fines de publicidad y de prospección comercial, en su punto 4 recoge el derecho de los interesados a oponerse al tratamiento de sus datos con dichos fines, previa petición y de forma gratuita debiéndose, en ese caso, cancelar las informaciones que sobre ellos se tengan.

Una vez mas contemplamos que, en cierto modo, la LOPD está hecha a parches y que es necesario, por lo menos, su desarrollo reglamentario, que es reclamado urgentemente en algunos casos, como es el del tratamiento de los ficheros no automatizados, especialmente en sus medidas de seguridad.

ASPECTOS A RECORDAR

- Es un derecho difuso.
- Cuando se efectúa, el responsable ha de abstenerse de someter a tratamiento el dato.
- Sólo se puede invocar en algunos casos marcados por la LOPD:
  - No sea necesario el consentimiento y existan razones justificadas.
  - Tutela.
  - Fines publicitarios y comerciales.
- El gasto corre por cuenta del responsable del tratamiento.

6. DERECHO DE TUTELA

La AEPD es el órgano garante previsto en la LORD para que se cumplan y apliquen las previsiones contenidas en ésta.

En el artículo 18 de la LOPD se regula la tutela de los derechos de los afectados por la AEPD y en el artículo 17 del Real Decreto 1332/1994, de 20 de junio, se desarrolla el procedimiento para sustanciar las reclamaciones de los afectados.

Según el artículo 18, las actuaciones contrarias a lo dispuesto en la LOPD pueden ser objeto de reclamación por los interesados ante la AEPD.

El afectado o interesado al que se deniegue total o parcialmente el ejercicio de sus derechos podría ponerlo en conocimiento de la AEPD o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación sufrida por el afectado.

La resolución expresa de tutela de derecho deberá dictarse en un plazo máximo de seis meses.

Contra esta resolución procede recurso de reposición ante la propia Agencia y, en su caso, el correspondiente recurso contencioso-administrativo ante la Audiencia Nacional.

ASPECTOS A RECORDAR

- Garantía de derechos.
- Se ejercen sobre las APD y AEPD.
- 6 meses para la resolución.
- Cabe recurso de reposición ante la AEPD y posterior recurso contencioso administrativo si es necesario.

7. DERECHO A LA INDEMNIZACIÓN

El artículo 19 de la LORD sintetiza en sus tres apartados el derecho a indemnización manteniendo, en esencia, la misma regulación que la antigua LORTAD salvo la inclusión de la figura del encargado del tratamiento junto a la del responsable del fichero y la utilización del término "*interesado*" en lugar de "*afectado*".

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 delito 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.».*

A primera vista, parece que la estructura lógica del artículo respondería al establecimiento de un régimen general en su primer apartado y a regímenes sectoriales **públicos** en el segundo y **privado** en el tercero.

Sin embargo, no hay tal paralelismo, sustantivamente hablando, pues el párrafo 2 remite a la legislación reguladora del régimen jurídico de las Administraciones Públicas en materia de responsabilidad, mientras que el 3 se refiere al ejercicio de la acción concretamente.

El régimen de responsabilidad de las Administraciones Públicas, aplicable a los Ayuntamientos, a tenor del artículo 223 del Real Decreto 2568/1986, de 28 de noviembre, por el que se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales, será el recogido en el Titulo X de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de Administraciones Públicas y del Procedimiento Administrativo Común.

El Principio General de Responsabilidad de las Administraciones Públicas regulado en el artículo 139 de la LRJPAC: *«Los particulares tendrán derecho a ser indemnizados por las Administraciones Públicas correspondientes, de toda lesión que sufran en cualquiera de sus bienes y derechos, salvo en los casos de fuerza mayor, siempre que la lesión sea consecuencia del funcionamiento normal o anormal de los servicios públicos»*.

El artículo 139 es clarificador de cara a la consideración de daño o lesión: *«El delito alegado habrá de ser efectivo, evaluable económicamente e individualizadamente relacionado a una persona o grupo de personas»*.

Por otro lado, y en lo que a los daños provenientes de la Administración Pública se refiere, sólo serán indemnizables las lesiones producidas al particular provenientes de daños que éste no tenga el deber jurídico de soportar de acuerdo con la Ley.

Y, lo que es importante de cara a la materia que nos ocupa: *«no serán indemnizables los daños que se deriven de hechos o circunstancias que no se hubiesen podido prever o evitar, según el estado de los conocimientos de la ciencia o de la técnica existentes en el momento de la producción de aquellos, todo ello sin perjuicio de las prestaciones asistenciales o económicas que las leyes puedan establecer pare estos casos»*. (articulo 141.1 LRJPAC).

El procedimiento se sustanciará de acuerdo con lo regulado en el Real Decreto 429/1993, de 26 de marzo, por el que se aprueba el Reglamento de los Procedimientos de las Administraciones Públicas en materia de responsabilidad patrimonial.

Unidad 4

Medidas de Seguridad en la Empresa

UNIDAD DIDÁCTICA 4 // MEDIDAS DE SEGURIDAD EN LA EMPRESA

1. EXCELENCIA DE UNA POLÍTICA DE SEGURIDAD

La citada LOPD y su Reglamento de medidas de seguridad imponen a los encargados y empleados de una empresa u organización, a la vez que a su directiva, una serie de obligaciones que, de no cumplirse, recibirán sanciones establecidas en estas Leyes.

El cumplimiento de los preceptos de protección y tratamiento impuestos por la Ley implica un cambio en el modo de trabajar día a día de la empresa.

Es por ello que para cumplir la legislación vigente y mejorar la imagen al cliente y el funcionamiento interno, las empresas habrán de implantar sistemas de gestión de la seguridad cuyos principios se marcarán en una política interna de seguridad elaborada por la propia organización.

Algunas empresas limitarán esta política al estricto cumplimiento normativo, pero otras, más sensibles en su negocio a la protección y tratamiento de datos, podrán llegar a implantar sistemas de seguridad (creados *ad hoc* o inspirados en normas ya existentes como la ISO 17799:2000). Sea como fuere la estrategia seguida, resulta evidente la necesidad imperiosa de las empresas de añadir a sus variables de gestión la seguridad de los datos que obtiene y trata, ya que de no hacerlo tendrá consecuencias negativas desde el punto de vista sancionador y desde el punto de vista del marketing, ya que en la **Sociedad de la Información** en la que nos encontramos, la información es cada día un valor más en alza y guardado cada día con más celo por sus propietarios.

ASPECTOS A RECORDAR

- La política de seguridad de la empresa es necesaria para cumplir la legislación vigente y para implantar Sistemas de Gestión de la Seguridad.
- No es necesario implantar un Sistema de Gestión de Seguridad sólo para cumplir la Ley.

2. MARCO REGULADOR DE LA SEGURIDAD EN EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

El marco regulador de la seguridad se enmarca principalmente en 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.

2.1. EL REGLAMENTO DE MEDIDAS DE SEGURIDAD

El objeto de este reglamento es el desarrollo de lo dispuesto en la LORTAD referente a la seguridad de los ficheros automatizados que contienen datos de carácter personal y, hasta que no sea modificado para aplicación y desarrollo de la LOPD, continuará en vigor, siempre que no se oponga a esta última. Se deduce pues, que sólo será de aplicación para aquellos tratamientos de datos automatizados citados de forma común, tanto en la LORTAD como en la LOPD.

Según su artículo primero, establece **medidas de naturaleza técnica y organizativa** necesarias para garantizar la seguridad que deben reunir:

- Los ficheros automatizados.
- Los centros de tratamiento y locales.
- Los equipos, sistemas y programas.
- Las personas que intervengan en el tratamiento automatizado de los datos de carácter personal.

De modo que se pueda asegurar la confidencialidad e integridad de la información, la intimidad personal y el pleno ejercicio de los derechos personales frente a su alteración, pérdida, tratamiento o acceso no autorizado.

