La PYME ante la LOPD

Eduardo Pinedo González

La PYME ante la LOPD

El primer paso para evitar una fuerte sanción

netbiblo

Para comentarios sobre los títulos de esta serie:

bpocket@netbiblo.com

LA PYME ANTE LA LOPD

netbiblo
www.netbiblo.com

DERECHOS RESERVADOS 2007, respecto a la primera edición en español, por
© Netbiblo, S. L.

NETBIBLO, S. L.
C/. Rafael Alberti, 6 bajo izq.
Sta. Cristina 15172 Oleiros (La Coruña) – Spain
Tlf: +34 981 91 55 00 • Fax: +34 981 91 55 11
editorial@netbiblo.com

ISBN: 978-84-9745-197-0
Depósito Legal: C-3364-2007

Directora Editorial: Cristina Seco López
Editora: María Martínez
Producción Editorial: Gesbiblo, S. L.

Impreso en España – Printed in Spain

A Gloria y María.

A mis padres, abuelos,
hermano, cuñada y suegros.

El autor

Eduardo Pinedo González

Licenciado en Derecho por el Centro Universitario Francisco de Vitoria, posteriormente realizó el Curso Superior en Derecho de las Telecomunicaciones y Nuevas Tecnologías del Instituto de Empresa. Empezó su carrera profesional en el despacho de abogados Gomez-Acebo&Pombo y posteriormente trabajó en el despacho Bufete Linares y Asociados. Actualmente, es abogado en una de las más prestigiosas entidades aseguradoras españolas, asesorando, entre otras materias, en protección de datos de carácter personal.

Contenido

Orígenes de la normativa de protección de datos de carácter personal y ámbito de aplicación de la LOPD

1.1 Orígenes de la normativa de protección de datos de carácter personal y objeto de la LOPD

El **artículo 18 de la Constitución Española**, establece que *"se garantizará el derecho al honor, a la intimidad personal y familiar y a la propia imagen (…)"* especificando el punto cuarto del citado artículo que*: "la Ley garantizará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"*.

En el desarrollo de dicho artículo, así como para el pleno cumplimiento de lo dispuesto por el **Convenio nº 108 del consejo, de 28 de enero de 1981,** de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, el cual fue ratificado por España en 1984, se aprobó la **Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal** (en adelante, LORTAD).

El objeto y fin del Convenio nº 108 era garantizar a cualquier persona física el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de sus datos de carácter personal. Las finalidades, por tanto, giraban en torno a la protección de la intimidad y a la protección de la vida privada.

El principal objetivo de la LORTAD era la protección de la intimidad y el honor frente a su utilización mecanizada, ordenada y discriminada, lo que podría entenderse como "libertad informática" o *habeas data*.

Los anteriores objetivos marcados por la LORTAD se tendrían que ver irremediablemente ampliados, debido al nuevo marco que surgiría tras la aprobación de la **Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.** El objeto de dicha norma pasa a ser la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales. Se mantiene el objeto de proteger la intimidad, pero ya desligada exclusivamente de la utilización de los datos de forma automatizada o mecanizada. Por tanto, dicha norma ya se aplicará tanto a los *tratamientos automatizados,* como a los *tratamientos de datos manuales.*

La citada Directiva se incorporó al derecho interno español a través de la **Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal,** la cual, en adelante, en el presente trabajo será nombrada LOPD. Dicha norma tiene como 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. Ya no se recoge, como hacía la LORTAD, la referencia a la limitación de la informática y otras técnicas, por lo que el objetivo y el ámbito de aplicación de la norma será infinitamente más extenso. Se recoge en el ámbito objetivo de la LOPD una clara referencia al artículo 18 de la CE, en la medida en que aún no se tenía al derecho a la protección de datos como un derecho autónomo e independiente del derecho a la protección de la intimidad personal y familiar y a la propia imagen.

Es a partir de la **sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre** cuando se perfila el derecho a la protección de datos como autónomo respecto al artículo 18 de la Constitución Española y con una esfera mucho mayor que la propia intimidad. Se argumenta en la citada sentencia *"De ahí la singularidad del* ***derecho a la protección de datos****, pues, por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el artículo 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal (STC 170/1987, de 30 de octubre, FJ 4), como el derecho al honor, citado expresamente en el artículo 18.4 CE, e igualmente, en expresión bien amplia del propio artículo 18.4 CE, al pleno ejercicio de los derechos de la persona. El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado.*

De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el artículo 18.1 CE otorga, sino los datos de carácter personal. (...) *el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que 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 saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales (STC 254/1993, FJ 7).”

Por tanto, a partir de esta sentencia, el derecho fundamental a la protección de datos pasa a tener identidad propia y diferente naturaleza jurídica que el derecho a la intimidad personal frente a la utilización de la informática, consagrado por el artículo 18 de la Constitución.

En apoyo de lo anterior, la **Carta de los Derechos Fundamentales de la Unión Europea (7/12/2000),** recoge en su artículo octavo que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. Esos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a su rectificación. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

1.2 Qué es un dato de carácter personal y otros conceptos fundamentales

1.2.1 Dato de carácter personal

A los efectos de la LOPD, un **dato de carácter personal** es **cualquier información concerniente a personas físicas identificadas o identificables.** Por tanto, cualquier dato que haga referencia a una persona física concreta, o a una persona

Continúa

que si bien *a priori* no tenemos identificada, pero que a través de cualquier medio de identificación que no exija un tiempo o una actividad desmesurada pueda llegar a identificarse, será un dato de carácter personal y, por tanto, quien trate dicho dato estará sujeto a los principios protectores de la LOPD.

a. Cualquier información

Se puede notar la amplitud que el legislador ha querido incluir dentro del ámbito de protección de la LOPD. El tratamiento de **cualquier información de una persona física, por ejemplo, asociado a cualquier información que le concierna,** a modo de ejemplo, características físicas de la persona, su nivel de estudios, si forma parte de la plantilla de una empresa, su cargo en la misma, su estado civil, y un interminable etcétera, deberán ajustarse a la LOPD. El concepto incluirá tanto datos objetivos (altura, características físicas, nivel de estudios, etc.) como datos subjetivos (cualquier clase de opinión que pudiera realizar el responsable del tratamiento o un tercero). Esto significa que con independencia de que entendamos que estamos absolutamente legitimados para tratar determinados datos, habrá que tener en cuenta los principios y garantías establecidas en la citada norma. Por ejemplo, una empresa estaría legitimada para tratar los datos de sus empleados o de sus proveedores de servicios. El que esté legitimada para ello, no supone una patente de corso que exima de cumplir con una serie de requisitos que se irán analizando en la presente obra y que se encuentran principalmente recogidos en la LOPD.

Los datos personales que fuéramos a tratar de determinadas personas físicas, **no deben estar necesariamente relacionados con la esfera íntima de éstos,** sino que basta que se trate de cualquier clase de dato, excediendo, por tanto, la protección regulada a través de la LOPD a lo recogido en el artículo 18.4 de la Constitución Española, relativo al derecho a la intimidad.

Por ejemplo, el que tratemos datos por todos conocidos de una persona física, no será supuesto de no aplicación de la LOPD.

Según se desprende de la sentencia del Tribunal Constitucional número *292/2000 "el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo"*.

Igualmente, será indiferente, excepto para la aplicación de las medidas de seguridad, el medio en el que se encuentren almacenados los datos personales, ya sea en papel, la memoria de un ordenador, imágenes, grabaciones de voz, fotografías, etc., quedando garantizado por la LOPD el tratamiento de dichos datos contenidos en dichos medios, garantizando asimismo los mismos niveles de protección.

b. Datos de personas físicas

El segundo matiz que debe destacarse de la definición de dato de carácter personal, es la referencia exclusiva a las **personas físicas,** lo cual supone que el tratamiento de datos de las personas jurídicas quede excluido de la LOPD. El artículo primero de la LOPD, al establecer cuál es el objeto de la LOPD, dispone que es el *"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"*. Queda claro, por tanto, que la voluntad del legislador es mantener al margen de la Ley Orgánica el tratamiento de datos de las **personas jurídicas.** La cuestión que se plantea es qué ocurrirá con el tratamiento de datos de carácter personal de comerciantes y empresarios individuales.

La Audiencia Nacional, en su sentencia de fecha 11-2-2004 **(recurso 132/2002)** estableció que: *"*(…) *Acorde con la doctrina anterior, y teniendo en cuenta que la LO 15/1999 tiene por objeto garantizar y proteger, por lo que ahora interesa, los datos personales, entendiéndose por tales, ex artículo 3.a) de la citada Ley,*

'cualquier información concerniente a personas físicas identificadas o identificables', debe concluirse que en el caso examinado el dato afectado, aunque se refiera al lugar de ejercicio de su profesión, es un dato de una persona física con una actividad profesional, cuya protección cae en la órbita de la Lo 15/1999 de tanta cita, como viene declarando esta Sala reiteradamente, por todas sentencia de 21 de noviembre de 2002. En efecto, los datos personales son predicables de todos los ciudadanos, sin que pueda excluirse de dicha previsión los relativos a aquellos que realizan una actividad profesional, pues el ejercicio de esta actividad no puede ser equiparado a estos efectos a la de una empresa, como parece mantener el recurrente". En la misma línea las SAN (1ª) de 22 de noviembre de 2002 (rec 881/2000) y 25 de junio de 2003 (rec 1099/2000). Sentencias en las que indicamos que no existían motivos para considerar fuera del ámbito de la LO 15/1999 a los profesionales pues ***"no ejercen su actividad bajo forma de empresa, no ostentando en consecuencia la condición de comerciante a que los refieren los artículos primero y siguientes del Código de Comercio".***

Por tanto, en virtud de lo establecido en la citada sentencia, el tratamiento de datos de los profesionales que no ejerzan su actividad bajo la forma de empresa, y que no ostenten la condición de comerciante según se establece en el Código de Comercio, quedarán amparados por la LOPD. A fin de cuentas, se trata de datos de personas físicas.

La Resolución R/00556/2005, de la Agencia Española de Protección de Datos (en adelante, AEPD) (www.agpd.es), estableció que "(…) *de acuerdo con la doctrina legal expuesta, los* ***profesionales*** *y los* ***comerciantes individuales*** *quedarán bajo el ámbito de aplicación de la LOPD y, por tanto, amparados por ella cuando los primeros no tuvieran organizada su actividad profesional bajo la forma de empresa, no ostentando, en consecuencia, la condición de comerciante, y los segundos cuando no fuera posible diferenciar su actividad mercantil de la propia actividad privada*".

Será muy complejo el poder desvincular, clara y terminantemente, la faceta mercantil del propio entorno de su privacidad como persona física, según se indica en la citada resolución de la AEPD, dado que en la mayoría de los casos es posible que ambas facetas se puedan, incluso, yuxtaponer. En caso de duda habrá que decantarse siempre a favor de la aplicación de la LOPD.

c. Datos de personas físicas identificables

Se pueden dar determinados supuestos en los que, en principio, no tengamos los datos identificativos de la persona física, aunque sí otros datos que la **pudieran hacer identificable.** A modo de ejemplo, si tratamos los datos de una persona física "A", sin tener su nombre, apellido, etc., únicamente llamándola y conociéndola por "A", no se trataría de datos de persona identificable. Pero si igualmente supiéramos que "A" es propietario del inmueble sito en la calle X, portal A, piso 1ºB, al tratar y conocer esta información, los datos que poseamos de "A" corresponderían a una persona identificable, dado que no es muy complejo llegar al dato de la persona física a través de la titularidad de un inmueble.

La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que supuso la derogación de la LORTAD y su sustitución por la vigente LOPD, definió como dato personal toda aquella información sobre una persona física identificada o identificable, considerándose identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social. Sirva por tanto la imagen, o la voz, el dato relativo al número de teléfono, entre otros muchos elementos, los que pueden hacer identificable a la persona. Por tanto, y en consideración con lo anterior, queda claro que los datos que se obtengan a través de grabaciones de

vídeo o sonido deben tratarse como datos personales, dado que se pueden tratar de datos de personas identificables.

El Considerando 26 de la citada Directiva añade que para determinar si una persona es identificable, hay que considerar el *conjunto de los medios que puedan ser razonablemente utilizados* por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona.

Por su parte, el Real Decreto 1332/1994, de 20 de junio[1], que desarrollaba determinados aspectos de la LORTAD, establece en su artículo primero, que se entiende por datos de carácter personal toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable.

La sentencia de la Sección primera de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de fecha 8 de marzo de 2002 dispuso lo siguiente: *"Sin embargo, y para que exista dato de carácter personal (en contraposición con dato disociado) no es imprescindible una plena coincidencia entre el dato y una persona concreta, sino que es suficiente con que tal identificación pueda efectuarse sin esfuerzos desproporcionados, tal y como se desprende del mencionado artículo 3 de la Ley, en sus apartados a) y f) y también del Considerando 26 de la invocada Directiva 95/46/CE que expresamente señala que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona; que los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado; que los códigos de conducta con arreglo al artículo 27 pueden constituir un elemen-*

[1] Vigente en cuanto no contradiga la LOPD y no se apruebe un Reglamento que aplique la anterior norma, según establece la Disposición Transitoria tercera de la LOPD.

to útil para proporcionar indicaciones sobre los medios gracias a los cuales los datos pueden hacerse anónimos y conservarse de forma tal que impida identificar al interesado".

Para saber si estamos ante un dato de carácter personal de persona identificable, habrá que analizar el caso concreto. Si no es posible mediante la utilización de medios razonables, asociar determinados datos a una persona física, no estaremos ante datos de carácter personal y, por tanto, no sería de aplicación la LOPD. La prudencia obliga a que en caso de duda, se entienda que estamos ante una persona identificable.

Igualmente, podemos señalar como dato de persona identificable, a modo de ejemplo, la matrícula de un vehículo, así como la dirección de correo electrónico de una persona (dado que podría consistir en NOMBRE y APELLIDOS @..., lo que convierte dicha dirección en datos de una persona física, o bien, a través del dominio al que pertenece dicha dirección, ...@AAA, se podría conseguir el dato del titular de la dirección), su número de teléfono móvil, una grabación de una cinta de seguridad, una fotografía, un dibujo, etc. Dado que en dichos supuestos, se podría pasar de persona identificable a identificada, sin aplicar esfuerzos desproporcionados.

Hay que tener igualmente en cuenta, que lo que *a priori* podría no considerarse un dato de carácter personal, sí puede serlo atendiendo a la información que se pueda obtener del mismo. Por ejemplo, de un determinado dibujo se puede extraer información de la personalidad de quien lo pintó; o de una prueba psicotécnica de un análisis grafológico; una determinada prueba médica (por ejemplo, un TAC) asociada simplemente a unas iniciales, en el supuesto de que el resultado sea una enfermedad no común (respecto a los familiares y amigos que conozcan la existencia de dicha enfermedad no común), por lo que esta información podría ser considerada a efectos jurídicos como datos de carácter

personal, y además relacionada con una de las esferas que gozan una especial protección en la LOPD, la protección de los datos de salud.

1.2.2 Tratamiento de datos

Según establece el artículo tercero de la LOPD, se entiende por tratamiento de datos, *"aquellas operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".*

Partimos de una definición muy amplia que englobaría todas las fases, desde que se recogen los datos del interesado o afectado, hasta su posterior manipulación, incorporación en ficheros, cesión a terceros, realización de segmentaciones a los efectos de obtener información adicional, la compra y el arrendamiento de bases de datos, y así un largísimo etcétera.

Siempre que se realice un tratamiento de datos de carácter personal, y nos encontremos dentro del ámbito de aplicación de la LOPD (punto 1.3.) **deberemos observar todos los principios protectores recogidos en la citada norma,** y ello, como ya se ha indicado, sin perjuicio de que tengamos un interés o derecho en el tratamiento de los mismos. Respecto al concepto "tratamiento de datos", de forma muy general, podemos señalar qué es lo que vamos a hacer con los datos de carácter personal.

1.2.3 Interesado o afectado

El **interesado o afectado** es la persona física titular de los datos que van a ser objeto de tratamiento, la persona física cuyos datos serán tratados por la compañía.

Desde los trabajadores de la empresa, sus proveedores, las personas que colaboren con ésta, sus clientes, etc. Es importante indicar que la LOPD reconoce al interesado como el verdadero titular de los datos y no al responsable del fichero o tratamiento, pudiendo realizar éste último un tratamiento de dichos datos, siempre y cuando se cumplan las garantías y presupuestos establecidos por la Ley.

Igualmente es reseñable que sólo las personas físicas ostentarán la condición de interesados o afectados (como ya se indicó en el epígrafe 1.2.1).

El afectado es quien tiene el **poder de control** sobre sus datos personales, a través de los mecanismos jurídicos previstos en la LOPD que conllevan una serie de obligaciones a quien pretenda tratarlos y los consecuentes derechos que corresponden a las personas cuyos datos vayan a ser objeto de tratamiento.

1.2.4 Responsable del fichero y del tratamiento

El **responsable del fichero** o tratamiento es la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que **decide sobre la finalidad, contenido y uso** del tratamiento.

Por tanto, pueden ser responsables:

- Personas físicas de naturaleza pública o privada.
- Personas jurídicas de naturaleza pública o privada.
- Órganos administrativos.

En algunos casos se pueden dar supuestos en los que sea complejo determinar *a priori* quién es el verdadero responsable del tratamiento y del fichero, sobretodo en supuestos en los que intervenga algún encargado del tratamiento, o existan diferencias entre el responsable del fichero y responsable del tratamiento.