2.2. NIVELES DE SEGURIDAD

Dependiendo de la **naturaleza de la información** y del **grado de necesidad** de garantizar su confidencialidad e integridad, las medidas de seguridad se pueden clasificar en **tres niveles**, que son: básico, medio y alto. Estas medidas pueden ser **técnicas** u **organizativas**, pudiendo ser las técnicas de tipo **físico** o **lógico.**

Como veremos a continuación de forma gráfica, todos los ficheros que contengan datos de carácter personal han de cumplir unas medidas de seguridad básicas, estableciéndose otras adicionales para aquellos que, por la naturaleza de sus datos, exigen un grado de protección más alto.

NIVEL BÁSICO:
Todos los ficheros que contengan datos de carácter personal.

NIVEL MEDIO:
Ficheros que contengan datos relativos a:

- Comisión de infracciones administrativas o penales.
- Hacienda pública.
- Servicios financieros.
- Solvencia patrimonial y crédito.

NIVEL ALTO:
Ficheros que contengan datos sobre:

- Ideología.
- Religión.
- Creencias.
- Origen racial.
- Salud.
- Vida sexual.
- Recabados para fines policiales sin consentimiento de las personas afectadas.

Cuando el acceso a los datos de carácter personal se haga a través de una red de comunicaciones, o el tratamiento se haga fuera de los locales de ubicación del fichero, o trabajemos con ficheros temporales, se garantizará el nivel de seguridad correspondiente al tipo de fichero con arreglo a los criterios establecidos anteriormente.

2.3. TIPOS DE MEDIDAS DE SEGURIDAD

En función de cada nivel de seguridad de datos, existen diferentes medidas de seguridad y salvaguarda de los mismos. Así, el Responsable de seguridad deberá saber qué tipo de datos trata y en función de eso establecer cuantas medidas sean necesarias en función de los niveles de los mismos.

Por lo tanto, podemos decir que existen medidas de seguridad de nivel:

- Básico
- Medio
- Alto

Y que son los tipos de datos del punto anterior los que marcan cuando hay que aplicarlas.

2.3.1. Medidas de seguridad de nivel básico

Previsiblemente, toda organización que trate datos de carácter personal va a tener que implantar estas medidas:

Documento de seguridad_

El responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información.

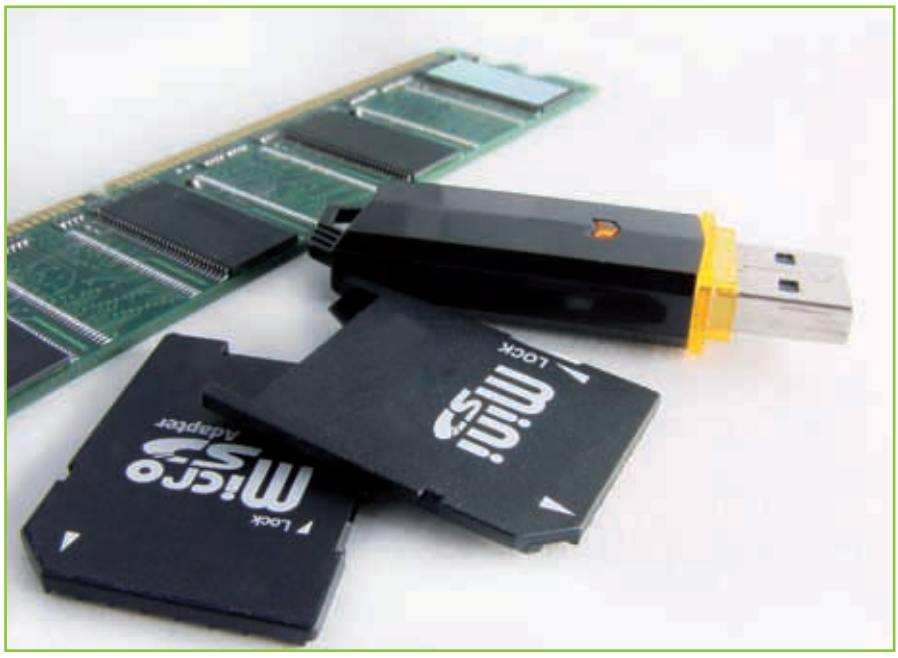
El documento deberá contener, como mínimo, los siguientes aspectos:

- Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.
- Funciones y obligaciones del personal.
- Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
- Procedimiento de notificación, gestión y respuesta ante las incidencias.
- Los procedimientos de realización de copias de respaldo y de recuperación de los datos.

El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

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

No nos adentramos en él debido a que el siguiente punto trata exclusivamente del mismo.



Funciones y obligaciones del personal_

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas.

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

Registro de incidencias_

El procedimiento de notificación y gestión de incidencias contendrá necesariamente un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y los efectos que se hubieran derivado de la misma.

Identificación y autenticación_

El responsable del fichero se encargará de que exista una relación actualizada de usuarios que tengan acceso autorizado al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso.

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.

Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho periodo no se hubiera producido ninguna actualización de los datos.

2.3.2. Medidas de seguridad de nivel medio

Documento de seguridad_

El documento de seguridad deberá contener, además de lo dispuesto en el punto anterior, la identificación del responsable o responsables de seguridad, los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento y las medidas que sean necesarias adoptar cuando un soporte vaya a ser desechado o reutilizado.

Responsable de seguridad_

El responsable del fichero designará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad. En ningún caso esta designación supone una delegación de la responsabilidad, que corresponde al responsable del fichero de acuerdo con este Reglamento.

Auditoria_

Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditora interna o externa, que verifique el cumplimiento del presente Reglamento, de los

procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.

El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al presente Reglamento, 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 recomendaciones propuestas.

Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia de Protección de Datos.

Identificación y autenticación_

El responsable del fichero establecerá un mecanismo que permita la identificación, de forma inequívoca y personalizada, de todo usuario que intente acceder al sistema de información y la verificación de que está autorizado.

Se limitará la posibilidad de intentar, reiteradamente, el acceso no autorizado al sistema de información.

Control de acceso físico_

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal.

Gestión de soportes_

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

Igualmente, se dispondrá de un sistema de registro de salida de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario.

Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

Registro de incidencias_

En el registro regulado en el artículo 10 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.

Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

Pruebas con datos reales_

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 tipo de fichero tratado.

2.3.3. Medidas de seguridad de nivel alto

Distribución de soportes_

La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos, o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

Registro de accesos_

De cada acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permitirá identificar el registro accedido.

Los mecanismos que permiten el registro de los datos detallados en los párrafos anteriores estarán bajo el control directo del responsable de seguridad competente sin que se deba permitir, en ningún caso, la desactivación de los mismos.

El periodo mínimo de conservación de los datos registrados será de dos años.

El responsable de seguridad competente se encargará de **revisar periódicamente** la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes.

Copias de respaldo y recuperación_

Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan cumpliendo, en todo caso, las medidas de seguridad exigidas en este reglamento.

Telecomunicaciones_

La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

ASPECTOS A RECORDAR

- 3 niveles de seguridad.
- Para cada nivel, una serie de medidas obligatorias.
- Algunas medidas son coincidentes, simplemente aumenta su complejidad a medida que son más altos los niveles de seguridad.

3. RESPONSABILIDADES DE LA EMPRESA EN LA GESTIÓN DE SUS DATOS

Una cuestión esencial a la hora de adecuar una organización a la normativa sobre protección de datos de carácter personal es la atribución de responsabilidades y funciones dentro de la organización, pues va a ser principalmente de las **personas**, y no de las medidas implantadas, de quienes va a depender el mantenimiento y el cumplimiento, día a día, de la política de protección de datos implantada.

3.1. RESPONSABLE DE SEGURIDAD

El Responsable de seguridad prevé, entre las medidas de seguridad de nivel medio, la designación de uno o varios responsables de seguridad, seleccionados por el responsable del fichero, que se encargarán de coordinar y controlar las medidas definidas en el documento de seguridad. A pesar de que la figura del responsable de seguridad no es obligatoria en aquellas organizaciones que sean titulares únicamente de ficheros de nivel básico, sí es recomendable que también, en éstas, exista una persona a la que se atribuyan esas funciones.