La LOPD en su artículo tercero (definiciones) no diferencia entre quién es el responsable del tratamiento y responsable del fichero, siendo determinante su diferenciación.

La sentencia de fecha 28 de febrero de 2005 del Tribunal Supremo señaló: "*esto es así porque la nueva Ley Orgánica —a diferencia de la vieja Ley Orgánica, que atribuía la potestad de decidir sobre la finalidad, contenido y uso del tratamiento únicamente al responsable del fichero— reconoce que esa decisión pueda tomarla —y así ocurre muchas veces— el responsable del tratamiento.*

He aquí el nuevo texto: Ley 15/1999 . 'Artículo 3. A los efectos de la presente Ley se entenderá por: (...) *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'".*

No se trata como se ve de un mero cambio de redacción, de un simple giro gramatical, o una innovación puramente estilística. Es algo más profundo: estamos ante un cambio esencial en el modo de afrontar la regulación de las relaciones que se entablan entre quienes manejan los datos y el titular de los mismos."

Con independencia de la postura o funciones del responsable del fichero, puede coexistir la figura del responsable del tratamiento, quien, sin que tenga ningún contacto físico con los datos de carácter personal, puede ser sancionado por entenderse que fue éste quien decidió sobre la finalidad, contenido y usos del tratamiento. Sería por ejemplo el caso de una entidad que encargue a otra la realización de una campaña publicitaria. La primera entidad encargaría a la segunda que recabase de terceros determinados datos, y que les remitiese determinada información publicitaria. En ese caso, la primera entidad, pese a que no hubiera tenido contacto con los datos, podría ser la responsable del tratamiento y, la segunda, la responsable del fichero, pudiendo ser sancionadas ambas entidades en caso de tratamientos contrarios a los principios de la LOPD (por ejemplo,

que la responsable del fichero, en la obtención de los datos, no hubiese obtenido los consentimiento informados precisos).

Es por ello por lo que incluso en los supuestos en que encarguemos una determinada campaña, o un determinado tratamiento a un tercero, no deberemos pensar que será éste el responsable, y quien deba cumplir con todas las obligaciones derivadas de la LOPD, dado que en muchas circunstancias, **podremos ser igualmente sancionados aunque no hayamos tenido ninguna clase de contacto con los datos, en la media en que aunque no haya existido contacto con los datos, hayamos decidido sobre la finalidad, contenido y usos de los datos.**

1.2.5 Fichero

Un **fichero** es todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

La LOPD permite la creación de ficheros de titularidad privada que contengan datos de carácter personal, cuando sea necesario para el logro de una actividad u objeto legítimo del que fuera a ser el titular del fichero, y siempre y cuando se respeten los principios y garantías que se recogen y desarrollan en la LOPD, a los efectos de la necesaria protección de los derechos de las personas cuyos datos serán tratados.

Por un lado, la LOPD recoge lo que sería un tratamiento de datos y, por otro, lo que es un fichero, debiendo resaltarse, que el objeto de la LOPD (artículo 1 de la LOPD), es el 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. Por tanto, puede existir un determinado tratamiento de datos de carácter personal que estará amparado por la LOPD, con

independencia de que esos datos fueran o sean incorporados a un fichero, ya sea informatizado o manual.

En segundo lugar cabe indicar que no encajará en el concepto de fichero, la información que se incorpore a un archivo, que no esté organizado por criterios específicos y determinados de búsqueda y que no permita acceder a los datos de alguna forma eficaz y precisa, todo ello sin perjuicio de que los tratamientos de datos que se realizasen, sí estarían amparados por la LOPD (un archivo de texto, en el que se recoja determinada información referente a personas físicas, pero sin criterios de búsqueda, orden, etc.).

1.2.6 Encargado del tratamiento

El **encargado del tratamiento** es la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

El supuesto consiste en que un tercero trate, según establece la definición, los datos de carácter personal, por cuenta del responsable. Por tanto, el encargado, al no ser responsable de los tratamientos que fuera a realizar, deberá ceñirse a las instrucciones que a tal efecto le imparta el responsable, quien a la postre, será el que decida sobre la finalidad, contenido y uso del tratamiento.

Se trata de una figura que suele aparecer frecuentemente en las subcontrataciones de servicios, en las que el subcontratista, para prestar los servicios encomendados, debe acceder a datos de carácter personal que no son de su responsabilidad. Por ejemplo, en el supuesto en que una gestoría se encargue de llevar la contabilidad o las nóminas de los empleados de una empresa. En ese caso, dado que el responsable de los datos de los trabajadores es la propia empresa, y ésta ha decidido que las nóminas las elabore la gestoría, ésta última accedería a los datos responsabilidad de

la empresa para prestar el servicio de elaboración de nóminas (acceso a datos siempre que se cumplan escrupulosamente los requisitos exigidos en el artículo 12 de la LOPD).

Es importante señalar que no surgirá una nueva relación jurídica entre el trabajador de la empresa (afectado) y la gestoría (encargada del tratamiento), dado que el afectado la relación la tiene con el responsable, siendo ésta una de las notas diferenciadoras del acceso a datos y de la cesión de éstos.

1.2.7 Fuentes accesibles al público

Las **fuentes accesibles al público** son 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,** y siempre y cuando se cumpla la premisa anterior:

- El censo promocional.
- Los repertorios telefónicos en los términos previstos por su normativa específica (Reglamento sobre las Condiciones para la Prestación de Servicios de Comunicaciones Electrónicas, el Servicio Universal y la Protección de los Usuarios aprobado por Real Decreto 424/2005, de 15 de abril).
- Las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de: nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo.
- Los diarios y boletines oficiales y los medios de comunicación.

Hay que señalar que el artículo 28.3 de la LOPD indica que *"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 telepáticamente 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".

La LOPD como se ha visto, establece una lista *numerus clausus,* por lo que **exclusivamente** se beneficiarán del tratamiento más flexible que se recoge en la LOPD a los citados ficheros, y siempre y cuando se cumpla la premisa indicada, no siendo aplicable a otros por analogía.

1.2.8 Procedimiento de disociación

A través de la disociación tratamos los datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable. Si de la base de datos de proveedores, elimino todos los datos que pueden hacer a éstos identificables (nombre, domicilio, teléfono, dirección de correo electrónico, etc.) y asigno un código a dichos datos, estaremos tratando datos disociados. Ahora bien, no se podrá tener un fichero paralelo en el que se pueda vincular el código asignado a cada proveedor, a sus datos identificativos.

1.3 A quién se aplica la ley y exclusiones

La LOPD se aplica, en virtud de lo dispuesto en su artículo segundo, 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*".

Por tanto, es necesario que nos encontremos ante datos:

- De carácter personal.
- Que se encuentren registrados en un soporte físico. El soporte podrá ser tanto automatizado, como manual, así como papel, unidades de disco, DVD, etc.

- Que sean susceptibles de tratamiento. Como ya se vio, el concepto de tratamiento de datos es sumamente amplio, abarcando todas las fases que se pueden realizar con los datos personales (recogida, conservación, cesión, etc).
- El uso posterior que se pueda realizar de ellos. Quedarían comprendidos por dicho precepto, tanto el puro mantenimiento de los datos, como su modificación, segmentación, venta de los mismos, etc.

Será de aplicación la LOPD en los tratamientos y usos que se hagan de los datos tanto por el sector público como por el privado.

El **principio de territorialidad** de aplicación a la LOPD queda definido en el artículo 2.1 que establece que se regirá por la LOPD 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."

Como **supuestos de no aplicación** y, por tanto, de excepción al régimen general anteriormente indicado, serán según se recoge en el punto segundo del mencionado artículo 2 de la LOPD, los siguientes:

"a. A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas".

Dicho supuesto queda limitado únicamente al ámbito personal o doméstico, por lo que sí sería de aplicación la LOPD al resto de ámbitos (profesional, etc.).

"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."

En este último, pese a quedar recogido como supuesto de no aplicación del régimen de la LOPD, se recoge una obligación de comunicación de la existencia del fichero a la AEPD. Por tanto, dada la especial relevancia de los datos que serán tratados en dichos ficheros, al menos la AEPD debe ser informada de la existencia de dichos ficheros.

Será de aplicación supletoria la LOPD en los supuestos no previstos por su normativa específica, en los siguientes tratamientos de datos:

"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."

Movimiento internacional de datos

6.1 Concepto y régimen general

El principio general establecido por la LOPD en su artículo 33, establece *"no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia Española de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.*

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

6.2 Excepciones

Lo dispuesto en el artículo 33 de la LOPD no será de aplicación, según dispone el artículo 34 de la misma, en los siguientes supuestos:

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 médico, 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.

Tratamientos habituales en una PYME

7.1 Recogida de datos e incorporación a ficheros

La Figura 7.1 muestra las fuentes más habituales de entrada de datos en una empresa. Como se puede observar, se recaban datos, tanto de forma directa (clientes, contactos, personas que acceden al edificio, vigilancia del edificio, trabajadores, candidatos, potenciales clientes), como de forma indirecta (candidatos que remiten las empresas de selección, datos de familiares de los trabajadores y datos obtenidos de fuentes accesibles al público).

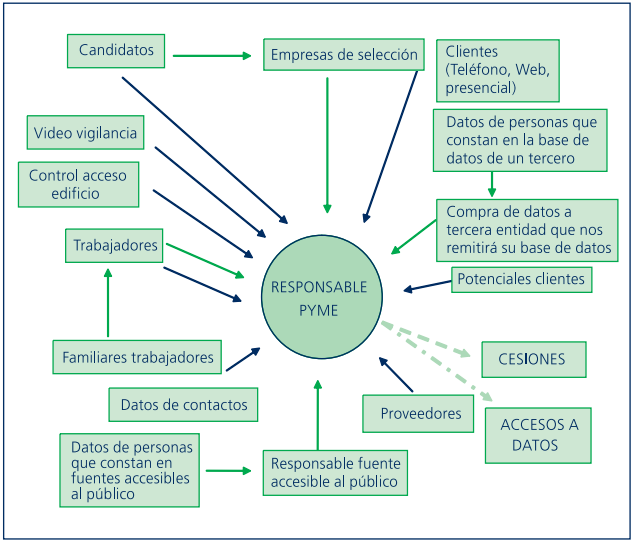
La entidad responsable, ha debido con carácter previo:

- Implementar las **medidas de seguridad** en los ficheros en los que se van a incorporar los datos que se van a recabar. Dichas medidas irán en función de la tipología de datos que se vayan a incorporar a dichos ficheros (artículo 9 LOPD y RD 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).
- **Inscribir los ficheros** en la AEPD (artículo 26 LOPD).
  - Clientes.
  - Clientes web.
  - Vigilancia del edificio.Aplicación de la reciente Instrucción 1/2006, de 12 de diciembre, de la Agencia Española de Protección de Datos sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. Dicha norma regula el concreto tratamiento

de dichos datos. Se puede descargar un modelo de identificación de zona videovigilada (www.agpd.es).

- Control de acceso al edificio.
- Proveedores.
- Clientes potenciales.
- Recursos humanos.
- Marketing y comercial.
- (…).

Figura 7.1. Fuentes de entrada de datos.



- Garantizar el **secreto profesional** en el tratamiento de datos a través de cláusulas de confidencialidad y secreto profesional con sus trabajadores (artículo 9 LOPD).

- Tener previsto un procedimiento para dar pleno cumplimiento, en forma y plazo, de las solicitudes de **ejercicio de los derechos** que corresponden a los afectados (artículos 13 a 19 LOPD).
- Verificar que los datos personales que va a introducir en sus ficheros, y que va a tratar, cumplen con el **principio de calidad de los datos.** Se debe determinar cuáles son los tipos de datos que realmente requiere para la consecución de las finalidades legítimas que pretende conseguir con el tratamiento de datos, debiendo ser éstos adecuados, pertinentes, no excesivos, exactos y puestos al día, etc. (artículo 4 LOPD).
- Verificar que se está **informando, de forma correcta,** en todos los supuestos en los que se están recabando datos. En concreto, la información varía en función de si los datos se están recabando directamente de los afectados o se están recabando de forma indirecta (artículo 5 LOPD). En caso contrario, establecer un sistema para informar a los afectados que no hayan sido informados y establecer procedimientos para informar en todos los supuestos detectados de entrada de datos. Se deberá guardar la documentación que justifique que se está cumpliendo con la obligación de información.
- Que los datos **se almacenen de forma que se pueda permitir el ejercicio del derecho de acceso** por parte de los afectados (artículo 4 LOPD).
- Establecer un procedimiento interno para garantizar la calidad de los datos tratados (dar debido cumplimiento a los derechos de rectificación así como establecer procedimientos, por ejemplo anuales, de verificación de los datos tratados, remitiendo una comunicación a los afectados).

7.2 Verificación de datos especialmente protegidos

En el supuesto en que se estén recabando, por cualquiera de los canales de entrada de datos en la empresa, datos especialmente

protegidos, debemos verificar que o tenemos el consentimiento expreso o bien expreso y por escrito (en función de las categorías de datos especialmente protegidos que recibamos) o es de aplicación alguna de las excepciones al tratamiento de dichos datos (artículo 7 LOPD).

En los supuestos en los que recabemos datos de ideología, religión o creencias, además deberemos advertir al interesado acerca de su derecho a no prestar dicho consentimiento (artículo 7.1 LOPD)

Deberemos guardar prueba suficiente que acredite el título que habilita el tratamiento de dichos datos, en concreto, el consentimiento expreso o expreso y por escrito, así como haber informado en el supuesto contemplado en el artículo 7 de la LOPD. En caso de no haberlo realizado, se deberá proceder de inmediato a establecer un procedimiento para la obtención de todos esos consentimientos, en los casos en que fuere preciso.

7.3 Verificación de consentimientos para los tratamientos de datos que son realizados por la compañía

Una vez analizados todos los canales de entrada de datos en la empresa y, por consiguiente, todos los datos que están siendo tratados, deberemos analizar si tenemos el consentimiento para tratar dichos datos, en el caso en que éste consentimiento fuere preciso. Deberemos guardar acreditación suficiente respecto a la obtención de dicho consentimiento en los supuestos en que sea necesario, ante eventuales reclamaciones que nos pudieran formular.

Habrá que ir analizando cada canal de entrada de datos y verificar las finalidades perseguidas a través del tratamiento de dichos datos. Una vez identificadas las finalidades, identificaremos si es o no necesario el consentimiento para el cumplimiento y ejecución de las mismas. Sirva como ejemplo la Tabla 7.1.

Tabla 7.1. Ejemplo de verificación de consentimientos.

Fichero	Finalidades	¿Datos especialmente protegidos?	Consentimiento general (art. 6 Lopd)	Consentimiento expreso
Clientes Proveedores	Mantenimiento de la relación contractual con clientes.	Sí. SALUD. Servicios de asistencia. No habilitación legal.	NO	SÍ (7.3 LOPD)
	Remisión de publicidad comercial de productos de alimentación.	–	SÍ	–
	Remisión de la anterior información comercial por correo electrónico.	–	SÍ	SÍ (LSSI)
	Mantenimiento de la relación contractual con proveedores.	–	NO	–
Trabajadores	Mantenimiento de la relación contractual.	–	NO	–
	Controles médicos voluntarios de los trabajadores.	Datos de salud derivados de reconocimientos médicos. (APTO Y NO APTO)	SÍ	SÍ (7.3 LOPD)
	Retención IRPF.	Datos de salud. Porcentaje discapacidad a efectos retención IRPF	SÍ	SÍ (7.3 LOPD)
Control de acceso al edificio	Control de la seguridad del edificio.	–	SÍ	–
Potenciales clientes	Remisión de publicidad.	–	SÍ	–

Una vez analizados dichos extremos, deberemos, en caso de que sea necesario algún consentimiento, proceder a recabar el mismo y almacenarlos ante eventuales reclamaciones.

Si el consentimiento necesario no es expreso ni expreso y por escrito, habrá que valorar el recabar dicho consentimiento de forma tácita (en los términos ya vistos al analizar la figura del consentimiento, remitiendo una comunicación al afectado y dándole un plazo de 30 días para oponerse a dicho tratamiento. En el supuesto de que se optase por esta vía, deberemos poder acreditar la recepción de la comunicación, así como el contenido de la misma).

Igualmente, respecto a los datos que estemos recabando de forma indirecta, deberemos verificar la existencia del consentimiento. Por ejemplo, respecto a los datos de los familiares de los trabajadores podremos recabar directamente el consentimiento a través de nuestros propios empleados. En el supuesto, por ejemplo, de adquisición de una base de datos a un tercero, deberemos actuar en el contrato de adquisición de dicha base de datos, como se indicó en el epígrafe 3.5 así como verificar de forma suficientemente diligente, la verificación de la existencia de dichos consentimientos para la comunicación de sus datos y su posterior tratamiento por la cesionaria.

7.4 Identificación de accesos a datos y comunicaciones

Deberemos identificar todos los accesos que se estén produciendo. En caso de que no existiese contrato de acceso a datos en dichos supuestos, se debería formalizar el mismo con las garantías exigidas por la LOPD.

En el supuesto de comunicaciones de datos, se deberá proceder como se hizo para la identificación de tratamientos de datos y necesidad o no de consentimiento. Si es preciso el

consentimiento, deberemos obtener el mismo, debiendo verificar que no se estén cediendo datos especialmente protegidos. En este caso, se debería verificar el cumplimiento de los requisitos para la comunicación de esa tipología de datos.

Tabla 7.2. Ejemplo de cesión de datos.