Sera competencia del responsable de seguridad:

- Supervisar la puesta en marcha de las medidas de seguridad.
- Colaborar con el responsable del fichero en la difusión del documento de seguridad.
- Mantener actualizado el documento de seguridad, realizando las modificaciones oportunas siempre que se produzcan modificaciones que deban ser indicadas en el mismo, así como para adaptarlo a la normativa vigente en cada momento.
- Realizar controles periódicos de verificación del cumplimiento de las medidas de seguridad.
- Controlar la existencia y el cumplimiento de los procedimientos de acceso establecidos.
- Habilitar y gestionar un inventario de soportes y un libro-registro de entradas y salidas de soportes informáticos, que contengan datos de carácter personal fuera del ámbito físico de las dependencias del responsable del fichero.
- Verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y recuperación de los datos.
- Habilitar y gestionar un registro de incidencias.

3.2. EMPLEADOS

Sin duda, la clave de una correcta adecuación a la normativa sobre protección de datos son las personas que, desde la organización, tienen encomendado el tratamiento de los datos personales de los que aquella es responsable. De los empleados y personal interno de la organización depende el **éxito de la implantación de una política de protección de datos**, pues el *«factor humano»* es casi siempre el más débil de cuantos integran una política de seguridad. Por tanto, no sólo se hace imprescindible atribuir **funciones y competencias claras y delimitadas** entre los empleados, sino que también es necesaria una labor de formación y sensibilización de los empleados respecto a la normativa sobre protección de datos adoptada por la organización, atendiendo a las responsabilidades que pueden derivarse para ésta en caso de un tratamiento no adecuado a la Ley.

Las funciones de los trabajadores en relación con los datos personales de los que es titular la organización podrían ser las siguientes:

- Garantizar la confidencialidad e integridad de la información a la que acceden por razón de su puesto de trabajo.
- Cumplir con las obligaciones que para ellos se deriven del documento de seguridad y con los procedimientos que, en su caso, se recogieran en el mismo.
- Garantizar la confidencialidad de las contraseñas.
- Utilizar los soportes que contengan datos de carácter personal con la diligencia debida y atendiendo al procedimiento aprobado al efecto en el documento de seguridad.
- Comunicar al administrador de sistemas o al responsable de seguridad cualquier incidencia de la que tengan conocimiento.
- En general, colaborar en todo aquello que se estime necesario para facilitar el cumplimiento de lo establecido en la legislación vigente en materia de protección de datos.

Además, dadas las responsabilidades que podrían derivarse para el responsable del fichero en caso de incumplimiento, sería conveniente que los empleados recibieran formación sobre los siguientes extremos:

- Aspectos básicos y directrices a tener en cuenta en relación con la política de protección de datos de carácter personal implantada.
- Hechos y actividades que inciden en eventuales modificaciones de las medidas de seguridad de carácter jurídico y técnico implantadas en su sociedad.
- Información sobre normas de actuación en relación con los derechos de terceros derivados de la normativa legal de protección de datos de carácter personal.

ASPECTOS A RECORDAR

- Es clave la actuación de los empleados.
- La formación es fundamental.
- El responsable de seguridad es necesario a partir de medidas de nivel medio.
- Funciones y responsabilidades del responsable de seguridad.

4. EL DOCUMENTO DE SEGURIDAD

4.1. CONCEPTO

El Documento de Seguridad está regulado en el Reglamento de Medidas de Seguridad en el artículo 8 de la LOPD para todos los niveles y en el artículo 15 de dicha Ley Orgánica para los niveles medio y alto (ver apartados anteriores).

Se hacen unas consideraciones de lo que debe contener como mínimo pero no se aclara cómo debe ser -documento escrito o electrónico-, por lo que cualquier opción, en principio, es válida. Tampoco si debe estar referido a una ubicación física o es válido para todas las ubicaciones de ordenadores que tenga la organización. O si tiene que haber un documento por fichero o por tipos de niveles de fichero o uno único para todos.

Como fácilmente se desprende de lo anterior, la elección queda para cada uno, que debe estudiar el **sistema mas favorable para su organización**.

Hemos de tener en cuenta que los documentos de seguridad deben estar actualizados por lo que, cuantos menos existan, mejor. Quizás lo conveniente sería un cuerpo común para todos los ficheros de la organización y después, tantas partes específicas como sean necesarias.

El grado de vinculación entre unas instalaciones y otras de una propia organización será uno de los indicativos de lo que tenemos que hacer.

En el caso de **grupos de empresas** hay que tener en cuenta siempre que cada empresa, aunque pertenezca al grupo, se considera independiente de las demás y que, a estos efectos, deberá tener su propio Documento de seguridad.

Según el artículo 8 del Reglamento, el Documento de seguridad, ya sea de una **institución pública** (patronato, empresa municipal, gerencia, instituto municipal...), como **privada** (empresa mixta, fundación, entidad sin ánimo de lucro, mercantil con mayoría de accionariado municipal), deberá contener, como mínimo, la siguiente información:

- Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.
- Funciones y obligaciones del personal.
- Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
- Procedimiento de notificación, gestión y respuesta ante las incidencias.
- Los procedimientos de realización de copias de respaldo y de recuperación de los datos.

El artículo 15 amplia la obligación de incorporar también la información siguiente cuando son medidas de nivel superior:

- Identificación del responsable de seguridad.
- Controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.
- Medidas que sea preciso adoptar cuando se vaya a desechar o reutilizar un soporte.

Para dar cumplimiento a todo lo anterior es necesario examinar escrupulosamente el articulado del Reglamento para averiguar qué procedimientos se deben incluir, así como qué registros o listados tienen que incorporarse al Documento de seguridad.

4.2. ESTRUCTURA Y CONTENIDOS

1. Introducción
   1.1. Introducción
   1.2. Identificación del responsable del fichero
   1.3. Identificación del responsable de seguridad

1.4. Identificación de los responsables propietarios de los ficheros

2. Ámbito de aplicación
   2.1. Ámbito de aplicación del Documento de seguridad con especificación detallada de los recursos protegidos
   2.2. Inventario de hardware
   2.3. Inventario de software
   2.4. Inventario de ficheros y bases de datos
   2.5. Configuración del sistema informático
   2.6. Organigrama de la organización
   2.7. Prestación de servicios
   2.8. Estructura de los ficheros y bases de datos
   2.9. Descripción del sistema de información

3. Normas de seguridad
   3.1. Políticas
   3.2. Política general de seguridad de la información
   3.3. Política general de protección de los datos de carácter personal
   3.4. Clasificación de la información
   3.5. Política de información al personal
   3.6. Formación del personal en materia de protección de datos de carácter personal

4. Procedimientos
   4.1. Procedimiento de acceso, rectificación, cancelación y oposición a datos de carácter personal
   4.2. Procedimiento de accesos lógicos
   4.3. Procedimiento de acceso a datos a través de redes de comunicaciones
   4.4. Procedimiento del régimen de trabajo fuera de los locales de la ubicación del fichero
   4.5. Procedimiento que deben cumplir los ficheros temporales
   4.6. Procedimiento de gestión de soportes
   4.7. Procedimiento de desecho y reutilización
   4.8. Procedimiento de notificación, gestión y respuesta ante las incidencias
   4.9. Procedimiento de control del cumplimiento
   4.10. Procedimiento de auditoría de la seguridad
   4.11. Procedimiento de control de accesos físicos
   4.12. Procedimiento de copias de respaldo
   4.13. Procedimiento de recuperación
   4.14. Procedimiento de puesta al día del Documento
   4.15. Procedimiento de pruebas con datos reales
   4.16. Procedimiento de registro de accesos
   4.17. Procedimiento de cifrado
   4.18. Procedimiento de almacenamiento de copias de seguridad

5. Relaciones de personal
   5.1. Relación de personal autorizado para acceder a datos de carácter personal

5.2. Relación de personal administrador de accesos
5.3. Relación de personal autorizado para acceder al almacén de soportes
5.4. Relación de personal autorizado a accesos físicos

6. Inventarios y registros
   6.1. Inventario de soportes
   6.2. Registro de entrada y salida de soportes
   6.3. Registro de incidencias

7. Funciones y obligaciones del personal
   7.1. Funciones y obligaciones en general
   7.2. Responsable del fichero
   7.3. Responsable de seguridad
   7.4. Responsables propietarios de los ficheros
   7.5. Director de Sistemas de Información
   7.6. Personal informático
   7.7. Usuarios de la organización

8. Documentación con la AEPD
   8.1. Notificaciones de altas, bajas y modificaciones
   8.2. Oficios de inscripción
   8.3. Otras notificaciones
   8.4. Publicación en Diario Oficial
   8.5. Actuación ante el ejercicio de un derecho por el interesado
   8.6. Actuación ante una inspección de la AEPD

9. Anexos
   9.1. Legislación vigente sobre Protección de Datos de Carácter Personal
   9.2. Glosario de términos de protección de datos

Entenderemos que un contenido de las características de éste cumple con creces lo regulado en el Reglamento y, a la vez, es válido para reforzar la seguridad de los sistemas informáticos de la organización.

4.3. EL CONTROL DEL CUMPLIMIENTO

Como vemos, en el artículo 15, incluido entre las medidas a adoptar en los ficheros de nivel medio y alto, se encuentra determinar los **controles periódicos** que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

De nada serviría disponer de un Documento de seguridad casi perfecto si no controlamos que, efectivamente, lo que se indica en el mismo, por un lado, cumple lo que dispone el Reglamento y, por otro, es lo que se viene realizando en la práctica. Algo que, si no se llevasen a cabo dichos controles, se averiguaría cada dos años al efectuar la auditoria bienal.

Si los controles se establecen correctamente, se convierten en un control interno y podríamos decir que hasta en una **auditoría continua**, con las ventajas que esto conlleva.

El control del cumplimiento se puede establecer semestralmente de forma aleatoria de modo que cada dos años complementa la auditoria bienal.

4.4. LA AUDITORÍA BIENAL

La auditoria bienal que regula el Reglamento en su artículo 17 sólo es **obligatoria** para los **ficheros de nivel medio y alto**, no siéndolo para el nivel básico.

La previsión de realizarla cada dos años que establece el Reglamento debe ser considerada **como un mínimo**. Por lo tanto, no existe ningún inconveniente para acometer la auditoría con una periodicidad inferior.

La auditoría, que es un híbrido entre auditoría informática y auditoría jurídica, podríamos decir que se trata de auditoría jurídica de sistemas de información con base informática, de ahí el problema que existe a la hora de determinar quién está autorizado a realizarla. Viene a ser un complemento de los controles periódicos que ha de realizar el responsable de seguridad para verificar el cumplimiento de lo dispuesto en el Documento de seguridad.

Ahondando en lo dicho en el párrafo anterior respecto **a quién puede realizar** una auditoría de datos de carácter personal, hemos de decir que no hay ningún profesional que monopolice esta función, por lo que, en principio, cualquiera puede realizarla, ya sea la interna, con personal propio y/o externo, o la externa, con personal externo al mismo.

En cuanto a la **independencia**, entendemos que es mas difícil que exista en el caso de una auditoría interna pero, dado los casos que se han producido recientemente con alguna gran auditora (Caso ENRON) relacionados con la auditoría de cuentas, no parece el momento más idóneo para exaltar la independencia de la auditoría externa.

En el informe, que quedará a disposisión de la Agencia de Protección de Datos, pues n**o es necesario enviárselo**, se dictaminará sobre las **medidas** y **controles establecidos**; se identificarán las **deficiencias encontradas** y se propondrán las **medidas correctoras** o complementarias que se consideren precisas. En él se incluirán también los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

Los informes deberán ser analizados por el responsable de seguridad competente, que enviará las conclusiones al responsable del fichero que será quien adopte las medidas correctoras que se precisen.

ASPECTOS A RECORDAR

- No se indica nada en la norma sobre la forma.
- La clave es su actualización.
- Es útil que exista un cuerpo común para todos los ficheros.
- Contenido mínimo del documento:
  - Índice general.
  - Conjunto de procedimientos de seguridad:
    * Auditoría continúa.
    * Auditoría bienal obligatoria.

5. AUDITORÍAS

El objeto de la auditoría es verificar el cumplimiento en los sistemas de información e instalaciones de tratamiento de datos, tanto en la organización del responsable como en la del encargado del tratamiento, de las disposiciones del responsable de seguridad y de los procedimientos vigentes en el mismo.

5.1. OBLIGACIÓN

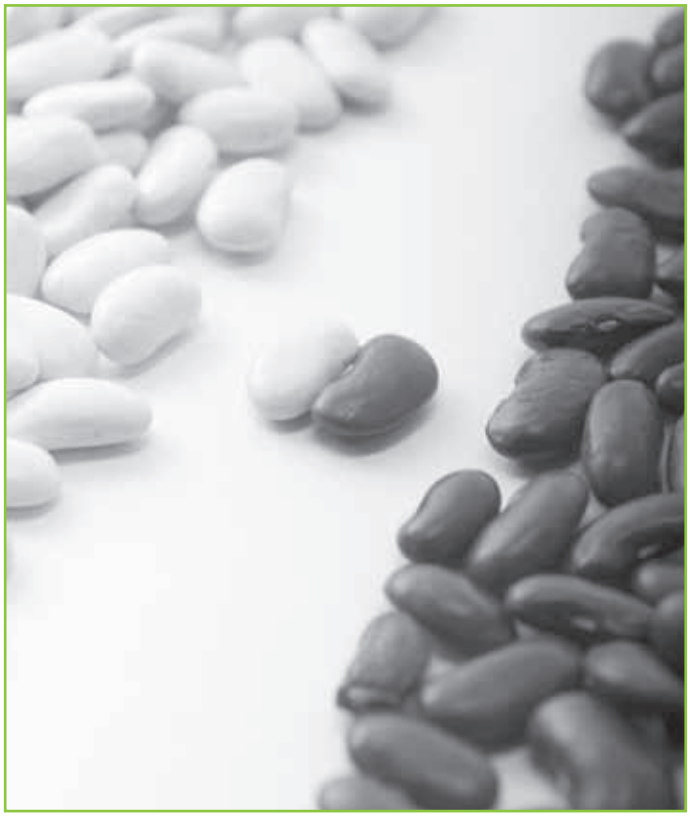
Ya hemos estudiado con anterioridad que existe en el Reglamento de medidas de seguridad la obligatoriedad de realizar, en determinadas circunstancias, una auditoría bienal (al menos) de las medidas de seguridad.

Veamos que esta obligatoriedad tiene dos ámbitos distintos pero conjuntos:

5.1.1. Obligación objetiva

Desde este punto de vista, el Reglamento de Medidas de Seguridad establece qué está sujeto a una auditoría bienal de medidas de seguridad de los sistemas de información e instalaciones de tratamiento de datos que se puedan encuadrar en los niveles medio y alto, como son los datos que clasifica el propio Reglamento y que son relativos a:

- La Comisión de infracciones administrativas o penales.
- Hacienda pública.
- Servicios financieros.
- Prestación de servicios de información sobre solvencia patrimonial y crédito.
- Ideología.
- Religión.



- Creencias.
- Afiliación sindical.
- Origen social.
- Salud.
- Vida sexual.

Datos recabados para fines policiales sin consentimiento de las personas afectadas.

Asimismo, todos aquellos ficheros y/o tratamientos que contengan un conjunto de datos de carácter personal suficiente como para obtener una evaluación de la personalidades del individuo.

5.1.2. Obligación subjetiva

Desde un punto de vista subjetivo, están sujetos a la obligación de realizar la auditoría bienal tanto los **responsables** como los **encargados del tratamiento de datos**, considerándose como responsable del fichero o tratamiento (como ya se vio en la UD. II.) a cualquier persona física o jurídica, de naturaleza privada o pública, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento de datos y, como encargado del tratamiento, a cualquier persona física o jurídica, autoridad servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

La obligatoriedad temporal de dos años funciona como límite de tiempo máximo, sin menoscabo de que una organización decida hacerlas en periodos mas cortos, por sensibilidad de negocio, porque tenga un sistema de seguridad implantado o porque en ese periodo hayan existido cambios significativos que merezcan el control de una auditoría.