Fichero	Cesiones/consentimiento necesario (sí/no)	Accesos a datos
Clientes	Bancos. Facturación/NO (artículo 11.2.c) LOPD)	Empresa que se encarga ensobrado.
		Call center externo de apoyo.
		Realizaciones de encuestas.
	Administración de Justicia. Impagados/NO (11.2.d) LOPD)	Gestión de cobros.
Proveedores	Bancos. Facturación/NO (artículo 11.2.c) LOPD)	NO
	Agencia Tributaria/NO (artículo 11.2.a) LOPD).	
Trabajadores	Bancos. Pago nómina/NO (artículo 11.2.c) LOPD)	Acceso por gestoría. Elaboración nóminas.
	Seguridad Social/NO (artículo 11.2.a) LOPD	NO
	Agencia Tributaria/NO (11.2.a) LOPD	
Control de acceso al edificio	–	Empresa de seguridad externa.
Potenciales clientes	Venta Base de datos a un tercero o arrendamiento/SÍ	Empresa que se encarga de ensobrado y remisión cartas.

En el caso de que se vayan a comunicar datos de carácter personal, deberemos informar de dicho extremo, salvo que fuera un supuesto de excepción (artículo 27 LOPD).

Principios generales de la LOPD

2.1 Calidad de los datos. Qué datos se pueden tratar

El principio de calidad se encuentra recogido en el artículo cuarto de la LOPD. A continuación, se recogen las principales obligaciones para aquellos que traten datos personales, respecto a la calidad de los datos:

> Los datos de carácter personal sólo se podrán recoger, así como someterlos a 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.

Esto supone que con el consentimiento del interesado o afectado no se pueden tratar todo tipo de datos. Previamente a la obtención de datos, se debe analizar cuáles son aquellos estrictamente necesarios para la consecución de las finalidades legítimas que pretendemos conseguir a través del tratamiento de datos de carácter personal y no recabar más datos. Por ejemplo, el tratamiento del dato del nivel de estudios de una persona que pretende contratar una línea telefónica se antoja, cuanto menos, excesivo y no pertinente para la consecución de dicha finalidad (la de la contratación de la línea telefónica).

Este principio se encuentra estrechamente ligado con la obligación de información en la recogida de datos, dado que de

dicha información se desprenderá cuáles son los datos imprescindibles o necesarios para la consecución legítima de las finalidades informadas. En concreto, y como se verá más adelante, en la recogida de los datos hay que informar del carácter obligatorio o facultativo de la respuesta a las preguntas que se puedan plantear al afectado en la recogida de los datos y de las consecuencias de la negativa a facilitarlos y de la obtención de los mismos por parte del responsable. No se deben recabar datos que realmente no sean imprescindibles.

Los datos de carácter personal **no podrán usarse para finalidades incompatibles** con aquellas para las que los datos hubieran sido recogidos (no se consideran incompatibles el tratamiento posterior de los datos con fines históricos, estadísticos o científicos).

Es decir, si recabo datos para prestar un servicio a una determinada persona. No podré tratarlos para algo que no esté estrechamente relacionado con ese servicio.

En apoyo de lo anterior, el Tribunal Constitucional, en su Sentencia 292/2000 de 30 de noviembre de 2000, establece: *"Ahora bien, aún habiendo llegado a esta conclusión no es ocioso señalar, de un lado, que el derecho a consentir la recogida y el tratamiento de los datos personales (artículo 6 LOPD) no implica en modo alguno consentir la cesión de tales datos a terceros, pues constituye una facultad específica que también forma parte del contenido del derecho fundamental a la protección de tales datos. Y, por tanto, la cesión de los mismos a un tercero para proceder a un* ***tratamiento con fines distintos*** *de los que originaron su recogida,* ***aun cuando puedan ser compatibles con éstos*** *(artículo 4.2 LOPD), supone una nueva posesión y uso que requiere el consentimiento del interesado. Una facultad que sólo cabe limitar en atención a derechos y bienes de relevancia constitucional y, por tanto, esté justificada, sea proporcionada y,*

además, se establezca por Ley, pues el derecho fundamental a la protección de datos personales no admite otros límites (...)*".*

Aunque esta sentencia del Tribunal Constitucional examine el supuesto de una cesión de datos, puede entenderse, aunque sea de forma indirecta, que su interpretación del principio de finalidad sería que dicho precepto no permite el tratamiento de datos con fines **distintos** de los que originaron su recogida, en contraposición con la referencia a finalidades incompatibles establecida en la LOPD.

Se podría dar un supuesto de doble vínculo con un determinado afectado. Por ejemplo, que éste haya contratado dos productos diferentes con un determinado responsable, o bien que existan dos vínculos de naturaleza jurídica distinta, como puede ser el laboral y el de prestación de servicios. De este último caso sería un buen ejemplo el supuesto en que a un empleado de una sociedad contrate un servicio comercializado por la sociedad para la que trabaje.

En estos supuestos, los datos que se han obtenido por el responsable como consecuencia de las dos finalidades distintas para las cuales ha recabado los datos del afectado (ámbito laboral y de prestación de servicios), deben ser estancas, sin que se puedan conectar ambos ficheros o tratamientos, enriqueciéndose así los datos. Ello es así porque para la relación laboral ha consentido el afectado el tratamiento de determinados datos para la consecución de dicha finalidad, y no otros, y lo mismo ocurría con los datos facilitados para la prestación del servicio solicitado a la compañía para la que trabaja. Si se cruzasen los datos, se estarían tratando indudablemente para finalidades distintas.

Serán **exactos** y **puestos al día** de forma que respondan con veracidad a la situación actual del afectado. En caso de que los datos de carácter personal fueran total o parcialmente inexactos, o incompletos, serán cancelados y sustituidos de oficio por los datos rectificados o completados. Dicha rectificación y cancelación podrá ser instada directamente por el afectado o interesado.

Cuestión más que razonable. El hecho de tratar datos inexactos o no puestos al día puede perjudicar al afectado (supuesto de los ficheros de "morosidad") así como conllevar que el responsable incumpla algún otro principio de la LOPD (por ejemplo, si remito una comunicación a un cliente a un domicilio distinto. Podría incumplir la obligación de secreto). La duda que puede surgir es qué ocurre en el supuesto en que se estén tratando datos que no sean exactos y puestos al día, en el caso en que el responsable desconozca esa inexactitud.

Lo que parece razonable es que deba ser el propio interesado o afectado el que deba informar de los cambios que se puedan producir en los datos que legítimamente son tratados por parte de un determinado responsable y que se obtuvieron con todas las garantías exigidas por la LOPD. Esto es así, dado que los contratos, desde que se perfeccionan, obligan, no sólo al cumplimiento de lo expresamente pactado, sino también a todas las consecuencias que, según su naturaleza, sean conformes a la buena fe, al uso y a la ley (artículo 1258 Código Civil).

Qué duda cabe que si a un determinado responsable, le facilita un afectado determinados datos, y se produce una variación en éstos, el afectado, conforme a la buena fe, debería indicar al responsable el cambio en sus datos personales, a los efectos que proceda el responsable a rectificarlos. De lo contrario, los responsables de ficheros deberían estar constantemente verificando los datos que están sujetos a tratamiento, dado que en cualquier momento se puede producir un determinado cambio en éstos.

Con independencia de lo anterior, el responsable deberá establecer procedimientos para la verificación de la exactitud de los datos. Bastaría, por ejemplo, que el responsable remitiese una comunicación cada cierto tiempo a las personas cuyos datos está tratando, informándoles de los datos objeto de tratamiento, a los efectos de que puedan revisarlos y modificarlos en el caso en que existiese alguna inexactitud.

En el supuesto en que los datos los recibamos directamente del afectado, se deberá presumir la exactitud de los datos recabados, ahora bien, se deberá establecer un sistema en la recogida de datos que permita verificar la identidad de quien nos los facilita, dado que, en caso contrario, podríamos estar tratando datos inexactos, y sin el consentimiento del afectado, pudiendo ser duramente sancionados por parte de la AEPD ("A" simulando ser "B", contrata a nombre de éste un determinado servicio con una empresa, no verificando ni comprobando ésta última dicho extremo).

La cancelación de los datos y la rectificación de los mismos se verán en el apartado 5.2 de este libro.

Los datos de carácter personal deberán ser 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.

Como ya se ha indicado, en el epígrafe 5.2 de este libro se analizará el derecho del afectado a cancelar y a rectificar los datos. Únicamente cabe indicar que, en aras de lo ya expuesto en los anteriores puntos, si los datos han dejado de ser necesarios o pertinentes, no podrán ser objeto de tratamiento, dado que en caso contrario se estaría incumpliendo con el principio de adecuación, finalidad y pertinencia.

No se podrán recoger datos por medios fraudulentos, desleales o ilícitos.

En caso contrario, nos encontraríamos ante un vicio en el consentimiento derivado del engaño sufrido durante la recogida de los datos.

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

Obligación formal que se impone al responsable. Se puede observar la importancia que otorga el legislador al derecho de acceso, al ubicar dicha obligación dentro del propio principio de calidad. El responsable deberá, por tanto, registrar los datos, de forma que sea capaz de:

- Facilitar información a los afectados de los datos que son tratados.
- Poder indicar a los afectados el origen de los datos.
- Cuáles han sido las cesiones de datos realizadas.
- Cuáles son las cesiones previstas.

2.2 Información

El principio de información es, junto con el del consentimiento, uno de los pilares básicos del derecho a la protección de datos de carácter personal. Se encuentra desarrollado en el artículo quinto de la LOPD.

Dado que los datos de carácter personal se pueden recabar, bien directamente del interesado o afectado, o a través de un tercero (de forma indirecta), las obligaciones de información variarán en los citados casos. Si no existiese una obligación de información, quedaría vacío de contenido el derecho del afectado a consentir, a controlar y a disponer el uso por parte de terceros de sus datos de carácter personal, dado que una ausencia de información, impedirá un ejercicio correcto de su derecho a consentir, un conocimiento de quién está tratando sus datos y para qué o con qué finalidades, y un adecuado ejercicio de sus derechos a acceder, rectificar, cancelar u oponerse, frente al tratamiento de sus datos personales.

Dado que el derecho de información garantiza el correcto ejercicio de otra serie de derechos recogidos en la LOPD, será de suma importancia que se efectúe conforme establece la ley, para evitar, por tanto, un tratamiento de datos ilícito y, como consecuencia, un vicio en el resto de tratamientos derivados del tratamiento de datos mal informado.

El consentimiento es una manifestación de voluntad. Libre, inequívoca, específica e **informada,** mediante la que el interesado consiente el tratamiento de datos personales que le conciernen. Por tanto, queda claro el vínculo entre información y consentimiento.

Si se obtuvo el consentimiento para un determinado tratamiento de datos, y no se informó según se verá a continuación, no nos encontraremos ante un tratamiento de datos validamente aceptado y consentido. Por tanto, el informar al afectado en la recogida de datos es lo único que podrá garantizar el derecho de éste a poder consentir.

Hay que indicar que pese a que los datos sean voluntariamente facilitados por el afectado, ello no exime del deber de información. Si, por ejemplo, para el consentimiento para el tratamiento de determinados datos como para la cesión de los mismos se recogen excepciones a la regla general, con la obligación de información, no existen tales excepciones. Únicamente, como se verá, no existiría la obligación de informar respecto a varios puntos concretos de los enumerados en el artículo 5.1 de la LOPD, y existirá una excepción al deber de informar en determinados supuestos en los que los datos no son recabados directamente del afectado.

Se debe cumplir con la obligación de información, con independencia del método que se utilice para la obtención de los datos (teléfono, Internet, formularios, etc.) si bien, cuando se utilicen cuestionarios u otros impresos para la recogida, deberán figurar en los mismos, de forma claramente legible, todas las

advertencias a que se refiere en los puntos siguientes. Respecto a la obtención de datos por otras vías distintas de los cuestionarios o contratos, indicar que el responsable deberá poder garantizar que cumplió con la obligación de informar al afectado (grabación de llamadas en las que se informe al afectado, etc.).

2.2.1 Datos obtenidos de forma directa del interesado

a. Contenido del derecho de información

El supuesto más habitual es aquel en el que los datos que se recaben lo sean directamente del titular de los mismos, esto es, del afectado. Ocurrirá en el momento en que celebremos un contrato de trabajo (se recabarán los datos personales del trabajador), un contrato de prestación de servicios (recabaremos el dato de la persona que vaya a realizar la prestación de servicio y de los representantes legales que firmen el contrato, en el supuesto de una persona jurídica), un cuestionario cumplimentado por el afectado y entregado al responsable, etc.

En los referidos contratos, también se podrán obtener datos de personas físicas de forma indirecta. En concreto, y por poner un ejemplo, de las personas físicas que consten en el contrato como personas de contacto para cualquier comunicación derivada del contrato.

La información que se debe facilitar al afectado, deberá ser expresa, precisa e inequívoca. No se podrá, por tanto, informar de forma ambigua, oscura, indeterminada, imprecisa, general, confusa, etc. Se deberá precisar al máximo, teniendo en cuenta que informaciones poco claras, demasiado genéricas, ambiguas, se entenderán que no cumplen con el principio de información. No deberá quedar ninguna duda respecto del contenido de la información que se facilite al afectado, dado que el contenido de la información será lo que en su caso autorice el afectado.

El contenido mínimo de la obligación de información para los supuestos en que se recaben los datos directamente del afectado, consta en el artículo 5.1 de la LOPD, que establece que:

> *"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."*

Lo normal es que los datos que se recaben, vayan a ser incorporados a un fichero responsabilidad de quien recabe los datos. Dicho fichero, podrá ser tanto automatizado como manual, siendo independiente el soporte en el que se encuentre el mismo (afectaría en cuanto a las medidas de seguridad que se deban implementar, formas de garantizar el cumplimiento de las obligaciones, etc.). En el caso de que no fueran a incorporarse a un fichero, habrá que indicar en cualquier caso la existencia de un tratamiento de datos de carácter personal. Al igual que en el caso anterior, el tratamiento de datos podrá ser automatizado o no.

Respecto a la finalidad para la cual se tratarán los datos, indicar que es uno de los puntos en que en mayor medida habrá que precisar y ajustar la información, dado que la AEPD no admite determinadas informaciones respecto a finalidades demasiado vagas o indeterminadas. Es preciso que la información que se facilite al afectado sea, como indica el artículo 5 de la LOPD, expresa, precisa e inequívoca. Por tanto, las finalidades que se informen no podrán ser demasiado genéricas como, por ejemplo, "para ofrecerle productos de su interés". ¿Qué clase de productos ha autorizado? ¿Quién determina lo que es de su interés?

La información respecto a la finalidad deberá ponerse en relación con lo dispuesto en el artículo 4.1 de la LOPD (calidad

de los datos). En concreto, se desprende de dicho precepto que únicamente se pueden recoger y tratar datos de carácter personal 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.** Los datos personales no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

Por tanto, la finalidad que se informe será aquella para la cual estemos habilitados, y si se produjera un cambio de finalidad en el tratamiento, debería, de nuevo, cumplirse con la obligación de información así como con la obtención del consentimiento si fuere preciso. Por ejemplo, si se obtuviera un consentimiento para remitirle información publicitaria sobre productos o servicios relacionados con turismo y el afectado recibiese información referente a productos o servicios financieros, nos encontraríamos con un tratamiento distinto o incompatible a la finalidad informada y consentida por el afectado y, por tanto, ilícita.

En último lugar, respecto a la información correspondiente a los destinatarios de la información, surgen dudas respecto a su interpretación o alcance. La Directiva 95/46/CE establece como contenido mínimo de la obligación de información, en el supuesto de que los datos sean recabados directamente del afectado, los siguientes puntos:

"a. la identidad del responsable del tratamiento y, en su caso, de su representante;

b. los fines del tratamiento de que van a ser objeto los datos;

c. cualquier otra información tal como:

- *los destinatarios o las categorías de destinatarios de los datos,*
- *el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder,*
- *la existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida*

cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado."

Se puede apreciar que la directiva recoge que se deberá informar al afectado de los destinatarios o de las categorías de destinatarios de los datos. Existe una diferencia significativa, dado que lo que parece más razonable es informar respecto a las categorías de destinatarios de los datos tratados, sin que sea preciso enumerar a todos los destinatarios posibles de los mismos, porque, en el momento en que se recaben los datos, no será posible, en la mayoría de los supuestos, identificarlos y, en caso de que se pudieran identificar durante el tratamiento de datos, podrían variar los destinatarios, permaneciendo, por lo general, invariable la categoría de los destinatarios de los datos.

Sería lógico, por tanto, interpretar que la información debe ir enfocada más a las categorías de los datos que a la identidad de los cesionarios, dado que el artículo 11 de la LOPD (cesiones de datos) establece la nulidad del consentimiento cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos y el tipo de actividad de aquel a quien se pretenden comunicar.

En el supuesto de no identificación concreta del cesionario, ¿quedaría desamparado el afectado por no poder identificar al nuevo responsable, cesionario de los datos? En principio, no debería quedar ni desinformado, ni desamparado, dado que el artículo 5.4 de la LOPD recoge la obligación de informar en supuestos en que los datos no hubieran sido recabados directamente del interesado (supuesto del cesionario al que hemos remitido los datos). Por tanto, si el cesionario cumpliese con su obligación de información, quedaría el interesado perfectamente informado sin que el cedente debiera identificar específicamente al cesionario de los datos. Igualmente, en apoyo a lo anterior, el responsable deberá informar en el momento en que se efectúe la

primera cesión de datos, entre otros aspectos que más adelante se verán, de los destinatarios de los datos, entre otros supuestos, salvo determinadas excepciones de aplicación a dicho caso.