5.2. TIPOS

5.2.1. Auditoría interna

Podrá ser realizada por un auditor interno si está **formalmente constituido**, **profesionalmente cualificado** y es **independiente** del órgano responsable del tratamiento y gestión de datos, con la recomendación de que sea personal:

- Competente.
- Independiente de otros departamentos.
- Asegurarse que se cumplen los requisitos de imparcialidad, objetividad e independencia.

5.2.2. Auditoría externa

Podrá ser realizada por un auditor externo profesionalmente cualificado e independiente del responsable o encargado del tratamiento (no vale un consultor que haya participado en alguna fase de la implantación del sistema), y que igualmente actúe con los criterios de:

- Independencia.
- Imparcialidad.
- Objetividad.

5.3. FASES

Seguidamente se enumeran de forma somera las fases de una auditoría de medidas de seguridad:

1. Suscripción entre el auditor y el responsable del tratamiento de un contrato de acceso a datos para la prestación de servicios.
2. Identificación de interlocutores: creación de una comisión y nombramiento de responsables por ambas partes.
3. Recogida de información:
   - Entrevistas y reuniones.
   - Teléfono.
   - Fax.
   - E-mail.
   - Internet.
   - Intranet.
   - Archivos.
   - Apreciación directa.
   - Fuentes: registros públicos, interlocutores de la entidad auditada, terceros, etc.
4. Elaboración, por parte del auditor, de un inventario exhaustivo de la información.
5. Control, por parte de la entidad auditada, de la información que se suministra.
6. Análisis de la información:
   - Cruce de la información obtenida por el auditor.
   - Análisis de conformidad de la información con el responsable de seguridad.
   - Procedimientos e instrucciones vigentes.
7. Aclaraciones con el comité de trabajo y con los distintos interlocutores.
8. Informe provisional.
9. Informe definitivo.

5.4. INFORMES DE AUDITORÍA

Se trata del **producto final** de las auditorías. Son documentos que reflejan las **conclusiones y recomendaciones** del equipo auditor y han de estar a disposición de la AEPD en caso de inspección.

ASPECTOS A RECORDAR

- Obligatoriedad de 2 años, pero se puede hacer antes.
- Para niveles de seguridad medio y alto.
- Interna y externa.
- Se necesita firmar un contrato antes del inicio de la auditoría para salvaguardar la confidencialidad de los datos inspeccionados.
- Resultado: Informe.

Al menos habrá que considerar los siguientes puntos:

- Adecuación de los procedimientos para todos los niveles de seguridad
- Adecuación de los controles para:
  - Nivel básico
  - Nivel medio
  - Nivel alto
- Adecuación de las medidas:
  - Carácter general
  - Nivel básico
  - Nivel medio
  - Nivel alto
- Propuesta de medidas correctoras (sobre las medidas de seguridad, controles, procedimientos u organización). Son fruto del estudio de la empresa y de la experiencia del auditor.
- Propuesta de medidas complementarias.
- Enumeración y descripción de datos, hechos y observaciones.
- Recomendaciones del auditor (no es obligatorio pero sí habitual).

6. INSPECCIONES Y RÉGIMEN SANCIONADOR

6.1. INSPECCIONES DE LA AEPD

La LOPD atribuye a la Agencia Española de Protección de Datos una facultad de inspección sobre los ficheros de carácter personal con objeto de controlar el cumplimiento de la Ley por parte de sus responsables, pudiendo recabar cuantas informaciones precisen para el cumplimiento de sus cometidos. Los inspectores pueden 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.

La Ley atribuye, asimismo, a los inspectores de la Agencia, la condición de autoridad pública y, como es lógico, están obligados a guardar secreto sobre la información a la que acceden en el desempeño de sus funciones.

Existen dos tipos de inspecciones de la Agencia Española de Protección de Datos:

- **Inspecciones sectoriales.** Como vimos en su momento, las inspecciones sectoriales son aquellas que tienen un carácter eminentemente preventivo.
  La Agencia Española de Protección de Datos audita a todo un sector, detecta las carencias que se producen en él en cuanto al tratamiento de datos de carácter personal y emite recomendaciones. Aunque no cabe excluirlas, en la práctica muy difícilmente se imponen sanciones en el marco de las inspecciones sectoriales.
- **Inspecciones de oficio.** Tienen lugar previa denuncia de un tercero ante la Agencia Española de Protección de Datos. En el caso de que la inspección traiga causa de una denuncia presentada por un particular ante la Agencia Española de Protección de Datos en defensa de sus derechos, la Agencia siempre actuará, al menos, con la apertura de un expediente informativo.

6.2. PROCEDIMIENTO SANCIONADOR

Iniciadas las actuaciones previas, ya sea de oficio, ya sea a instancias de un reclamante, si se detectaran por parte de la Agencia indicios de infracción, el Director de la Agencia podría iniciar contra el responsable del fichero un procedimiento administrativo sancionador.

En el marco de este procedimiento, el presunto infractor podría hacer las alegaciones y proponer los medios de prueba que estime oportunas para su defensa.

La duración de los procedimientos sancionadores tramitados por la AEPD tendrá una duración máxima de seis meses.

La resolución que dicte la Agencia Española de Protección de Datos en el marco del procedimiento sancionador agota la vía administrativa, con lo que la empresa sancionada deberá presentar su recurso contencioso administrativo ante la Sala de lo Contencioso Administrativo de la Audiencia Nacional, órgano al que corresponde actualmente la competencia revisora de las resoluciones de la Agencia.

Las resoluciones de la Agencia Española de Protección de Datos se harán públicas tras su notificación a los interesados. Aunque los términos de la publicidad de las resoluciones a la Agencia han de ser aún objeto de desarrollo reglamentario, la misma se realizará preferentemente a través de medios informáticos o telemáticos, a cuyo objeto el sitio web de la Agencia resulta un medio idóneo.

6.3. RÉGIMEN SANCIONADOR

Uno de los aspectos que hacen especial la regulación española de protección de datos de carácter personal es el importe de las sanciones. El importe de las sanciones contempladas en la LORD es **el más alto de los establecidos por las legislaciones de la Unión Europea y posiblemente de todo el mundo**. No es de esperar una revisión a la baja del importe de estas sanciones. La Agencia Española de Protección de Datos ha expresado en numerosas ocasiones que su elevada cuantía cumple un **papel disuasorio** muy importante, papel que pretende impulsar con rapidez la adecuación a la LOPD.

Sin embargo, la LOPD reserva a la Agencia la posibilidad de aplicar la cuantía de la sanción correspondiente a la escala de infracción, inmediatamente menos grave, cuando, en atención de las circunstancias concurrentes, se aprecie una cualificada disminución de la antijuricidad del hecho o de la culpabilidad del imputado.

Por otra parte, las sanciones pecuniarias no son las únicas medidas disuasorias con las que cuenta la Agencia para garantizar el cumplimiento de la legislación. La LOPD atribuye al Director de la Agencia la facultad de adoptar otras medidas, como la **cesación de los tratamientos** y **cancelación de los ficheros**.

6.4. INFRACCIONES

Las infracciones tipificadas en la Ley y su Reglamento pueden ser: **muy graves, graves y leves**. Cada una de ellas tiene distintas sanciones y prescripciones.

6.4.1. Infracciones leves

- No atender, por motivos formales, la solicitud del interesado rectificación o cancelación de los datos personales objeto tratamiento cuando legalmente proceda.
- 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.

- 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.
- Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que se ha comentado.
- Incumplir el deber de secreto establecido con anterioridad, salvo que constituya infracción grave.

6.4.2. Infracciones graves

- Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el BOE o Diario oficial correspondiente.
- 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.
- 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.
- Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la Ley Orgánica 15/1999 o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.
- El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.
- 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 Ley Orgánica 15/1999 ampara.
- 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.
- Mantener los ficheros, locales, pro-gramas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.
- No remitir a la Agencia Española de Protección de Datos las notificaciones previstas en la Ley Orgánica 15/1999 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 aquel a tales efectos.
- La obstrucción al ejercicio de la función del inspector.

- No inscribir el fichero de datos de carácter personal en el Registro General de Protección de Datos cuando haya sido requerido para ello por el Director de la Agencia Española de Protección de Datos.
- Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de la Ley Orgánica 15/1999, cuando los datos hayan sido recabados de persona distinta del afectado.