En conclusión, si se conoce al destinatario, habrá que identificarle en la cláusula de protección de datos. En caso contrario, habrá, al menos, que identificar la categoría de destinatarios, complementándose dicha información cuando se conozca dicho extremo.

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

c. De las consecuencias de la obtención de lo3s datos o de la negativa a suministrarlos."

Dichas obligaciones, habría que relacionarlas con lo recogido en el artículo 4.1 y 4.5 de la LOPD. Es importante resaltar como obligatorio para cumplir con el principio de calidad representado en los mencionados artículos, recabar únicamente los datos realmente obligatorios en relación a la finalidad para la cual vayan a ser tratados, dado que, en caso contrario, si obtuviéramos datos que excedan de lo realmente necesario para el cumplimiento de la finalidad, se estaría vulnerando el principio de finalidad y de calidad de los mismos.

Por ejemplo, si se obtienen datos para la formalización de un contrato laboral, no será necesario recabar datos, por ejemplo, relacionados con hábitos de consumo de la persona que vayamos a contratar. Suele ser habitual recabar más datos de los estrictamente necesarios, dado que, por lo general, se pretende, en un porcentaje muy alto, utilizarlos con una finalidad también comercial o publicitaria. Si eso es así, y no se indica como finalidad del tratamiento la remisión de una determinada publicidad, el recabar determinados datos de hábitos de consumo excedería del principio de calidad de los mismos, dado que no serían adecuados ni pertinentes para la finalidad de mantener una relación

laboral con la persona que facilite los datos y, por tanto, no se deberían consignar como obligatorias las casillas del formulario que hagan referencia a hábitos de consumo en el contrato de trabajo. Igualmente, si se recaban datos para una finalidad principal (que incluso no requeriría el consentimiento del afectado) y para otras accesorias (publicidad), habría que indicar los datos que se obtendrán para destinarlos a dicha finalidad accesoria como no obligatorios.

"d. De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición."

Se debe informar a los afectados de la posibilidad de ejercitar dichos derechos, para facilitar que éstos los conozcan tal y como los confiere la LOPD. Se analizarán dichos derechos de los afectados, en el capítulo cuarto del presente libro.

Únicamente queremos indicar que sólo se han recogido en el contenido de la obligación de informar los de acceso, rectificación, cancelación y oposición, dejando al margen, por tanto, el derecho a impugnación de valoraciones (artículo 13 de la LOPD), el derecho de consulta al Registro General de Protección de Datos (artículo 14 de la LOPD), el procedimiento de tutela de derechos (artículo 18 de la LOPD) y el derecho de indemnización (artículo 19 de la LOPD).

"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.

En determinadas circunstancias, podría consentir un afectado el tratamiento de sus datos por un determinado responsable, y negarse a esos mismos tratamientos por parte de otro responsable distinto.

En función de la seguridad o confianza que le ofrezca un determinado responsable, podrá o no consentir el tratamiento de los datos. Resulta igualmente necesario el conocimiento de la identidad y dirección del responsable del tratamiento, dado que, ante ese responsable y ante la dirección que se le indique, podría ejercitar los derechos conferidos por la LOPD.

b. Excepción a la obligación de información

El artículo 5.3 de la LOPD establece que no será necesario informar:

- 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.

No será necesario informar si el contenido de la información se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

En función de la naturaleza de los datos, o de las circunstancias en que se recaben, podría no ser obligatorio informar de los anteriores puntos. Ahora bien, ¿a qué se refiere exactamente la norma? No queda suficientemente claro en qué supuestos se podrá prescindir de informar, acerca del contenido referido en los anteriores puntos, siendo por tanto aconsejable informar en todos los casos de todos los aspectos mencionados, dado que si el responsable estima que no es necesario en función de las circunstancias en que se recabaron, y la AEPD estimase lo contrario, seríamos sancionados.

2.2.2 Datos obtenidos de forma indirecta

a. Contenido del derecho de información

En determinados supuestos, los datos no serán recabados directamente del afectado. Por ejemplo, los datos que nos facilita una determinada empresa de selección de un candidato (no los recabamos directamente del candidato, sino de la empresa de selección que nos los remite), los que constarían en un contrato de prestación de servicios en el cual se recogen los datos de varias personas como posibles contactos para cualquier cuestión derivada del contrato, los que recibimos como cesionarios de datos, etc.

En estos supuestos, establece el punto cuarto del artículo 5.4 de la LOPD que:

> *"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."*

Por tanto, dicha obligación surge en el supuesto en que el afectado no hubiera sido informado con anterioridad y, desde el momento del registro de los datos personales. La obligación está sujeta a un plazo de tres meses, desde el registro de los datos.

Podría haberle informado, por ejemplo, el cedente de los datos (la entidad o persona que nos entregó los datos), si bien, hay que tener en cuenta que si el cedente nos garantiza que ha informado, y no lo haya hecho realmente, como efectivamente se comprometió, estaríamos incumpliendo, dado que el tratamiento de datos no sería conforme a la LOPD (por incumplimiento de

la anterior obligación). La obligación de informar en el presente supuesto corresponde a la entidad que recibe los datos, por lo que ésta no podría "relajarse" en sus obligaciones por entender que otro cumplió.

El contenido de la obligación de informar en el presente supuesto, alcanzaría a los siguientes aspectos:

- Contenido del tratamiento.
- Procedencia de los datos.
- 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.
- De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de tránsito, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

El sentido de la obligación radica en que el afectado, o interesado, debe conocer en todo momento cuáles son sus derechos, quién está tratando sus datos, para qué se tratan, de qué forma, a quién se piensan remitir los mismos, cuál es el domicilio del responsable del tratamiento ante el cual puede ejercitar los derechos que la ley le confiere, etc. Dado que el cesionario de los datos, realizará un nuevo tratamiento de datos del afectado, éste último deberá ser informado de ese nuevo vínculo que surge entre el responsable y el afectado.

La obligación de información que se analiza en el presente punto no tendría demasiado sentido en los supuestos de cesiones de datos en los que no es de aplicación ninguna de las excepciones

recogidas en el artículo 27 de la LOPD (comunicación de la primera cesión de datos). Esto es así, dado que en los supuestos en que el cedente queda obligado a comunicar la primera cesión (en cumplimiento de lo dispuesto en el artículo 27 de la LOPD), ya se recoge entre sus obligaciones informar de la finalidad del fichero cedido, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario. Al menos respecto a dichos conceptos, no debería obligarse al cesionario de los datos a informar, dado que si lo hizo el cedente en cumplimiento de lo previsto en el artículo 27 de la LOPD, no tiene sentido el volver a recoger de nuevo dicha obligación. Por el contrario, tendría todo el sentido en los supuestos en que los datos no provienen de una cesión de datos, sino que son facilitados directamente por un tercero, sin que nada sepa la persona cuyos datos van a ser facilitados al responsable.

El cumplimiento de esta obligación, en ocasiones, y atendiendo al volumen de datos que se pudieran recibir por esta vía, puede ser de una gran complejidad para el responsable que recibe los datos.

Los supuestos más habituales son:

1. Cesionarios de determinados datos de carácter personal.

Lo deseable es, desde luego, intentar que el afectado hubiera sido informado previamente. En este supuesto, la situación menos costosa y más sencilla sería tratar que el cedente, en el momento en que obtenga el consentimiento para la cesión, en caso de que fuera preciso, o bien en el momento en que fuere a informar de la primera comunicación de datos (artículo 27 LOPD), aprovechara para informar en nombre del cesionario, de los aspectos a los que viene obligado a informar éste último en el plazo de tres meses.

Se podría conseguir obtener la obligación del cedente de los datos en el contrato que pudiera existir con éste. En el mismo, se recogería el contenido de la información que debe facilitar el cedente a los afectados, con carácter previo a la cesión. Si así

fuera, el interesado ya habría sido informado con anterioridad, y no sería preciso que el cesionario informara en el plazo de tres meses desde la incorporación de los datos en el fichero de su responsabilidad.

En caso de incumplimiento de la obligación, que el cedente podría asumir vía contrato en los términos indicados, el cesionario inevitablemente estaría incumpliendo con su obligación de información en el plazo de tres meses, desde el registro de los datos, dado que la obligación, por Ley, correspondería, en este supuesto, al cesionario de los datos, todo ello sin perjuicio de la responsabilidad que se pudiera derivar para el cedente de los datos por el incumplimiento del contrato en el que asumió informar en nombre del cesionario.

Ejemplos de datos que se pudieran recibir por esta vía son:

- Empresa que adquiera una determinada base de datos a los efectos de poder realizar determinadas campañas de marketing a las personas que consten en dichos ficheros.
- Supuestos de arrendamiento de bases de datos. Se discute respecto a dicha figura si se trata de una cesión de datos o un acceso a datos por cuenta de tercero.
- Datos que recibe una sociedad de otra, a los efectos de que la primera preste un determinado servicio al afectado. Una agencia de viajes cede los datos a la compañía aérea con la que su cliente va a viajar. La compañía aérea recibiría los datos personales de un tercero (la agencia de viajes).

2. Datos facilitados en el ámbito de un contrato, de personas distintas a quien lo formaliza.

Por ejemplo, en un contrato de arrendamiento de servicios, es usual que se incorpore una cláusula en la que se indiquen las personas de contacto de las dos entidades que formalizan el contrato. Cuando se registren dichos datos, se les deberá informar del contenido recogido en el artículo 5.4 de la LOPD.

Ocurriría lo mismo en el supuesto en que, en un determinado contrato, el responsable recabase datos, no sólo de la persona que contratará con éste, sino de un tercero. Por ejemplo, al celebrar un contrato de cuenta corriente con una entidad bancaria, ésta podría recabar igualmente los datos de las personas autorizadas por el afectado en la cuenta corriente. El Banco debería informar a éstas personas autorizadas dado que, en caso contrario, desconocerían dicho tratamiento.

Al igual que en el caso anterior, dada la complejidad que puede suponer informar a estas personas, el responsable podría incorporar una cláusula por la cual traslade su obligación de información al afectado, si bien, en caso de incumplimiento, y al igual que en el supuesto anterior, el responsable estaría incurriendo en responsabilidad, dado que no habría cumplido con su obligación de información.

3. Datos que procedan de fuentes accesibles al público.

En el epígrafe 1.2.7 ya se indicaron cuáles son las fuentes accesibles al público. El tratamiento de dichos datos tiene un régimen especial, cuando se vayan a destinar a la actividad de publicidad o prospección comercial, que, como se verá en el punto siguiente, se encuentran excepcionados respecto a la obligación de información en supuestos de obtención indirecta de los datos.

b. Excepciones a la obligación de información en supuestos de obtención indirecta de los datos

No será necesario informar, según dispone el artículo 5.5 de la LOPD, en los siguientes casos:

- **Cuando una ley lo prevea expresamente.**

  Según el tenor literal de la LOPD, la ley debe prever expresamente la excepción a la obligación de información. La AEPD ha matizado dicha excepción, dado que del contenido de la Directiva transpuesta, a través de la vigente LOPD, se

desprende que el régimen de la LOPD es mucho más riguroso que el de la propia directiva.

A juicio de la AEPD, la excepción del artículo 5.5 será aplicable a supuestos en que el tratamiento o cesión de los datos de carácter personal aparezca recogido expresamente en una norma con rango de Ley. Por el contrario, no será de aplicación la excepción en aquellos supuestos en que la Ley únicamente habilite la cesión de los datos, pero sin recoger expresamente la autorización para la cesión de datos. Se trata de una interpretación acorde con la referida Directiva, razonable y beneficiosa para los responsables de tratamiento, pero claramente contraria a la interpretación literal de la LOPD.

- **Cuando el tratamiento tenga fines históricos, estadísticos o científicos.**
- **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.**

  La aplicación de dicha excepción requiere, ineludiblemente, un acto jurídico de la AEPD a través del cual se establezca la imposibilidad de informar, o que entienda que exigiría medios desproporcionados. Dicho procedimiento deberá ser instado por el responsable del tratamiento, a quien le corresponderá acreditar la existencia de la causa de exención, de acuerdo al número de interesados, antigüedad de los datos y a las posibles medidas compensatorias (publicación de la información en medios de comunicación, etc.).
- **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.

La información que se debe facilitar en estos supuestos, va precisamente encaminada a que el afectado pueda conocer en qué fuente, accesible al público, constan sus datos, dado que podría desconocerlo, para que se pueda dirigir al responsable de ésta y ejercitar sus derechos ante dicho responsable. Igualmente, para que el afectado pueda dirigirse a quien está utilizando sus datos personales para remitirle información comercial, para oponerse a dicho tratamiento.

Existe un régimen especial para quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas (artículo 30 de la LOPD). Éstos podrán utilizar nombres y direcciones u otros datos de carácter personal cuando los mismos:

- Figuren en fuentes accesibles al público.
- Hayan sido facilitados por los propios interesados u obtenidos con su consentimiento.

En el supuesto en que los datos procedan de fuentes accesibles al público, de conformidad con lo establecido en el párrafo segundo del artículo 5.5 de la LOPD, en cada comunicación que se dirija al interesado se informará:

- Del origen de los datos.
- De la identidad del responsable del tratamiento.
- De los derechos que le asisten. 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 de la LOPD.

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 todas las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

2.2.3 Información adicional en el supuesto de tratamiento de datos referentes a ideología, religión y creencias

El artículo 16.2 de la Constitución Española, establece que: "*nadie podrá ser obligado a declarar sobre su ideología, religión o creencias*".

Como consecuencia de dicha previsión, la LOPD recoge en su artículo séptimo (datos especialmente protegidos) una obligación específica respecto al derecho de información en los supuestos en que se vayan a recabar dichos datos. En concreto, establece el párrafo segundo del citado artículo que: "*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***". En el apartado 2.3.3 se analizará el consentimiento preciso para el tratamiento de los citados datos especialmente protegidos y en el 3.2 lo referente a su cesión.

2.2.4 Información de la primera cesión de datos

Se recoge en el artículo 27 de la LOPD un deber de información adicional que debe ser cumplimentado **en el momento en que se efectúe la primera cesión de datos.** El responsable, deberá informar a los afectados de la primera cesión de datos que éste vaya a realizar, debiendo indicar:

- Realización de la primera cesión de datos.
- Finalidad del fichero.
- Naturaleza de los datos que han sido cedidos.
- Nombre y dirección del cesionario.

La obligación de informar **no existirá** en los siguientes supuestos:

- 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 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.
- Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
- Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.
- Cuando la cesión venga impuesta por la Ley (no será de aplicación en los casos en que la Ley únicamente habilite la cesión para el cumplimiento de distintas obligaciones sustantivas que requieran la comunicación de los datos).

Se trata de parte de las excepciones al consentimiento para la cesión de datos que se verán en el Capítulo 3.

2.2.5 Modelo de cláusula informativa

A modo de ejemplo, sirvan las cláusulas que aparecen en las páginas siguientes como líneas generales a seguir a los efectos de informar a los afectados.

Supuesto general

De conformidad con lo recogido en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de Datos de Carácter Personal, quedo informado y consiento que los datos que voluntariamente facilite a través del presente documento *(si de la relación que surja, se van a recibir o tratar más datos, se deberá igualmente indicar. Por ejemplo: así como todos los datos e informaciones que nos facilite a durante la gestión, mantenimiento y desarrollo de la relación* _____ *(laboral, contractual, etc.)*, quedarán registrados en el fichero _____ *(introducir nombre del fichero y código de inscripción en la AEPD)* responsabilidad de _____ *(datos identificativos de la persona responsable, ya sea persona física o jurídica)*, único destinatario de los datos *(si hubiere otros destinatarios, se deberán identificar. En caso de no conocer éstos, indicar al menos las categorías de destinatarios)* con la finalidad de _____ *(indicar la finalidad o finalidades del tratamiento, no indicando finalidades incomprensibles, vagas, imprecisas, etc. Igualmente, habrá que tener en cuenta que las finalidades que no se indiquen, no podrán realizarse).*

Quedo informado de la obligatoriedad de las respuestas a las preguntas planteadas que se encuentran marcadas con un asterisco (*) en el documento *(habrá que indicar en el documento los campos obligatorios con un asterisco)*, en caso de no facilitar dichos datos, no se podrá atender mi solicitud.

Una vez facilite los datos, éstos serán tratados por el responsable anteriormente indicado, y de acuerdo a las finalidades determinadas, explícitas y legítimas que se indican en la presente cláusula.

Quedo informado que podré ejercitar los derechos de acceso, rectificación, cancelación y oposición, mediante comunicación al domicilio del responsable del tratamiento, sito en _____ *(indicar todos los datos del domicilio. Igualmente, si se hubiese habilitado un teléfono de información respecto a protección de datos, indicarlo).*

Si se produjese algún cambio en los datos personales facilitados, quedo informado de mi obligación de notificar dicho extremo al responsable, a los efectos de su correcta actualización.

Información como cesionarios de los datos en los que el afectado no hubiera sido informado con anterioridad

(supuestos en los que nos han cedido determinados datos de carácter personal. Artículo 5.4 LOPD)

De conformidad con lo recogido en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de Datos de Carácter Personal, y dentro del plazo legal conferido *(tres meses desde el registro de los datos)*, le informamos que han sido registrados sus datos de _____ (*informar contenido tratamiento)* los cuales han sido remitidos por la entidad _____ *(indicar todos los datos identificativos a los efectos de justificar la procedencia de los datos)* en el fichero _____ *(introducir nombre del fichero y código de inscripción en la AEPD)* responsabilidad de _____ *(datos identificativos de la persona responsable, ya sea persona física o jurídica),* único destinatario de los datos *(si hubiere otros destinatarios, se deberán identificar. En caso de no conocer éstos, indicar al menos las categorías de destinatarios)* con la finalidad de _____ *(indicar la finalidad o finalidades del tratamiento, no indicando finalidades incomprensibles, vagas, imprecisas, etc. Igualmente, habrá que tener en cuenta que las finalidades que no se indiquen, no podrán realizarse).*

Quedo informado que podré ejercitar los derechos de acceso, rectificación, cancelación y oposición, mediante comunicación al domicilio del responsable del tratamiento, sito en _____ *(indicar todos los datos del domicilio. Igualmente, si se hubiese habilitado un teléfono de información respecto a protección de datos, indicarlo).*

Si se produjese algún cambio en los datos personales facilitados, quedo informado de mi obligación de notificar dicho extremo al responsable, a los efectos de su correcta actualización.

Información de la primera comunicación de los datos
(artículo 27 LOPD)

De conformidad con lo recogido en el artículo 27 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de Datos de Carácter Personal, le informamos que se ha producido la primera cesión de sus datos _____ *(indicar la naturaleza de los datos que han sido cedidos)* a _____ *(indicar nombre y dirección del destinatario de los datos).* Los referidos datos constan debidamente registrados en nuestro fichero _____ *(indicar nombre y código de inscripción del fichero)* el cual tiene por finalidad _____ *(indicar las finalidades del fichero).*

Información en supuestos de remisión de publicidad si los datos se obtienen de fuentes accesibles al público
(artículos 5.5 y 30 de la LOPD)

De conformidad con lo recogido en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de Datos de Carácter Personal, le informamos que los datos personales utilizados para la realización de la presente campaña publicitaria, ha sido obtenidos de _____ *(indicar el origen de los datos).* Dichos datos han sido incorporados en un fichero, responsabilidad de _____ *(indicar los datos del responsable del tratamiento)*, pudiendo usted ejercer los derechos de acceso, rectificación, cancelación y oposición, mediante comunicación al domicilio del responsable del tratamiento, sito en _____ *(indicar todos los datos del domicilio. Igualmente, si se hubiese habilitado un teléfono de información respecto a protección de datos, indicarlo).*

2.3 Consentimiento

2.3.1 Principio general

Lo define la LOPD en su artículo 3, apartado h), como "*toda manifestación de voluntad,* ***libre, inequívoca, específica e informada,*** *mediante la que el interesado consienta el tratamiento de datos personales que le conciernen*". Se enlaza, por tanto, con el principio de información.

El Tribunal Constitucional, en su Sentencia 292/2000, de 30 de noviembre, dispuso: "*De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos*".

El principio del consentimiento, con carácter general, se encuentra regulado en el artículo 6 de la LOPD. Dicho artículo establece que el tratamiento de los datos de carácter personal **requiere el consentimiento inequívoco del afectado.** Por

tanto se trata de un principio general, que como se verá, admite ciertas excepciones.

La obligación de acreditar la existencia del consentimiento respecto a un determinado tratamiento de datos de carácter personal, corresponderá al responsable del tratamiento, por tanto, el supuesto habitual será que sea éste quien lo recabe directamente del afectado guardando justificación del mismo.

Dicha obtención directa del consentimiento podrá ser bastante compleja en los supuestos en que los datos tratados no hayan sido entregados al responsable directamente del afectado sino por un tercero. En dicho supuesto, en muchas ocasiones las entidades trasladan la obligación, tanto de informar, como de obtener el consentimiento a la persona que facilita los datos. El problema de dicha opción derivaría de un incumplimiento, por parte de la persona a la que confiamos la obligación de informar o de obtener el consentimiento. En este caso nos encontraríamos ante un claro incumplimiento de las obligaciones derivadas de la LOPD.

El principio general es el del **consentimiento inequívoco** al que se hace referencia en el artículo sexto de la LOPD, y que se analiza en este punto, no siendo de aplicación dicho consentimiento en aquellos supuestos en los que se requiera un consentimiento reforzado (tratamiento de datos especialmente protegidos).

La entidad que pretenda obtener el consentimiento para un determinado tratamiento de datos, deberá establecer los procedimientos necesarios para acreditar que dicho consentimiento existió, y que fue válido conforme a derecho, dado que en caso contrario, dicha entidad sería sancionada aunque realmente se hubiera obtenido el mismo.

Se recoge en la sentencia de la Audiencia Nacional de fecha 10 de mayo de 2007: *"por regla general, corresponde a quien realiza el tratamiento estar en condiciones de acreditar que ha obtenido el consentimiento del afectado pues, salvo las excepciones establecidas en la ley, sólo el consentimiento justifica o*

legitima el tratamiento, y a tal fin deberá arbitrar los medios necesarios para que no quepa ninguna duda de que efectivamente tal consentimiento ha sido prestado. Interpretación ésta que es la que más correctamente se acomoda a lo dispuesto, no sólo en el repetido artículo 6.1 de la LOPD, sino también en la Directiva 95/46/CE, que en su artículo 7 preceptúa que los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si el interesado ha dado su consentimiento de forma inequívoca. Para ello deberá arbitrar los medios necesarios para que no quepa ninguna duda de que efectivamente tal consentimiento ha sido prestado, es decir, que el tratamiento de datos personales ha sido consentido de modo claro y terminante".

El consentimiento tácito viene siendo admitido generalmente como inequívoco, no ocurriendo lo mismo con el presunto. Respecto a la aceptación del consentimiento tácito, y la no admisión del consentimiento presunto, la sentencia de la Audiencia Nacional de 28 de febrero de 2007 establece: "*Por lo demás, los requisitos del consentimiento se agotan en la necesidad de que éste sea 'inequívoco', es decir, que no exista duda alguna sobre la prestación de dicho consentimiento, de manera que en esta materia el legislador, mediante el artículo 6.1 de la LO de tanta cita, acude a un criterio sustantivo, esto es, nos indica que cualquiera que sea la forma que revista el consentimiento —expreso, presunto o tácito— éste ha de aparecer como evidente, inequívoco —que no admite duda o equivocación—, pues éste y no otro es el significado del adjetivo utilizado para calificar al consentimiento, de manera que el establecimiento de presunciones, como la falta de denuncia de los hechos por el afectado o las demás circunstancias a las que se alude en la demanda, equivaldría a establecer un sistema de suposiciones que pulverizaría esta exigencia esencial del consentimiento, porque dejaría de ser inequívoco para ser 'equívoco', es decir, que su interpretación admitiría varios sentidos* (...)".

Los **términos del consentimiento** general son:

Tabla 2.1. Caracteres del consentimiento.

CONSENTIMIENTO GENERAL Artículo 6.1. LOPD
LIBRE. No debe existir ningún vicio del consentimiento. El consentimiento, de acuerdo con lo previsto en el artículo 1.262 del CC se manifiesta por el concurso de la oferta y de la aceptación sobre la cosa y la causa que han de constituir el contrato, siendo nulo el consentimiento prestado por: i) *error.* Deberá recaer sobre la sustancia de la cosa que fue objeto del consentimiento, o sobre aquellas condiciones de la misma que principalmente hubiesen dado motivo a celebrarlo. Si el afectado o interesado no es informado según se ha analizado en el punto 2.2, es decir, de conformidad con lo dispuesto en el artículo 5 de la LOPD, estaríamos ante un supuesto de vicio del consentimiento producido por error y, por tanto, ante un consentimiento nulo y no válido. ii) *violencia.* Hay violencia cuando para arrancar el consentimiento se emplea una fuerza irresistible. iii) *intimidación.* Existiría intimidación cuando se inspira a uno de los contratantes el temor racional y fundado de sufrir un mal inminente y grave en su persona o bienes, o en la persona o bienes de su cónyuge, descendientes o ascendientes. iv) *dolo.* Hay dolo cuando con palabras o maniquinaciones insidiosas de parte de uno de los contratantes, es inducido el otro a celebrar un contrato que sin ellas, no hubiera hecho.
ESPECÍFICO. El consentimiento se debe obtener para una finalidad específica, explícita y legítima del responsable, no pudiéndose obtener consentimientos genéricos para finalidades ambiguas o no comprensibles para el afectado o interesado. Podríamos en ese supuesto encontrarnos de nuevo con un vicio del consentimiento, dado los datos de carácter personal únicamente se pueden someter a 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 caso contrario, estaríamos tratando los datos con una clara vulneración del principio de calidad, el cual se encuentra estrechamente ligado con esta característica del consentimiento.

CONSENTIMIENTO GENERAL
Artículo 6.1. LOPD

INFORMADO. Previamente a la obtención del consentimiento, se deberá haber informado al afectado, de conformidad con lo establecido en el artículo 5 de la LOPD. En caso contrario, nos encontraríamos de nuevo con un consentimiento nulo, dado que existiría un claro vicio de nulidad.

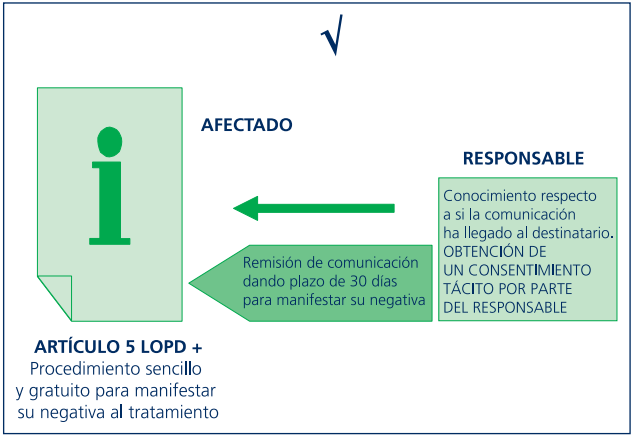
Si no se informa al afectado de las finalidades del tratamiento de datos, de la identidad del responsable, de los destinatarios de los datos, etc. difícilmente podrá consentir, o al menos, consentir con efectos jurídicos válidos.

Es por ello, por lo que el consentimiento se encuentra estrechamente ligado con el principio de información, dado que no cabe un consentimiento válido, sin que se haya informado al afectado.

INEQUÍVOCO. Debe existir necesariamente una acción u omisión del afectado que implique necesariamente la existencia del consentimiento. Por tanto, sí será posible la obtención de consentimientos tácitos, pero en ningún caso será admisible la obtención de consentimientos presuntos, entendiendo por presunto, aquel consentimiento que se deduce de determinados actos realizados por el afectado. Por tanto, si un afectado nos entrega una serie de datos y no nos denuncia por tratarlos, no podemos deducir de ese comportamiento la existencia de un consentimiento (consentimiento presunto). Ahora bien, si le indicamos un plazo para oponerse (1 mes) a un determinado tratamiento de datos, le informamos del contenido del artículo 5 de la LOPD, y en ese plazo no se opone, sí estaríamos ante un consentimiento válido (consentimiento tácito). Las fórmulas de obtención del consentimiento de forma tácita, no podrán ser aplicables a los tratamientos de datos especialmente protegidos, como se verá en el punto 2.3.3 (supuestos especiales). Ahora bien, se deberá constar la recepción de la comunicación (dado que en caso contrario, no podríamos afirmar que obtuvimos un consentimiento inequívoco) así como establecer un procedimiento sencillo para que manifieste su voluntad contraria respecto a ese tratamiento para el que solicitamos su consentimiento (envío sobre prefranqueado, teléfono gratuito, etc.).

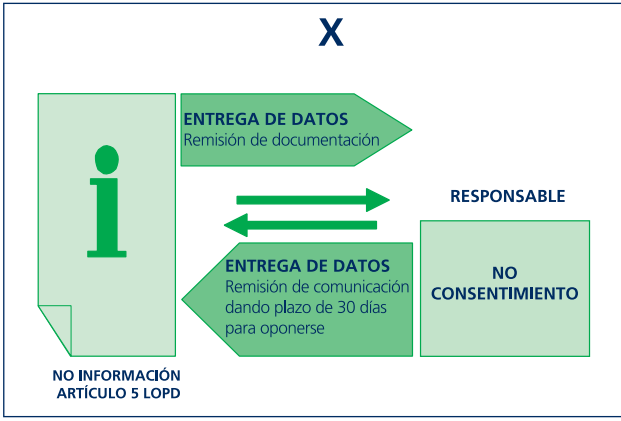
En el siguiente gráfico, se puede observar un ejemplo de obtención de consentimiento tácito válidamente obtenido por parte del responsable. Señalar que, junto con la comunicación, se debería acompañar una carta a franquear en destino o un número gratuito para que el afectado pudiera no consentir dicho tratamiento de modo sencillo y gratuitamente (o algún procedimiento similar).

Figura 2.1. Ejemplo de obtención de un consentimiento tácito.



Por el contrario, en el siguiente gráfico se observa el supuesto contrario. En este ejemplo, el responsable remite una comunicación al afectado dándole un plazo para que no acepte un determinado tratamiento de datos, pero sin informar debidamente del contenido del artículo 5 de la LOPD, así como un segundo supuesto en el que el afectado rellena un cupón sin la información del artículo 5 de la LOPD, que ha sido entregado por el responsable al afectado, con una serie de casillas para que sean completadas por éste último. El afectado completaría el cupón y se lo remitiría al responsable.

Figura 2.2. Ejemplo de no obtención de un consentimiento válido.



2.3.2 Excepciones al consentimiento

El tratamiento de datos de carácter personal sin consentimiento de los afectados supone un claro límite al derecho fundamental a la protección de datos de carácter personal, dado que uno de los fines esenciales perseguido por la norma es el garantizar el poder de disposición de los afectados respecto a los tratamientos de datos que puedan ser realizados por terceros. Sin consentimiento, el afectado puede perder el poder de disposición y conocimiento de lo que se está realizando con sus datos personales y sobre quién está tratando dichos datos.

Como garantía necesaria que debe imperar con carácter general, está que el afectado pueda consentir la recogida y almacenamiento de sus datos personales, así como conocer los usos concretos que se realizarán con los mismos. Es por ello, por lo que las excepciones que se recogen, en particular en este punto, y en general en la LOPD deben tomarse como lo que

son, excepciones a un principio general, debiendo interpretarse en caso de duda de forma favorable a los derechos e intereses de los afectados.

La carga de la prueba respecto a la aplicación de la excepción que a juicio del responsable fuera de aplicación, corresponde a éste. Si el responsable no fuera capaz de acreditar la aplicación de la excepción, o, a juicio de la AEPD, no fuese de aplicación la misma, y el responsable no hubiese obtenido el consentimiento de los afectados, éste sería sancionado por un tratamiento de datos no consentido.

El artículo 6.2 de la LOPD recoge los siguientes supuestos en los que no será preciso el consentimiento del afectado, no siendo dichas excepciones aplicables a los supuestos en que los datos que estén siendo tratados, sean datos especialmente protegidos:

- **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.**

  Dichos datos podrán ser tratados por la Administración competente únicamente para el ejercicio de las funciones legítimas que tenga atribuidas. Si la Administración requiriese el consentimiento de los afectados para tratar sus datos a los efectos de imponer una sanción administrativa, podría tener más que algún problema para el cumplimiento de sus funciones. Ahora bien, se excepciona del consentimiento, más que un determinado tipo de tratamiento de datos, o categorías de tratamientos, a la Administración en su conjunto, siempre que se circunscriba el tratamiento de los datos a sus funciones legítimas y propias, y siempre dentro del ámbito de sus competencias.

  Dicha excepción, parece *a priori* algo amplia. Podría entenderse derivada de lo recogido con carácter general en el artículo 103 de la Constitución Española que recoge que: "*La Administración pública sirve con objetividad los intereses generales y actúa de acuerdo con los principios de eficacia,*

jerarquía, descentralización, desconcentración y coordinación, con sometimiento pleno a la ley y el Derecho (…)".

- **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.**

  Si se establece una relación contractual entre las partes, es razonable que se matice el régimen del tratamiento de datos, dado que es claro que la relación jurídica que nazca del contrato o precontrato, lo será en interés de ambas partes.

  Únicamente podrán beneficiarse de esta excepción aquellos datos que sean obtenidos y tratados únicamente con la finalidad del mantenimiento o cumplimiento de la relación contractual, y no por tanto aquellos otros datos y aquellas otras finalidades que no sean **imprescindibles** para dicho mantenimiento o cumplimiento.

  El ejemplo más común sería el tratamiento de los datos de carácter personal para la remisión de información publicitaria de forma complementaria al mantenimiento de la relación contractual. Es obvio que para mantener, por ejemplo, un contrato de línea telefónica, no es necesario remitir publicidad, por lo que dicho tratamiento quedaría al margen de la excepción del consentimiento y sería, por tanto, preciso para el cumplimiento de dicha finalidad (la de remisión de publicidad).

  En aquellos supuestos en que se vayan a obtener varias categorías de datos de carácter personal, y se vayan a tratar para distintas finalidades, es importante indicar en el momento de la recogida de datos, de **forma claramente separada,** por un lado las finalidades y los datos que son necesarios para la consecución de la relación contractual, y, por otro lado, aquellos datos y aquellas finalidades que sean accesorias de la principal y que no sean imprescindibles, dando opción al afectado a consentir las finalidades accesorias o no (marcación de una casilla claramente visible y que no se encuentre

previamente marcada en el documento que se le entregue para la formalización del contrato o un procedimiento similar que permita mostrar su negativa a dichos tratamientos).