6.4.3. Infracciones muy graves

- La recogida de datos en forma engañosa y fraudulenta.
- La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.
- Recabar y tratar los datos de carácter personal 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 la ley.
- 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.
- 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.
- 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.
- 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.
- No atender u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.
- No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

6.5. PRESCRIPCIÓN

LEVES	GRAVES	MUY GRAVES
1 año	2 años	3 años

6.6. SANCIONES

LEVES	GRAVES	MUY GRAVES
Multa de 601,01 € a 60.101,21 €	Multa de 60.101,21 € a 300.506,05 €	• Multa de 300.506,05 a 601.012,10 € • Inmovilización de ficheros en el caso de utilización o cesión ilícita de datos que atenten contra los derechos fundamentales

7. SISTEMAS DE GESTIÓN DE LA SEGURIDAD Y LA NORMA ISO/IEC 17799:2000

7.1. ISO/IEC 17799:2000

La norma ISO/IEC 17799:2000 nace como respuesta estandarizada a la cada vez mayor demanda de seguridad en el trato dado a la información en su más amplia acepción, para poder crear un **entorno común** y conocido que proteja a la información de la gran cantidad de amenazas a que se ve expuesta, de manera que se puedan reducir al máximo los datos a la organización y a la vez maximizar la rentabilidad de las inversiones y oportunidades de negocio.

7.2. PROPÓSITOS DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD

7.2.1. Introducción

La gestión de la seguridad de la información requiere que los medios técnicos estén apoyados en una gestión y unos procesos adecuados.

Para poder aplicar cualquier Sistema de Gestión de Seguridad se deberán establecer, en primer lugar, los requisitos de seguridad, obtenidos a partir de **tres fuentes principales**:

- La identificación de los requisitos de seguridad de la información que realice la propia organización, que comprenderá la identificación de amenazas a sus activos, la evaluación de la vulnerabilidad y probabilidad de su ocurrencia y realizar estimaciones de su impacto en los diferentes ámbitos de la organización.
- El compendio de requisitos legales, estatutarios y regulatorios que deberá satisfacer la organización con sus socios comerciales, los contratistas, los proveedores de servicios y los terceros interesados, en general.

- Por último, el marco común constituido por los principios, políticas, objetivos y requisitos que haya adoptado, con carácter interno, la organización, para el tratamiento de la información en el desarrollo de sus operaciones.

Los requisitos de seguridad se identifican mediante una evaluación periódica de los riesgos, manteniendo un equilibrio entre los costes generados por la implantación de controles de seguridad con el impacto económico de posibles fallos en dicha seguridad.

Estas técnicas de diagnóstico se podrán aplicar en la organización en su conducta, como un todo, o bien circunscribirse a partes o, incluso, sistemas individualizados de ella, siempre y cuando esto resulte factible, realista y, sobre todo, útil.

Los **dos factores** fundamentales para la evaluación del riesgo son:

- La determinación del impacto económico que resulte probable por un fallo de seguridad teniendo en cuenta las posibles consecuencias en los parámetros mencionados de confidencialidad, integridad y disponibilidad.
- El estudio probabilístico realista de que estos sucesos ocurran en virtud de las amenazas previstas y los controles implantados.

El resultado de esta evaluación permitirá discernir un escenario ajustado de la realidad en seguridad de la organización y permitirá desarrollar una prelación de riesgos y acciones para su gestión, así como la implantación de controles adecuados para la protección frente a dichos riesgos. El proceso debe ser concebido como un sistema dinámico que permita la revisión periódica del mismo y el establecimiento de evaluaciones sobre aspectos más concretos para enfocar riesgos más específicos.

Los controles deben permitir la reducción de los riesgos a unos umbrales de tolerancia conforme a los requisitos de seguridad identificados.

7.2.2. Análisis de riesgos

El aspecto fundamental y más complejo para la implantación de un Sistema de Gestión de la seguridad es la elaboración de un análisis de riesgos especifico, acorde con los requisitos y el estado de la tecnología, que nos permita identificar las amenazas, priorizar acciones y establecer controles para garantizar un nivel de seguridad adecuado a las necesidades de cada organización.

La determinación de los controles de seguridad apropiados, maximizando la eficacia de sus costes, es a menudo compleja y tratada como hechos subjetivos, de manera que la premisa inicial será **dotar a este proceso de selección de unas bases lo más objetivas posible**.

Existen numerosos sistemas para aproximarse al análisis de riesgos, sin embargo, todos ellos se pueden englobar en dos grandes raíces: el **análisis cuantitativo** y el **cualitativo**.

7.2.3. Análisis Cuantitativo

Requiere únicamente el empleo de las dos premisas fundamentales: la **probabilidad de que cierto suceso ocurra** y los **costes estimados** que conllevará. Este análisis, denominado **expectativa anual de pérdidas** o **coste anual estimado (CAE)**, se obtiene mediante la simple multiplicación de sus elementos fundamentales, de manera que se nos posibilita para realizar una prelación de hechos según el parámetro CAE asociado al riesgo, para adoptar las medidas oportunas sobre esta relación ordenada.

El mayor problema que presentan estos estudios se asocia a la falta de fiabilidad o incorrección de los datos manejados para su elaboración, ya que las posibilidades rara vez son absolutamente precisas, y además, los controles y medidas de corrección pueden ofrecer información diferenciada de varios elementos que, a su vez, pueden tener una relación entre sí, situación que no siempre se contempla.

Pese a estos inconvenientes, el análisis cuantitativo ha sido adoptado con éxito por numerosas organizaciones.

7.2.4. Análisis Cualitativo

Es, con diferencia, el enfoque de análisis de riesgos **más frecuentemente adoptado** por las organizaciones de todo el mundo, basando su metodología en el estudio de **tres elementos** interrelacionados:

- *Amenazas*. Todo aquel proceso lesivo que implique mal funcionamiento del sistema o ataque al mismo, donde se engloban, entre otros, los actos delictivos y los desastres naturales. Debemos tener presente en todo momento que siempre existen amenazas en cualquier sistema.
- *Vulnerabilidades*. El estudio de los puntos más vulnerables del sistema debe ser adecuado pues son los elementos sobre los que una amenaza tiene más capacidad para generar daños al sistema y a la organización. Debemos detectar los eslabones débiles en relación con las amenazas que hayamos establecido.
- *Controles*. Son acciones tomadas para evaluar y evitar la vulnerabilidad del sistema a través de sus puntos débiles. Estos controles podrán obedecer a alguna de las cuatro naturalezas siguientes:

- DISUASORIA: orientados a dificultar los ataques antes de su comisión.
- PREVENTIVA: protegen los puntos débiles impidiendo el éxito del ataque o reduciendo su impacto.
- CORRECTIVA: corrigen el efecto de la vulneración y tratan de neutralizar su causa.
- DE INVESTIGACIÓN: mediante el estudio del entorno del sistema, se trata de descubrir nuevas amenazas para diseñar e implantar acciones preventivas y correctivas.

La norma ISO 17799:2000 pretende ser una guía, no exclusiva ni excluyente, de las prácticas de aplicación de controles de seguridad y, además, al nacer con una **vocación universalista**, contiene controles que podrían resultar inadecuados o, al menos, excesivos e ineficientes según el objeto, alcance, naturaleza o dimensión de los sistemas u organizaciones en donde se pretenda implantar, por lo que abre la posibilidad a excluir parte de ella en la implantación del sistema, siempre y cuando esas salvedades estén claramente identificadas y registradas, justificando de manera suficiente la adopción de estas exclusiones.

7.3. GUÍA DE BUENAS PRÁCTICAS

La norma ISO/IEC 17799:2000 nace como un código de buenos usos para la implantación de un sistema de gestión de la seguridad de la información, es decir, unas recomendaciones o directrices que permiten constituir el marco abstracto del proceso de gestión, dejando la realización específica del mismo a las mejores prácticas de las organizaciones. Este sistema, aunque crea un marco de actuación definido, no llega a concretar una estructura de controles determinada común, lo que imposibilita la comparación por estándares para la certificación. Por ello, debemos mencionar que en este momento se está elaborando en España una norma interna, bajo la denominación de **UNE 71502**, de especificaciones para estos sistemas, que intenta **armonizar la experiencia certificadora** desarrollada en Gran Bretaña sobre gestión de la seguridad de información basada en sus normas BS 779 1 y 2, con el espíritu y objetivos manifestados por la asociación internacional ISO, en la norma ISO/IEC 17799:2000 que estamos exponiendo.

En este punto, y dada la inmediatez de la aprobación de esta segunda norma en España y la apertura del correspondiente proceso certificador, se estudiará la norma y sus eventuales relaciones con nuestro derecho desde una **doble perspectiva**, que incluirá el análisis del código de buenas prácticas, así como una aproximación a las probables especificaciones que se introducirán en la norma de desarrollo que se promulgará y sobre la que se realizará, en su caso, la certificación por entidades acreditadas para ello.

7.4. ESTRUCTURA ISO/ IEC 17799:2000

La norma ISO 17799:2000 se vertebra en **diez contenidos primarios**, que son:

1. Política de seguridad
2. Aspectos organizativos para la seguridad
3. Control de accesos

4. Clasificación y control de activos
5. Seguridad ligada al personal
6. Seguridad física y del entorno
7. Gestión de las comunicaciones y operaciones
8. Desarrollo y mantenimiento de sistemas
9. Gestión de continuidad del negocio
10. Conformidad

ASPECTOS A RECORDAR

La norma ISO 17799:2000 intenta crear una incipiente corriente de sistemas de gestión de la seguridad, en la línea de los sistemas de gestión de la calidad de la ISO 9001.

ANEXO I
Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

ANEXO I // LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

(Cambio denominación por artículo 79 Ley 62/2003, de 30 de noviembre: Las referencias a la Agencia de Protección de Datos deberán entenderse realizadas a la Agencia Española de Protección de Datos).

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.
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 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, solo 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.

a. 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 prohibe 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 tránsito, 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 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

a. tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
b. 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.
c. Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
d. 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 aquél a quien se pretenden comunicar.

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

5. Aquél 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 podrá 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 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 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 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 1
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. 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. (Resultado STC 292/2000, de 30 de noviembre).

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.

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 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

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 impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones Públicas o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales. (Resultado STC 292/2000, de 30 de noviembre).

Capítulo 2
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 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 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 de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos.

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 creedor 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 aquellos.

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 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 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 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 de 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 DE PROTECCIÓN DE DATOS

Artículo 35. Naturaleza y régimen jurídico.

1. La Agencia 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 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 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 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 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 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 aquéllas propuestas que éste le realice en el ejercicio de sus funciones.

3. El Director de la Agencia 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 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

1. Son funciones de la Agencia 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 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 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 82.1 Ley 62/2003, de 30 de diciembre)

Artículo 38. Consejo Consultivo

El Director de la Agencia 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 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 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 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 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 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 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 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. 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.

d. El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.
e. 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.
f. 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.
g. 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.
h. No remitir a la Agencia 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.
i. La obstrucción al ejercicio de la función inspectora.
j. No inscribir el fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos.
k. 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 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 de Protección de Datos.

a. Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando
b. con ello se impida o se atente contra el ejercicio de los derechos fundamentales.
c. 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.
d. No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.
e. 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

1. Las infracciones leves serán sancionadas con multa de 100.000 a 10.000.000 de pesetas.

2. Las infracciones graves serán sancionadas con multa de 10.000.000 a 50.000.000 de pesetas.

3. Las infracciones muy graves serán sancionadas con multa de 50.000.000 a 100.000.000 de pesetas.

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.

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 inmediantamente 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 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 de Protección de Datos u órgano correspondiente de la Comunidad Autónoma agotan la vía administrativa.

3. Los procedimientos sancionadores tramitados por la Agencia 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. (Artículo 82.2 Ley 62/2003, de 30 de diciembre)

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 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 de Protección de Datos podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas.

DISPOSICIONES ADICIONALES

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 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 deberá 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.

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.

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 50 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.

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.

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.

Sexta. Modificación del artículo 24.3 de la Ley de Ordenación y Supervisión de los Seguros Privados.

Se modifica el artículo 24.3, párrafo 2º 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".

DISPOSICIONES TRANSITORIAS

Primera. Tratamientos creados por Convenios Internacionales

La Agencia 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.

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.

Tercera. Subsistencia de normas preexistentes

Hasta tanto se lleven a efecto 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

Queda derogada la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

DISPOSICIONES FINALES

Primera. Habilitación para el desarrollo reglamentario

El Gobierno aprobará, o modificará, las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la presente Ley.

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.

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.

Palacio del Congreso de los Diputados, a 25 de noviembre de 1999.

Federico Trillo-Figueroa Martínez-Conde
PRESIDENTE DEL CONGRESO DE LOS DIPUTADOS

ANEXO II
Reglamento de Medidas de Seguridad

ANEXO II // REAL DECRETO POR EL QUE SE APRUEBA EL REGLAMENTO DE DESARROLLO DE LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

B.O.E. num. 17
19 de enero 2008

PUBLICIDAD DEL REGISTRO

Artículo 53. Publicidad formal

1. El Registro es público.

2. La publicidad se hará efectiva por certificación del contenido de los asientos expedida por el Encargado del Registro, por nota simple informativa o por copia de los asientos y de los documentos depositados en el Registro preferentemente por medios telemáticos. En todo caso, la publicidad formal se ajustará a los requisitos establecidos en la normativa vigente en materia de protección de datos de carácter personal y en la específica sobre acceso a registros administrativos.

3. La información obtenida del Registro no podrá tratarse para fines que resulten incompatibles con el principio de publicidad formal que justificó su obtención. El Encargado del Registro velará por el cumplimiento de las normas vigentes en las solicitudes de publicidad en masa o que afecten a los datos personales reseñados en los asientos.

Artículo 54. Certificaciones

1. Corresponderá exclusivamente al Encargado del Registro la facultad de certificar los asientos del Registro y de los documentos archivados o depositados en el mismo.

2. Las certificaciones constituyen el único medio de acreditar fehacientemente el contenido de los asientos del Registro. En ningún caso podrán expedirse certificaciones sobre datos de fundaciones inscritas en otros registros de fundaciones.

3. Las certificaciones podrán solicitarse por cualquier medio que permita la constancia de la solicitud realizada y la identidad del solicitante.

4. Las certificaciones, debidamente firmadas por el Encargado del Registro, se expedirán en el plazo de cinco días contados desde la fecha en que se presente su solicitud.

Artículo 55. Clases de certificación y de nota

Tanto la certificación como la nota podrán ser literales o en extracto, y referirse a todos los asientos relativos a una fundación o sólo a alguno o algunos de ellos. Podrán expedirse en formato electrónico. Las notas se expedirán en el plazo de tres días desde su solicitud.

PRINCIPIO DE COLABORACIÓN

Artículo 56. Colaboración entre el Registro y los registros autonómicos

1. Las relaciones entre el Registro y los registros de fundaciones de las comunidades autónomas se regirán por el principio de lealtad institucional. En consecuencia, ambos registros deberán:

a. Facilitar a los otros registros de fundaciones cuantos datos, documentos o medios probatorios se hallen a su disposición y se precisen para el ejercicio de sus propias competencias.
b. Prestar la cooperación y asistencia activas que los otros registros pudieran recabar para el eficaz ejercicio de sus competencias.

2. Los intercambios de documentación y datos entre los registros de fundaciones deberán realizarse por medios telemáticos. A estos efectos, la Comisión de Cooperación e Información Registral establecerá las condiciones generales, requisitos y características técnicas de las comunicaciones y de los distintos documentos.

Artículo 57. Flujos de información entre registros en materia de denominaciones

A efectos de dar cumplimiento a lo dispuesto en el capítulo V de este Reglamento, se asegurará el flujo de información entre los registros de las comunidades autónomas y el Registro y entre éste y aquéllos, en relación con denominaciones utilizadas o meramente reservadas por las fundaciones inscritas en dichos registros.