Esto ocurrirá principalmente en los contratos de adhesión, en los que, el responsable, va a tratar los datos para prestar un determinado servicio, pero, igualmente, en la cláusula de protección de datos del contrato, se recogerán una serie de tratamientos accesorios, como por ejemplo, aquellos que tengan una finalidad comercial o publicitaria.

Por tanto, para las finalidades accesorias, no imprescindibles, se deberá informar y dejar una casilla en blanco, para que, en caso de no consentir dicho tratamiento, pueda el afectado marcarla. En caso de no existir dicha casilla, se podrán establecer procedimientos alternativos por parte del responsable para dar la opción al afectado a no consentir las finalidades accesorias, no imprescindibles y que éste no desee.

De acuerdo con lo anterior, no sería necesario el consentimiento en el caso del tratamiento de datos de los proveedores de una sociedad, de los empleados, de los clientes, etc. Ahora bien, si se van a tratar datos especialmente protegidos, la excepción al consentimiento, como ya se ha adelantado, no será de aplicación a los mismos, operando únicamente para los datos que no ostenten dicha condición. Respecto al tratamiento de datos especialmente protegidos, éstos deberán tratarse según se indica en los epígrafes 2.3.4. y 3.3.

Una excepción para los responsables de ficheros privados, como la vista en el punto anterior, recogida a favor de la Administración pública, podría suponer ciertos abusos por parte de los responsables privados. Ahora bien, parecería razonable que el legislador recogiese como excepción al consentimiento, la consecución de los fines legítimos a los que venga obligado por disposición legal o contractual el responsable del fichero o tratamiento. Esta excepción podría amparar el tratamiento

de datos de personas físicas, que si bien no forman parte, en sentido estricto, de la relación jurídica, su tratamiento sería imprescindible para la satisfacción y cumplimiento de dicha relación (si se solicita a una empresa que remita un paquete a una determinada persona, la empresa de mensajería deberá tratar necesariamente los datos del destinatario, no siendo en sentido estricto parte de la relación contractual).

En último lugar, señalar que más que una excepción al consentimiento, se trataría de un consentimiento implícito en el propio consentimiento del cual se deriva la relación contractual o negocial que surgirá entre el afectado y el responsable.

- **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.**

  Como se verá más adelante, el tratamiento de datos especialmente protegidos, requiere un consentimiento expreso o expreso y por escrito en determinados casos. Dicho consentimiento se encuentra excepcionado en el artículo 7.6 de la LOPD en determinados supuestos como se verá en el punto 2.3.3 apartado c). Por tanto, la LOPD ha exceptuado del consentimiento, tanto expreso, como expreso y por escrito, en aquellos supuestos en que el tratamiento resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, siempre que se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto, así como 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.

- **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.

2.3.3 El tratamiento de datos especialmente protegidos. Consentimientos reforzados y tratamientos especiales

A los supuestos que se recojan en este punto, no les será de aplicación lo dicho respecto a la posibilidad de obtención del consentimiento tácito, ni las excepciones generales al consentimiento, recogidas en el artículo 6 de la LOPD (punto 2.3.2), ni las previstas con carácter general para las cesiones de datos del artículo 11.2 de la misma norma, dado que en la medida en que se regulan tratamientos de datos más sensibles, el legislador ha querido establecer unos requisitos más rigurosos para su tratamiento, así como una serie de excepciones al consentimiento más reducidas que las vistas para el consentimiento "general" del artículo 6 de la LOPD.

En numerosas ocasiones, podemos estar tratando datos especialmente protegidos sin ser realmente conscientes de ello. Por ejemplo, en un *curriculum vitae,* se pueden encontrar dichos datos. Lo mismo ocurre en formularios con casillas abiertas, por ejemplo, de comentarios. Es por ello, por lo que hay que extremar las cautelas en estos casos, tratando de eliminar, en la medida de lo posible, los campos abiertos, para conocer siempre la clase de datos que tratamos.

Las siguientes categorías de datos requieren de unas cautelas especiales en cuanto a la obtención del consentimiento, como norma general para su tratamiento, tratándose de un consentimiento expreso y expreso y por escrito para determinadas categorías de datos.

Los supuestos especiales en los que el consentimiento no bastará que sea el general del artículo 6 de la LOPD son los siguientes:

a. Consentimiento expreso y por escrito

Establece el punto segundo del artículo 7 de la LOPD que:

> *"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."*

A modo de ejemplo, en muchas sociedades se trataría el dato de afiliación sindical de los trabajadores. El tratamiento de dicho dato requerirá, por tanto, el consentimiento expreso y por escrito. El resto de categorías no son habituales, o, por lo menos, no deberían serlo.

b. Consentimiento expreso

Establece el punto tercero del artículo 7 de la LOPD que:

> *"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.***"

Como supuesto habitual de tratamiento de datos que requieran un consentimiento expreso por parte del responsable, se encontrarían los supuestos de reconocimientos médicos de los trabajadores, datos de minusvalías a efectos tributarios, bajas por enfermedad, así como los datos relativos a la salud de clientes, cuando los servicios que preste la sociedad tengan alguna relación (por ejemplo, una compañía de asistencia, etc.).

En estos supuestos la norma general será la de obtención del consentimiento expreso, debiendo tener el responsable las máximas cautelas en cuanto al principio de calidad, dada la sensibilidad de los datos tratados y no bastando que exista una relación contractual con el cliente, para entender que podemos tratar sus datos de salud, origen racial o vida sexual.

A modo de ejemplo, hay que señalar que la cantidad de tabaco que fuma una persona, el grado de minusvalía de un trabajador, el absentismo laboral por causas de salud, el apto y no apto para el desempeño de determinado puesto, etc. serían considerados como datos de salud.

c. Excepciones comunes tanto para los tratamientos que requieren el consentimiento expreso (2.3.3.b) y los que requieren un consentimiento por escrito y expreso (2.3.3.a)

Como no podía ser de otra forma, el legislador ha situado, por encima del derecho a la protección de datos de carácter personal, el derecho a la vida, salud e integridad física, debiendo ceder el primero en estos supuestos, en la medida en que el bien jurídico protegido por medio de los otros derechos se encuentra en un plano superior.

Con independencia de la aplicación de las siguientes excepciones, no hay que olvidar que el resto de los principios regulados por la LOPD serán de plena aplicación, debiendo por tanto el responsable informar, conforme marca el artículo 5 de la LOPD, establecer las medidas de seguridad oportunas, guardar el debido secreto respecto a los datos tratados, etc.

Como excepciones a lo dispuesto respecto a la **necesidad de contar con el consentimiento expreso y expreso y por escrito para el tratamiento de datos** especialmente protegidos anteriormente referidos, el artículo 7.6 de la LOPD establece que:

"(…) podrán ser ***objeto de tratamiento*** *los datos de carácter personal"* refiriéndose a datos referentes a ideología, afiliación sindical, religión y creencias (consentimiento expreso y por escrito) y origen racial, salud y vida sexual (consentimiento expreso) *"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.****"*

Se permite, por tanto, tratar los anteriores datos especialmente protegidos, cuando sean precisos para:

- Prevención o diagnóstico médico.
- Prestación de asistencia sanitaria.
- Tratamientos médicos.
- Gestión de servicios sanitarios.

La condición imprescindible para que sea de aplicación la excepción sería que el tratamiento se realice por un profesional sanitario o por persona sujeta asimismo a una obligación equivalente de secreto.

El tratamiento de estos datos, deberá ser igualmente de conformidad con lo dispuesto, entre otras, en la normativa de Sanidad y la Ley 41/2002, de 14 de noviembre, en la cual se recogen diferentes obligaciones (paralelas) respecto a la debida confidencialidad de la información, accesos a la historia clínica, tratamiento de la información clínica (Ley General de Sanidad, Ley Básica Reguladora de la Autonomía del Paciente y Derechos

y Obligaciones en Materia de Información y Documentación Clínica, etc.).

> *"También podrán ser* ***objeto de tratamiento*** *los datos"* de ideología, afiliación sindical, religión y creencias (consentimiento expreso y por escrito) y origen racial, a la salud y a la vida sexual (consentimiento expreso) "(…) *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.***"

En la línea de lo anterior, la Ley 41/2002 establece que los facultativos podrán llevar a cabo las intervenciones clínicas indispensables en favor de la salud del paciente, sin necesidad de contar con su consentimiento, refiriéndose dicha norma al consentimiento informado de la Ley 41/2002 y no al consentimiento de la LOPD, en los siguientes casos:

a. Cuando existe riesgo para la salud pública a causa de razones sanitarias establecidas por la Ley. En todo caso, una vez adoptadas las medidas pertinentes, de conformidad con lo establecido en la Ley Orgánica 3/1986, se comunicarán a la autoridad judicial en el plazo máximo de 24 horas siempre que dispongan el internamiento obligatorio de personas.

b. Cuando existe riesgo inmediato grave para la integridad física o psíquica del enfermo y no es posible conseguir su autorización, consultando, cuando las circunstancias lo permitan, a sus familiares o a las personas vinculadas de hecho a él.

Por otra parte, se podrá otorgar el consentimiento informado de la Ley 41/2002 por representación en los siguientes supuestos:

a. Cuando el paciente no sea capaz de tomar decisiones, a criterio del médico responsable de la asistencia, o su estado físico, o psíquico, no le permita hacerse cargo de su situación. Si el paciente carece de representante legal, el consentimiento lo

prestarán las personas vinculadas a él por razones familiares o de hecho.

b. Cuando el paciente esté incapacitado legalmente.

c. Cuando el paciente, menor de edad, no sea capaz intelectual ni emocionalmente de comprender el alcance de la intervención. En este caso, el consentimiento lo dará el representante legal del menor después de haber escuchado su opinión si tiene doce años cumplidos. Cuando se trate de menores no incapaces ni incapacitados, pero emancipados o con dieciséis años cumplidos, no cabe prestar el consentimiento por representación. Sin embargo, en caso de actuación de grave riesgo, según el criterio del facultativo, los padres serán informados y su opinión será tenida en cuenta para la toma de la decisión correspondiente.

Igualmente, el artículo 8 de la LOPD establece, **respecto a los datos de salud,** que:

> *"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."*

d. Excepción únicamente aplicable para los tratamientos que requieren el consentimiento expreso (apartado b)

Como ya se ha indicado, el punto tercero del artículo 7 de la LOPD establece que:

> *"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.***"

Como excepción al principio general, que sería el de la obtención del consentimiento expreso para el tratamiento de los datos de origen racial, salud y vida sexual, se encuentra la existencia de una habilitación legal que ampare dicho tratamiento. Esta previsión no se recoge para el tratamiento de los datos que requieren un consentimiento expreso y por escrito (ideología, afiliación sindical, religión y creencias).

A modo de ejemplo, una compañía aseguradora que opere en el ramo de la responsabilidad civil, podrá tratar los datos de salud de los perjudicados en siniestros amparados por la póliza, sin necesidad de consentimiento, de conformidad con la LOSSP y TRLSCVM (se trataría de un supuesto amparado por Ley).

Igualmente entrarían en dicha excepción aquellos supuestos de reconocimientos médicos obligatorios de conformidad con lo establecido en el artículo 22 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.

e. Prohibición absoluta

El punto cuarto del artículo 7 de la LOPD prohíbe los ficheros que sean 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.

En atención al sentido literal, los ficheros con finalidades mixtas, no quedarían amparados por dicha prohibición debiendo valorarse la pertinencia de las mismas, de acuerdo a los principios ya vistos respecto a la calidad de los datos tratados.

f. Tratamientos especiales

Dispone el punto quinto del artículo 7 de la LOPD:

"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."

2.3.4 El consentimiento de los menores de edad

Cuestión tratada por la AEPD en su informe jurídico número 2000-0000 (www.agpd.es) en el cual, se concluye: "(…) *En consecuencia, a tenor de las normas referidas, cabe considerar que los mayores de catorce años disponen de las condiciones de madurez precisas para consentir, por sí mismo, el tratamiento automatizado de sus datos de carácter personal.*

Respecto de los restantes menores de edad, no puede ofrecerse una solución claramente favorable a la posibilidad de que por los mismos pueda prestarse el consentimiento al tratamiento, por lo que la referencia deberá buscarse en el artículo 162 1º del Código Civil, tomando en cuenta, fundamentalmente, sus condiciones de madurez.

En consecuencia, a la vista de lo anteriormente señalado, será necesario recabar el consentimiento de los menores para la recogida de sus datos, con expresa información de la totalidad de los extremos contenidos en el artículo 5.1 de la Ley, recabándose, en caso de menores de catorce años cuyas condiciones de madurez no garanticen la plena comprensión por los mismos del consentimiento prestado, el consentimiento de sus representantes legales".

Igual fundamentación se puede encontrar en la Resolución de archivo de actuaciones correspondiente al expediente Expediente Nº: E/00182/2005 (www.agpd.es).

Si el consentimiento lo otorga los representantes legales del menor, de conformidad con lo anterior, habrá que verificar la edad del menor así como la representación de los anteriores y la autenticidad de su consentimiento.

La información que en cualquier caso se dirija a los menores, deberá cumplir los caracteres indicados con carácter general en el artículo 5 de la LOPD, pero adaptada en este caso a la circunstancia de que quien la debe comprender es un menor.

2.3.5 Revocación del consentimiento

El artículo 6 de la LOPD establece, con carácter general, que el consentimiento puede ser revocado cuando exista causa justificada

para ello y no se le atribuyan efectos retroactivos. El supuesto más razonable, debía ser que cuando alguien, de forma libre, informada, específica e inequívoca emite una voluntad de aceptación de un determinado tratamiento de datos por parte de un específico responsable, pueda, del mismo modo, revocar dicho consentimiento sin necesidad de alegar una determinada causa para dicha revocación. El medio para la revocación del consentimiento deberá ser sencillo y que no implique un ingreso adicional al responsable ni un coste adicional a los interesados (números de tarificación adicional, obligación de utilización de cartas certificadas burofax con acuse de recibo y certificación de texto, etc.).

La mención a la causa justificada, tiene su sentido atendiendo a determinadas relaciones aceptadas por un determinado afectado, que, por ejemplo, estén sujetas a un determinado plazo. Por ejemplo, una relación contractual válida, no parece razonable que pueda extinguirse por la sola voluntad del afectado, invocando su derecho a revocar el consentimiento previamente otorgado, dado, que si así fuera, se estaría dejando el contrato al arbitrio de una de las partes de la relación jurídica dejando sin efecto, por tanto, el plazo que se hubiere pactado para esa relación jurídica, así como las causas válidas y aceptadas de resolución del contrato.

A su vez, el artículo 11.4 de la LOPD recoge que el consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable. Ahora bien, en este concreto precepto, no se realiza la mención a "causa justificada para ello".

El artículo 30.4 de la LOPD, en lo que respecta al tratamiento de datos con fines de publicidad y de prospección comercial recoge, igualmente, que 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.

Respecto a los datos que se estuvieran tratando con carácter previo a la revocación del consentimiento, deberán bloquearse conforme establece el artículo 16.3 de la LOPD.

Tabla 2.2. Tratamiento de datos especificamente protegidos (artículo 7 LOPD).

Consentimiento expreso y por escrito	**Ideología** **Afiliación sindical** **Religión** **Creencias**	Se deberá advertir necesariamente, además de lo establecido con carácter general para todos los tratamientos, que no tiene obligación de prestar su consentimiento, dado que nadie puede ser obligado a declarar sobre su ideología, religión o creencias.	**Se exceptúan** los ficheros mantenidos por 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.	Podrán ser objeto de tratamiento cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, 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 cuando 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.	No aplicación de las excepciones al consentimiento recogidas en el artículo 6 de la LOPD (punto 2.3.2.) y para la cesión de los mismos, no serán de aplicación las excepciones del 11.2 LOPD.
Consentimiento expreso y/o disposición legal	**Origen racial** **Salud** **Vida sexual**				
Prohibición	**Ideología** **Afiliación sindical** **Religión** **Creencias** **Origen racial o étnico** **Vida sexual**	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.			
Ficheros reservado	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.				

2.3.6 Campañas comerciales a través de medios electrónicos. Consentimiento expreso

Se recoge, como punto independiente, dado que la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI) recoge una serie de obligaciones en supuestos de remisión de información comercial o publicitaria a través de correo electrónico.

En concreto, el artículo 21 establece la prohibición de remisión de comunicaciones publicitarias o promocionales por correo electrónico o cualquier otro medio de comunicación electrónica equivalente, que no haya sido solicitada o expresamente autorizada por los destinatarios de las mismas.

Por tanto, supone un tipo de consentimiento distinto a los recogidos en la LOPD, dado que, en principio, los datos que se utilizarían para la realización de la campaña, en concreto, el correo electrónico, no se encontraría dentro de los supuestos de datos especialmente protegidos. Por tanto, bastaría para tratar dichos datos y para la realización de la finalidad de remisión de publicidad vía correo electrónico un consentimiento inequívoco al que se hace referencia con carácter general en el artículo 6 de la LOPD.

Pues bien, la LSSI viene a modificar, de forma discutible dada la menor jerarquía normativa de la LSSI frente a la LOPD, el régimen general establecido de consentimiento (inequívoco, expreso y expreso por escrito), incorporándose a través de la LSSI el consentimiento expreso para la remisión de publicidad por medios electrónicos.

Existe una excepción al régimen indicado que viene recogida en el punto segundo del artículo 21 al establecer: "*Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario*

y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente".