Artículo 58. Colaboración con los Protectorados

1. El Registro comunicará de oficio al Protectorado todas las inscripciones de cada fundación, cuando se trate de actos que requieran la previa intervención de aquél.

2. Siempre que sea conveniente, el Registro podrá solicitar información a los protectorados ministeriales y a los protectorados de las comunidades autónomas.

3. Se establecerán los procedimientos por los que los Protectorados puedan tener acceso a la publicidad del Registro.

Articulo 59. Colaboración con el Consejo Superior de Fundaciones

1. El Registro y los departamentos que ejerzan los protectorados de las fundaciones facilitarán al Consejo Superior de Fundaciones cuanta documentación e información relativa a éstas sea necesaria para el debido ejercicio de sus funciones.

2. El Registro podrá solicitar informe al Consejo Superior de Fundaciones. La consulta versará sobre aquellos aspectos relacionados con las funciones que el Registro tiene normativamente atribuidas.

979 REAL DECRETO 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

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:

1ª. 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:
   - 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.
   - Aquéllos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.
   - 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 delas 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.

a. 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:
   - Aquéllos que contengan datos derivados de actos de violencia de género.
   - 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.

b. 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.

2ª. 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.

3ª. 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

ANEXO II

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 internacionalpúblico.
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

a. 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.
b. 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.
c. 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.
d. 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.
e. 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.
f. 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.
g. 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.
h. 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.
i. Procedimiento de disociación: Todo tratamiento de datos personales que permita la obtención de datos disociados.
j. 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.
k. 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.

l. 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.
m. 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

a. automatizados, no automatizados o parcialmente automatizados.
b. 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.
c. Transmisión de documentos: cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.
d. 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 BOE núm. 17 Sábado 19 enero 2008 4111 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 1
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. 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 libertadesfundamentales 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 2
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 BOE núm. 17 Sábado 19 enero 2008 4113 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 3
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 1
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 2
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:

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

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 3
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 4
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.

a. 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.
b. 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 1
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

a. 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.
b. 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 1
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 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:

- Si la solicitud se dirigiera al titular del fichero común, éste deberá comunicar al afectado todos los datos relativos al mismo que obren en el fichero. En este caso, el titular del fichero común deberá, además de dar cumplimiento a lo establecido en el presente reglamento, facilitar las evaluaciones y apreciaciones que sobre el afectado se hayan comunicado en los últimos seis meses y el nombre y dirección de los cesionarios.
- Si la solicitud se dirigiera a cualquier otra entidad participante en el sistema, deberá comunicar al afectado todos los datos relativos al mismo a los que ella pueda acceder, así como la identidad y dirección del titular del fichero común para que pueda completar el ejercicio de su derecho de acceso.

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:

- 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.
- 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.

- 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 2
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 1
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 2
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 1
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 2
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 3
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 1
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.
c. 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 2
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 3
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.

ANEXO II

Capítulo 4
Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados

SECCIÓN 1ª. 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 1
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 2
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 3
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 4
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.

Capítulo 5
Procedimientos relacionados con las transferencias internacionales de datos

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 6
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 7
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 art. 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.

MINISTERIO DE FOMENTO

980 REAL DECRETO 1762/2007, de 28 de diciembre, por el que se determinan los requisitos relativos a la lista maestra de equipo mínimo y la lista de equipo mínimo, exigidos a las aeronaves civiles dedicadas al transporte aéreo comercial y a los trabajos aéreos.

Las Autoridades Aeronáuticas Conjuntas (JAA), organismo asociado a la Conferencia Europea de Aviación Civil (CEAC), e integrado por las Autoridades nacionales de aviación civil de los Estados europeos firmantes de los Acuerdos sobre la elaboración, aceptación y puesta en práctica de los requisitos conjuntos de aviación (Chipre 1990), acordaron el 1 de junio de 2000

los requisitos conjuntos de aviación (JAR) relativos a la lista maestra de equipo mínimo (Master Minimum Equipment List o MMEL), y la lista de equipo mínimo (Minimum Equipment List o MEL) denominados JAR MMEL/MEL.

Estos requisitos conjuntos de listas maestras y listas de equipos mínimos (JAR-MMEL/MEL) fueron incorporados al ordenamiento jurídico español mediante la Orden FOM/3538/2003, de 9 de diciembre, para su aplicación a los aviones civiles de transporte aéreo comercial, en desarrollo del Real Decreto 220/2001, de 2 de marzo, por el que se determinan los requisitos exigibles para la realización de las operaciones de transporte aéreo comercial por aviones civiles.

La utilización de estas listas de equipo aporta cierta flexibilidad para operar aeronaves que de otro modo quedarían forzosamente inoperantes, en ausencia del personal certificador que pueda analizar en que grado se ve afectada la seguridad del vuelo con dicho defecto.

El Reglamento (CE) n.º 2042/2003 de la Comisión, de 20 de noviembre de 2003, sobre el mantenimiento de la aeronavegabilidad de las aeronaves y productos aeronáuticos, componentes y equipos y sobre la aprobación de las organizaciones y personal que participan en dichas tareas, cuyo ámbito de aplicación abarca a casi todas las aeronaves civiles, salvo algunas excepciones expresamente determinadas en el mismo, prevé la posibilidad de que el piloto al mando de la aeronave o el personal certificador autorizado pueda utilizar la lista de equipo mínimo aprobada y exigida por la autoridad competente, en caso de que surjan defectos en la aeronave.

Por lo expuesto, y tras la reciente aprobación del Real Decreto 279/2007, de 23 de febrero, por el que se determinan los requisitos exigibles para la realización de las operaciones de transporte aéreo comercial por helicópteros, así como, el gran desarrollo alcanzado en el campo de los trabajos aéreos, este real decreto tiene por finalidad de establecer los requisitos exigidos para la utilización de la lista maestra de equipo mínimo y la lista de equipo mínimo, por todas las aeronaves que realizan transporte aéreo comercial o trabajos aéreos, en aplicación de lo dispuesto en el artículo 20.4 de la Ley 48/1960, de 21 de julio, de Navegación Aérea, y al amparo de la habilitación prevista en la disposición final cuarta de la misma Ley.

Asimismo, se establece el procedimiento para la aprobación o, en su caso, aceptación, de las mencionadas listas (lista maestra de equipo mínimo MMEL y lista de equipo mínimo MEL), y se incorpora la enmienda 1 adoptada por las Autoridades Aeronáuticas Conjuntas (JAA) el 1 de agosto de 2005, en relación con los requisitos conjuntos de aviación antes mencionados (JAR-MMEL/MEL).

En su virtud, a propuesta de la Ministra de Fomento, con la previa aprobación del Ministro de Administraciones Públicas, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 28 de diciembre de 2007,

D I S P O N G O :

Artículo 1. Objeto y ámbito de aplicación

Este real decreto tiene por objeto la determinación de los requisitos exigibles para la utilización, aprobación o, en su caso, aceptación de los documentos denominados lista maestra de equipo mínimo (MMEL), y lista de equipo mínimo (MEL), de las aeronaves civiles dedicadas al transporte aéreo comercial y a los trabajos aéreos que operen en España.

Artículo 2. Definiciones

A los efectos de este real decreto se entenderá por:

a. Extensión del intervalo de corrección: consiste en la ampliación de la duración del Intervalo de Corrección sujeto a los condicionantes recogidos en este real decreto.
b. Intervalo de corrección: significa una limitación en la duración de operaciones con equipos inoperantes.
c. Lista maestra de equipo mínimo (MMEL): lista maestra establecida para un tipo de aeronave, que determina los instrumentos, elementos del equipo o funciones que pueden no estar en funcionamiento temporalmente manteniendo el nivel de seguridad pretendido por las correspondientes especificaciones de la certificación de aeronavegabilidad, debido a la redundancia del diseño de la aeronave o a procedimientos, condiciones o limitaciones específicas de carácter operacional o de mantenimiento, y de conformidad con los procedimientos aplicables para el mantenimiento de la aeronavegabilidad.

CEA Confederación de Empresarios de Andalucía

CEAT ANDALUCÍA
FEDERACIÓN ANDALUZA DE AUTÓNOMOS

Servicio Andaluz de Empleo
CONSEJERÍA DE EMPLEO