En estos supuestos se deberá ofrecer siempre al destinatario de la publicidad a través de medios electrónicos, la posibilidad de oponerse al tratamiento de sus datos con fines promocionales, mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija. Con independencia de lo anterior, habría que obtener el consentimiento general regulado por la LOPD para la remisión de dicha información publicitaria.

2.3.7 Modelo de cláusula de obtención del consentimiento

Supuesto general

De conformidad con lo recogido en el artículo 5 y 6 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de Datos de Carácter Personal, quedo informado y consiento, que los datos que voluntariamente facilite a través del presente documento *(si de la relación que surja, se van a recibir o tratar más datos, se deberá igualmente indicar. Por ejemplo: así como todos los datos e informaciones que nos facilite durante la gestión, mantenimiento y desarrollo de la relación* _____ *(laboral, contractual, etc))*, quedarán registrados en el fichero _____ *(introducir nombre del fichero y código de inscripción en la AEPD)* responsabilidad de _____ *(datos identificativos de la persona responsable, ya sea persona física o jurídica)*, único destinatario de los datos *(si hubiere otros destinatarios, se deberán identificar. En caso de no conocer éstos, se deben indicar al menos las categorías de destinatarios)* con la finalidad de _____ *(indicar la finalidad o finalidades del tratamiento, no indicando finalidades incomprensibles, vagas, imprecisas, etc. Igualmente, habrá que tener en cuenta que las finalidades que no se indiquen, no*

Continúa

podrán realizarse. Si se van a tratar los datos para finalidades accesorias, que no sean imprescindibles, se deberá informar de esas finalidades, recogiendo una casilla sin marcar para que el afectado pueda aceptar o no dichas finalidades accesorias).

Quedo informado de la obligatoriedad de las respuestas a las preguntas planteadas que se encuentran marcadas con un asterisco (*) en el documento *(habrá que indicar en el documento los campos obligatorios con un asterisco)*, en caso de no facilitar dichos datos, no se podrá atender mi solicitud.

Una vez facilite los datos, éstos serán tratados por el responsable anteriormente indicado, y de acuerdo a las finalidades determinadas, explícitas y legítimas que se indican en la presente cláusula.

Quedo informado que podré ejercitar los derechos de acceso, rectificación, cancelación y oposición, ante el domicilio del responsable del tratamiento, sito en _____ *(indicar todos los datos del domicilio. Igualmente, si se hubiese habilitado un teléfono de información respecto a protección de datos, indicarlo).*

Si se produjese algún cambio en los datos personales facilitados, quedo informado de mi obligación de notificar dicho extremo al responsable, a los efectos de su correcta actualización.

Con la firma del presente documento, y su remisión a _____ autorizo de forma expresa los anteriores tratamientos de datos indicados en la anterior cláusula de protección de datos de carácter personal.

Supuesto consentimiento tácito

(no válido cuando el consentimiento requerido sea expreso o expreso y por escrito)

De conformidad con lo recogido en el artículo 5 y 6 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de Datos de Carácter Personal, queda informado que sus datos

Continúa

identificativos (nombre y apellidos, teléfono y dirección) que constan actualmente registrados en el fichero _____ *(introducir nombre del fichero y código de inscripción en la AEPD)* responsabilidad de _____ *(datos identificativos de la persona responsable, ya sea persona física o jurídica)*, único destinatario de los datos *(si hubiere otros destinatarios, se deberán identificar. En caso de no conocer éstos, se deben indicar al menos las categorías de destinatarios)* con la finalidad de _____ *(indicar la finalidad o finalidades del tratamiento, no indicando finalidades incomprensibles, vagas, imprecisas, etc. Igualmente, habrá que tener en cuenta que las finalidades que no se indiquen, no podrán realizarse)* serán tratados igualmente por esta entidad con la finalidad de _____ *(indicar nueva finalidad del tratamiento. Por lo general, será una finalidad comercial),* incorporándose al fichero _____ *(indicar nuevo fichero en el que se tratarán los datos. Por ejemplo, marketing)*, igualmente responsabilidad de _____, única destinataria de los datos, salvo que en el plazo de treinta días desde la recepción de la presente comunicación usted no nos manifieste su negativa a dicho nuevo tratamiento *(debemos verificar que la comunicación ha llegado a su destinatario)*. En caso de no comunicarnos su negativa, se entenderá que usted consiente el tratamiento de sus datos personales con la nueva finalidad indicada en la presente cláusula. Podrá mostrar su negativa al tratamiento, introduciendo la presente comunicación en el envío prefranqueado que se acompaña a la presente comunicación *(o número de teléfono gratuito, etc.).*

Si se produjese algún cambio en los datos personales facilitados, quedo informado de mi obligación de notificar dicho extremo al responsable, a los efectos de su correcta actualización.

Quedo informado que podré ejercitar los derechos de acceso, rectificación, cancelación y oposición, ante el domicilio del responsable del tratamiento, sito en _____ *(indicar todos los datos del domicilio. Igualmente, si se hubiese habilitado un teléfono de información respecto a protección de datos, indicarlo).*

La no autorización del anterior tratamiento no le ocasionará ningún perjuicio.

2.4 Seguridad

En el artículo 9 de la LOPD se recoge:

> *"1. El **responsable** del fichero y, en su caso, el **encargado** del tratamiento, deberán adoptar las medidas de índole técnica y organizativa 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."*

De ellos se extrae una primera conclusión importante: las medidas de seguridad van dirigidas tanto para el **responsable** del fichero como para el **encargado** del tratamiento.

Las medidas de seguridad deben ir encaminadas a garantizar la seguridad de los datos. Dicho fin únicamente se podrá conseguir implantando una serie de medidas que permitan mantener la confidencialidad de la información, en el bien entendido que la pérdida de confidencialidad se puede producir por intervención de un tercero o por cualquier causa ajena. Sirva como ejemplo la pérdida de confidencialidad de los datos almacenados en un servidor de una compañía que los haga accesibles a cualquier persona que acceda a una página Web.

El punto segundo del artículo noveno de la LOPD, establece:

> *"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."*

Se trata, como se puede observar, de una condición imprescindible y previa a la incorporación de los datos de carácter personal en los ficheros del responsable.

Las medidas de seguridad que deben ser implementadas por el responsable y/o por el encargado del tratamiento, actualmente se encuentran desarrolladas 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.** Dicha norma que desarrollaba la antigua LORTAD se encuentra aún vigente, en la medida en que no se oponga a la actual LOPD.

El principio general establecido en el citado artículo 9 de la LOPD requería un desarrollo reglamentario, que sirviese como marco de referencia y como guía para implementar un nivel de seguridad adecuado y estándar para todos aquellos que intervengan en el tratamiento de datos, ya sea en calidad de responsables o encargados del tratamiento.

En la exposición de motivos del mencionado Real Decreto, se dice: "*las medidas de seguridad que se establecen se configuran como las básicas de seguridad que han de cumplir todos los ficheros que contengan datos de carácter personal…*". Por tanto, supone un paso importante para poder garantizar la seguridad de los datos de carácter personal, aportando así seguridad jurídica en el tráfico mercantil y en el tratamiento de los datos de carácter personal.

Actualmente, está en fase de elaboración un nuevo Reglamento que sustituirá al citado Real Decreto, dado que éste requiere, al menos, ser adaptado a los tratamientos de datos no automatizados. Hay que indicar que cuando se aprobó el Real Decreto 994/1999, únicamente se encontraban regulados los tratamientos automatizados de datos de carácter personal a través de la LORTAD. Es por ello por lo que el artículo primero del Reglamento, recoge como objetivo de la norma el texto que se destaca en la siguiente página.

"establecer las medidas de índole técnica y organizativa necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal sujetos al régimen de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal."

Todas las referencias recogidas en el Real Decreto son relativas al tratamiento automatizado de datos de carácter personal, quedando, por tanto, fuera del objeto de la norma su tratamiento no automatizado, a los que se aplicaría, con carácter general, al menos lo dispuesto en el citado artículo noveno de la LOPD.

Ahora bien, con independencia de que el objeto del citado Real Decreto se encuentre ligado al tratamiento automatizado de datos de carácter personal, hay que tener en cuenta que las medidas de seguridad que puedan, por su naturaleza, ser aplicadas igualmente a tratamientos no automatizados de datos de carácter personal, se deberán aplicar, dado que hay que entender que se trata de una medida que garantizaría, como se establece en el artículo 9 de la LOPD, la seguridad de los datos de carácter personal, evitando su alteración, pérdida, tratamiento o acceso no autorizado. Lo que en ningún caso parece razonable, es entender que no se deba aplicar ninguna medida de seguridad a los tratamientos no automatizados, dado que el Real Decreto 994/1999 únicamente hace referencia a los tratamientos automatizados, y dado que no existe actualmente un desarrollo reglamentario de la LOPD que regule las medidas de seguridad para los ficheros no automatizados. Si así fuera, se estaría claramente incumpliendo la previsión legal del artículo 9 de la LOPD y el espíritu de la norma.

Del contenido del Real Decreto 994/1999, se desprende una clasificación de cuatro niveles de seguridad (básico, medio, medio atenuado y alto). Dichos niveles de seguridad se deberán aplicar

en función de la tipología de datos que vayan a ser tratados, ya sea por el responsable, o por el encargado del tratamiento. En función de la naturaleza de la información tratada, y de su sensibilidad, se aplicará un nivel u otro. Debe tenerse en cuenta que las medidas de seguridad que corresponden a cada nivel de seguridad, deben entenderse como una obligación de mínimos exigibles.

A los ficheros temporales se les deberá aplicar el nivel de seguridad siguiendo los mismos criterios de determinación que a los ficheros no temporales. Dichos ficheros temporales deberán borrarse una vez que hayan dejado de ser necesarios, de acuerdo a las finalidades que motivaron la creación de dicho fichero.

La regulación de las medidas de seguridad, se encuentra en los artículos 8 a 26 del Real Decreto 994/1999.

Se deberán aplicar los siguientes niveles de seguridad a los tipos de datos que se indican a continuación:

- **Nivel de seguridad básico:**
  - Todos los ficheros que contengan datos de carácter personal.
- **Nivel de seguridad básico y medio:**
  - Ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda pública, servicios financieros.
  - Ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito.
- **Nivel de seguridad básico, medio y alto:**
  - Ficheros que contengan datos de: ideología, religión, creencias, origen racial, salud, vida sexual, ficheros que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas.
- **Nivel de seguridad básico y medio atenuado:**
  - Se aplicarán los citados niveles de seguridad a los ficheros que contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo.

2.4.1 Medidas de seguridad de nivel básico

Documento de seguridad

Se deberá implementar y elaborar un documento, el cual será de obligado cumplimiento para el personal que tenga acceso a los datos automatizados o a los sistemas de información. El documento de seguridad deberá encontrarse en todo momento actualizado, debiéndose, siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo, revisar y actualizar. Dicho documento, deberá adecuarse en todo momento a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

El contenido mínimo del documento será el siguiente:

a. Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b. Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.

c. Funciones y obligaciones del personal.

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.

A través de la página web de la AEPD (www.agpd.es) se puede obtener un modelo de documento de seguridad.

Funciones y obligaciones del personal

Se deben definir y documentar las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información. Con independencia de lo anterior, todo el personal debe conocer las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias de su incumplimiento.

El responsable del fichero deberá establecer los procedimientos adecuados para el cumplimiento de lo anterior.

Sería aconsejable que, junto al contrato de trabajo, se entregara a los trabajadores la documentación a la que se hace referencia en el presente artículo, así como que firmase un recibí de dicha información.

Registro de incidencias

Se debe establecer un procedimiento de notificación y gestión de incidencias. Dicho procedimiento deberá contener, al menos:

- Tipo de incidencia.
- Momento en que se produjo la incidencia y persona que realiza la notificación, a quién se le comunica así como los efectos que se hubieran derivado de la misma.

Identificación y autenticación

Deberá existir una relación actualizada de los usuarios que tengan acceso al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso. Si el mecanismo de autenticación se basa en la existencia de contraseñas, debe existir un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

Las contraseñas se deben cambiar con la periodicidad que se determine en el documento de seguridad y mientras estén vigentes se almacenarán de forma ininteligible.

Control de acceso

Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

Se deberán establecer mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.

La relación de usuarios con acceso autorizado al sistema de información deberá contener el acceso autorizado para cada uno de ellos.

Únicamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el responsable del fichero.

Gestión de soportes

Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad.

La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero, únicamente podrá ser autorizada por el responsable del fichero.

Copias de respaldo y recuperación

Se deberá verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos. Las copias deberán realizarse, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberán garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

2.4.2 Medidas de seguridad de nivel medio

Documento de seguridad

Además de lo indicado, al reseñar las medidas de seguridad correspondientes al nivel básico, el documento de seguridad deberá contener:

- 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.

- Las medidas que sea necesario 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. Esta designación no supone una delegación de la responsabilidad, dado que ésta corresponde al responsable del fichero.

Auditoría

Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento de las obligaciones contenidas en el Real Decreto 994/1999, así como 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 citado Real Decreto, 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 debe establecer 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.

Se debe limitar 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 conocer, directa o indirectamente, 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 deberá disponer de un sistema de registro de salida de soportes informáticos que permita conocer:

- El tipo de soporte.
- La fecha y hora de salida del soporte.
- El destinatario y el número de soportes.
- El tipo de información que contienen los soportes, 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

El registro de incidencias recogido en las medidas de seguridad correspondientes al nivel básico regulado se debe consignar, además de lo allí referido, los procedimientos realizados de recuperación

de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, aquellos datos que haya 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.

2.4.3 Medidas de seguridad de nivel medio atenuado

Las medidas de nivel medio atenuado serán, además de las recogidas en el nivel básico, que, como ya se dijo, son de aplicación a todos los ficheros que contengan datos de carácter personal, las siguientes, que corresponden al nivel medio:

- Auditoría.
- Identificación y autenticación.
- Control de acceso físico.
- Gestión de soportes

2.4.4 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 permita 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 período 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 aquél 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.

2.4.5 Medidas comunes

Accesos a datos a través de redes de comunicaciones

Las medidas de seguridad en el presente supuesto deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

Régimen de trabajo fuera de los locales de la ubicación del fichero

En este supuesto, se deberá contar con la autorización expresa del responsable del fichero y, en todo caso, se deberá garantizar el nivel de seguridad correspondiente al tipo de fichero tratado.

Tabla 2.3. Niveles de seguridad.

	Básico	Medio	Medio atenuado	Alto
Documento de seguridad (contenido mínimo).	X			
Documento de seguridad (contenido avanzado). Indicación del responsable/s de seguridad, controles periódicos y medidas en caso de desecho de soportes o reutilización de éstos.		X		
Funciones y obligaciones del personal.	X			
Registro de incidencias.	X			
Identificación y autenticación (contenido mínimo).	X			
Identificación y autenticación (contenido avanzado). Sistemas que permitan la identificación de todo usuario que intente acceder al sistema de información y verificación de que está autorizado. Limitación de intentos reiterados de accesos al sistema de información.		X	X	
Control de acceso.	X			
Gestión de soportes (contenido mínimo).	X			
Gestión de soportes (contenido avanzado).		X	X	
Copias de respaldo y recuperación.	X			
Responsable de seguridad.		X		
Auditoría.		X	X	
Control de acceso físico.		X	X	
Registro de incidencias.		X		
Pruebas con datos reales.		X		
Distribución de soportes.				X
Registro de accesos.				X
Copias de respaldo y recuperación.				X
Telecomunicaciones.				X
Acceso a datos a través de redes de comunicaciones.	X			
Régimen de trabajo fuera de los locales de la ubicación del fichero.	X			
Ficheros temporales.	X			

2.5 Deber de secreto

2.5.1 Aspectos generales

Se establece en el artículo 10 de la LOPD: "*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*".

La obligación de guardar secreto se aplica por tanto a cualquier persona o entidad que intervenga en el tratamiento de los datos. Desde quien recoge los datos, los manipula, los remite a un tercero, etc. Todo el personal de una empresa deberá, por tanto, comprometerse a mantener y respetar dicha obligación de confidencialidad y secreto profesional. Dicha obligación, como se indica, deberá mantenerse incluso una vez que se hubiera extinguido la relación con el responsable del fichero, dado que en caso contrario, se trataría de una obligación carente de contenido, bastando el cese en la relación laboral, para la ruptura de la obligación de secreto.

Cualquier trabajador de una empresa, en la medida en que intervenga, de cualquier forma, en el tratamiento de los datos, deberá quedar vinculado con la empresa, incluso una vez hubiera dejado de trabajar para dicho responsable. Por ello, a los efectos de garantizar el cumplimiento de dicha obligación, y para que el trabajador tenga presente la importancia que tiene el tratar los datos personales que sean responsabilidad de la empresa para la cual desempeñan sus funciones, se le debe entregar un

compromiso de confidencialidad que garantice el cumplimiento de esta obligación.

La obligación de secreto está, como no podría ser de otra manera, estrechamente ligada con la regulación de la cesión de datos, ya que es habitual, que un incumplimiento de la obligación de confidencialidad, a la postre supondrá una cesión no consentida de los datos personales. Es por ello por lo que la causa y el efecto de la falta de deber de secreto será una comunicación de datos no consentida. Como se verá con más detenimiento en el capítulo tercero, cesión de datos es toda revelación de información realizada a una persona distinta del interesado, pudiendo realizarse siempre y cuando sea para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario y se cuente con el consentimiento del interesado, salvo que sea de aplicación, alguna de las excepciones al consentimiento para la cesión de datos del artículo 11.2 o que la cesión se efectúe previamente al procedimiento de disociación.

Estaremos ante un incumplimiento de lo dispuesto en el artículo 11 de la LOPD (cesiones de datos) y no del 10 (deber de secreto) cuando la vulneración del deber de secreto suponga una conducta cualificada en la comunicación de los datos, cual es que la misma tenga por finalidad el que los datos personales vayan a ser tratados por el cesionario, como se indica en la Memoria de la Agencia Española de Protección de Datos correspondiente al año 2005.

Igualmente, en la Resolución: R/00880/2005 correspondiente al Procedimiento Nº PS/00156/2005 (www.agpd.es), se recoge la anterior conclusión respecto a la distinción del incumplimiento del deber de secreto respecto a la comunicación de datos no consentida, estableciéndose: "*Debe compararse el texto de los artículos 10 y 11 de la LOPD, que definen, respectivamente, los deberes de secreto profesional respecto de los datos de carácter personal que integran el fichero y la prohibición de comunicación*

de dichos datos, salvo en los supuestos expresamente previstos, pues la trasgresión de cualquiera de dichas garantías por parte de quien se responsabiliza del fichero supone, desde un punto de vista meramente fáctico, una conducta semejante, la comunicación de la información que se contiene en el fichero. Así, la distinción entre ambos tipos de garantías exige que la cesión suponga un comportamiento cualificado de la comunicación de datos, cualificación que no puede ser otra que la voluntad de que los datos sirvan para ser tratados por parte del cesionario, circunstancia que concurre en este caso, por lo que la comunicación acontecida debe encuadrarse dentro del marco de la cesión de datos".

Se incumplirá el deber de confidencialidad si se notificase, por ejemplo, algún dato de carácter personal tratado por determinado responsable a un familiar del afectado, como dejar un recado a un familiar respecto a alguna deuda que tenga contraída el afectado con el responsable, entregar una determinada comunicación a un tercero distinto del interesado o afectado, entregar a una persona distinta del destinatario un sobre con el membrete de un determinado área hospitalaria, etc.

2.5.2 Modelo de cláusula de confidencialidad

Se deberán incorporar las cláusulas de confidencialidad en los contratos con el personal de la empresa que vayan a tener acceso a los datos personales objeto de tratamiento, así como respecto a los empleados que presten servicios para la entidad y que tengan acceso a datos personales de la empresa. Respecto a este caso, en el contrato de acceso a datos de carácter personal, se debería incluir una cláusula en virtud de la cual la entidad encargada del tratamiento de datos mantiene respecto de sus empleados que vayan a acceder a los datos de carácter personal de la empresa un compromiso de confidencialidad que vincule al encargado del tratamiento con sus trabajadores.

Modelo de cláusula de confidencialidad

El trabajador declara ser plenamente consciente de la importancia que tiene el tratamiento de datos de carácter personal de las personas físicas, tratándose de un derecho de relevancia constitucional, que goza de una especial protección, entre otras normas, a través de la Constitución Española, la Ley Orgánica 15/1999, de 13 de diciembre, de protección de Datos de Carácter Personal, así como por lo dispuesto por el Código Penal.

El trabajador, en la medida en que durante la relación laboral intervenga en cualquier fase del tratamiento de datos de carácter personal, así como respecto a los datos de carácter personal que pudiera conocer, ya sea de forma directa o indirecta, y con independencia del soporte o modo de acceso a dichos datos, queda obligado al secreto profesional y al deber de guardarlos, subsistiendo las anteriores obligaciones, aun después de finalizar sus relaciones con la empresa.

El Trabajador, mediante la firma del presente documento, acepta y asume de forma expresa, las anteriores obligaciones.

Nombre
DNI
Firma

2.6 Inscripción registral

Es en el artículo 14 de la LOPD dónde se recoge el derecho que tiene cualquier persona, a conocer la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento, a través de la consulta al Registro General de Protección de Datos, siendo dicha consulta gratuita.

Con carácter previo a la creación de ficheros con datos de carácter personal, se deberá notificar tal circunstancia a la AEPD. La obligación de notificar recaerá en las personas físicas

o jurídicas, de naturaleza pública o privada, u órgano administrativo, que fueran a crear un fichero que contenga datos de carácter personal. Existe una salvedad respecto a los ficheros manuales (no automatizados) que ya existieran antes de la entrada en vigor de la LOPD. En este supuesto, no será necesaria su notificación para su inscripción hasta octubre de 2007, de conformidad con lo establecido en el último párrafo de la Disposición Adicional Primera de la LOPD.

Lo que debe ser objeto de notificarse no es el contenido íntegro del fichero, junto con los datos personales que consten en éste, sino una serie de circunstancias relativas al tratamiento de datos que se realizará (encargados del tratamiento, cesiones, ubicación del fichero, etc.), así como las modificaciones posteriores respecto al contenido de la inscripción.

Entre las funciones de la AEPD, se recoge en el artículo 37, apartado j), el "*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*". Por tanto una de las notas principales de la finalidad de la inscripción registral radica en dar publicidad a la existencia de ficheros. Actualmente, a través de la página Web de la AEPD se pueden consultar los ficheros inscritos por los responsables de los mismos.

Las inscripciones se realizan a través del sistema de **NO**tificaciones **T**elemáticas a la **A**EPD (NOTA), aprobado mediante Resolución de la Agencia Española de Protección de Datos de 12 de julio de 2006, pudiéndose descargar dicho formulario a través de la página Web de la AEPD.

Comunicaciones de datos a terceros

3.1 Supuesto general

Se entiende por cesión o comunicación de datos, según se establece en el artículo tercero, letra i) de la LOPD, "*toda revelación de datos realizada a una persona distinta del interesado*".

Esta definición debe completarse con lo que se recoge en el artículo 1.2 del RD 1332/1994 de 20 de junio. En dicho artículo, se define cesión de datos como "*toda obtención de datos resultante de la consulta a un fichero, la publicación de los datos contenidos en el fichero, su interconexión con otros ficheros y la comunicación de datos realizada por una persona distinta de la afectada*".

Por su parte, la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, en su artículo 2.b), precisa el concepto de cesión de datos, como comunicación por transmisión, difusión, o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión.

Se trata de una definición amplísima. Cualquier revelación de datos que se haga a un tercero, con independencia del modo o soporte en que se realice, será considerada como cesión de datos. Es importante indicar que quedan a salvo de lo anterior aquellos supuestos en que los que lo que se produzca no sea una cesión de datos, sino un acceso a datos por cuenta de tercero (se analizará dicha figura en el capítulo cuarto).

La norma general será la de prohibición de cesión o comunicación de los datos a un tercero, salvo en aquello supuestos contemplados por la Ley (consentimiento, habilitación legal, etc.).

Es necesario para que se pueda proceder a realizar una cesión de datos de carácter personal, de conformidad con lo establecido en los artículos 11 de la LOPD:

En primer lugar, y por obvio que pueda parecer, será necesario que tengamos una **habilitación que nos permita tratar los datos que pretendemos ceder,** en los términos analizados en el punto 2.3 (consentimiento).

Si no tenemos habilitación legal para tratar determinados datos de carácter personal, difícilmente podremos comunicárselos legítimamente a un tercero. Como norma general, la ilicitud del tratamiento realizado por el cedente de los datos, se extenderá al tratamiento que fuera a realizar el cesionario.

En segundo lugar, será necesario que la cesión de datos que se vaya a producir sea únicamente para para el **cumplimiento de fines directamente relacionados con las funciones legítimas** del cedente y del cesionario (quien recibe los datos).

Por ejemplo, si el cliente de una determinada empresa ha contratado con ésta un viaje combinado, entraría dentro del concepto funciones legítimas tanto del cedente como del cesionario que dicha empresa pudiera remitir los datos a la cadena hotelera donde el cliente se va a alojar, o a la compañía aérea con la que volará, con las finalidades de la gestión de las respectivas reservas y contrataciones.

Es por ello por lo que, en cumplimiento de lo recogido en este punto, no estaremos habilitados a comunicar los datos a un tercero en cualquier circunstancia y con independencia de que contemos con el consentimiento de los afectados.

Se deberá facilitar, con carácter previo a la obtención del consentimiento para la cesión de los datos, **información** acerca de la **finalidad** a que destinarán los datos cuya comunicación se autoriza **y** el **tipo de actividad** de aquel a quien se pretende comunicar.

En caso contrario, el consentimiento sería nulo por disposición legal, dado que así queda expresado en el punto tercero del artículo 11.3 de la LOPD. La información al afectado respecto a la finalidad y el tipo de actividad, deberá ser determinada y explícita, de modo que le permitan prestar un consentimiento inequívoco (para supuestos de tratamientos de datos que no sean especialmente protegidos) como el exigido con carácter general por la LOPD, no siendo válidas finalidades muy genéricas e indeterminadas e indicaciones a título indicativo y no definitivo. Respecto a la información acerca de la finalidad, me remito a lo dicho en el punto 2.2.1 del presente libro.

Como complemento a la citada información, hay que recordar que en el contenido del derecho de información general recogido en el artículo 5 de la LOPD, se debía informar entre otros aspectos, acerca de los destinatarios de los datos, por lo que dicha obligación de información se complementaría con la recogida en el presente punto.

Que la cesión de datos se produzca con el **consentimiento previo del interesado,** siempre y cuando no sea de aplicación alguna de las excepciones al consentimiento respecto a la cesión de datos.

Como ya se pudo ver al analizar la figura del consentimiento, se trata, indiscutiblemente, de uno de los puntos de mayor relevancia en cuanto a protección de datos de carácter personal. Dicho consentimiento, será igualmente necesario para poder comunicar los datos a un tercero, salvo que, expresamente, se

prevea alguna excepción. Si es preciso con carácter general el consentimiento para tratar los datos personales, igual ocurrirá en lo que respecta a su comunicación, dado que de dicha cesión surgirá un nuevo e independiente tratamiento de datos.

Por tanto, en los supuestos en que vayamos a tratar determinados datos de carácter personal, y no sea de aplicación ninguna de las excepciones al consentimiento, deberemos contar ineludiblemente con el consentimiento del afectado. Si además pretendemos ceder o comunicar los datos que están siendo tratados, precisaremos igualmente de otro consentimiento adicional para poder realizar dicha comunicación o cesión, salvo en los casos en que legalmente no sea exigible.

No bastará que el responsable cuente con el consentimiento del afectado para la cesión de datos, sino que será igual de importante para evitar una sanción, el poder acreditar que efectivamente se contaba con éste. De poco servirá la obtención de un determinado consentimiento para la comunicación de datos, si luego el responsable no es capaz de acreditar ante un eventual procedimiento sancionador, que efectivamente obtuvo el consentimiento de dicho afectado.

Como ya se ha analizó en el epígrafe 2.3, los requisitos que deberá cumplir el consentimiento que se vaya a obtener para su plena eficacia y validez son:

- Inequívoco.
- Libre.
- Específico.
- Informado.

Es por ello, por lo que el consentimiento deberá cumplir con todos los requisitos ya vistos en el citado punto 2.3, por lo que nos remitimos a dicho punto en aras de evitar reiteraciones innecesarias.

Por último, queremos señalar que el consentimiento para la cesión de datos es revocable.

Que se dé pleno cumplimiento a la información respecto a la primera comunicación de datos (artículo 27 de la LOPD), en los términos ya vistos en el epígrafe 2.2.4.

Si pretendemos remitir, comunicar o permitir que cualquier tercero pueda visualizar, de cualquier forma (en pantalla, entregando una copia por escrito, remitiendo un fax, etc.), los datos personales de los que somos responsables, incluidas empresas del mismo grupo empresarial (dado que serían consideradas como terceros), la norma general implica que obtengamos previamente el **consentimiento del afectado,** debiendo informar respecto a la finalidad a que se destinarán los datos que van a ser cedidos y el tipo de actividad de aquel a quien se pretenden comunicar, indicando igualmente quién será el destinatario de los datos.

3.2 Excepciones al consentimiento para la comunicación de datos

Existen una serie de supuestos en los que **no será preciso contar con el consentimiento previo del interesado para la cesión de sus datos.** Dichas excepciones se encuentran reguladas con carácter general, en el artículo 11.2 de la LOPD, no siendo de aplicación las mismas en aquellos supuestos en los que se pretendan ceder datos especialmente protegidos, como más adelante se verá.

Los supuestos que se salen de la norma general que establece como obligatorio el contar con el consentimiento previo para la cesión de datos, son los siguientes:

- **Cuando la cesión esté autorizada en una ley.**

  La norma habilitante deberá ser una Ley, no bastando por tanto reglamentos, etc.

- **Cuando se trate de datos recogidos de fuentes accesibles al público.**

  Por tanto, se podrán ceder los datos que se obtengan de fuentes accesibles al público, remitiéndonos a la definición de datos de fuentes accesibles al público a lo indicado en el capítulo primero respecto a su interpretación restrictiva, acorde a la lista cerrada que ostenta tal carácter.

  Para el tratamiento de dichos datos, y cuando se vayan a destinar a la actividad de publicidad o prospección comercial, no será necesario informar en el plazo de tres meses desde su registro, por disponerlo así el párrafo segundo del artículo 5.5. de la LOPD, debiendo informar en cada comunicación que se efectúe en los términos ya vistos. Igualmente, no sería necesario el consentimiento general para su cesión, según se analiza en el presente punto. Por último, y respecto a dicha categoría de datos, sí sería necesario informar respecto a la primera comunicación de los mismos, según establece el artículo 27.2 de la LOPD.

- **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.**

  Dado que la excepción al consentimiento no afecta al resto de obligaciones derivadas de la LOPD, también en estos casos se deberá informar al afectado del tratamiento de datos que será realizado por el responsable, así como del resto de puntos recogidos en el artículo 5 de la LOPD (ya analizada la obligación de información).

  En el momento en que se recaben los datos, se deberá informar del contenido del tratamiento de datos personales, finalidades, destinatarios de los datos, se podrían entender

que más que una excepción al consentimiento, se trataría de un supuesto de consentimiento tácito, ya que el afectado, una vez que es convenientemente informado, facilita los datos al responsable (acto positivo de aceptación del tratamiento).

Esta excepción, está precisamente establecida en beneficio del afectado, dado que, en caso de no producirse dicha comunicación, no se podría atender la finalidad que aceptó, que no es otra que la relación jurídica vinculante entre ambas partes. De acuerdo a lo anterior, ese será precisamente el límite de la excepción, que sea imprescindible la comunicación para el mantenimiento de la relación jurídica. Si se entendiese que realmente no hay necesidad de comunicar los datos para cumplir la finalidad aceptada por el afectado, sería preciso obtener el consentimiento, salvo que fuera de aplicación alguna otra excepción. Precisamente si el afectado no permitiese esa comunicación, estaría revocando la autorización para el tratamiento de datos de acuerdo a la finalidad que se aceptó.

- **Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal, 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.

Excepción relacionada con lo que se analizará en el punto siguiente (cesión de datos especialmente protegidos), así como lo dicho para los supuestos de excepción al consentimiento para el tratamiento de datos (artículo 6.2 LOPD) y tratamientos de datos especialmente protegidos (artículo 7 de la LOPD).

En último lugar, hay que indicar que si los datos se disocian con carácter previo a la cesión, no será de aplicación lo dispuesto en el artículo 11 de la LOPD. Si los datos se disocian de forma correcta, no pudiendo el cesionario llegar a conocer o asociar los datos recibidos a una persona física, no se habrán cedido datos de carácter personal de personas físicas, ni identificadas ni identificables. Para la aplicación de lo anterior, es importante indicar que de los datos disociados, no se debe poder conseguir la identificación de su titular, dado que en caso contrario, la disociación no se habría producido.

Existen determinados supuestos en los que no es necesario el consentimiento del afectado para poder remitir sus datos a un tercero. En caso de duda respecto a si es o no de aplicación alguna de las excepciones indicadas, será aconsejable obtener el consentimiento para la cesión de los datos, por la propia seguridad tanto del cedente como del cesionario de los datos, dado que podrían ser fuertemente sancionados por la AEPD. Las excepciones generales al consentimiento que se han visto en el presente apartado no son de aplicación a los supuestos en que lo que se vayan a ceder son datos especialmente protegidos, dado que éstos tienen un régimen de habilitación para su tratamiento mucho más riguroso que los requerimientos para el tratamiento y cesión del resto de datos personales.

3.3 Supuestos especiales. Consentimientos reforzados en la cesión de datos

En el epígrafe 2.3.3 ya se han analizado los supuestos en los que es preciso la obtención de un consentimiento reforzado, no bastando, por tanto, el consentimiento inequívoco al que se hace referencia en el artículo 6 de la LOPD. En concreto, y recordando lo referido en el citado punto 2.3.3 señalar que el tratamiento de los siguientes datos, requerirían un consentimiento especial:

La comunicación de los siguientes datos, requerirá el **consentimiento expreso y por escrito** de los afectados:

- Ideología.
- Afiliación sindical.
- Religión.
- Creencias.

No bastará que exista una habilitación legal que prevea o admita determinada cesión de datos, ni será de aplicación ninguna de las excepciones generales al consentimiento recogidas en el artículo 6 ni 11.2 de la LOPD (cuando e refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento, etc.).

Incluso en el supuesto excepcionado de consentimiento que se recoge en el artículo 7.2 de la LOPD (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), también será preciso el consentimiento expreso y por escrito para la comunicación de dichos datos. Y ello, aunque en el artículo 7.2

de la LOPD dice: "(…) *sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado*", sin que se haga mención a la necesidad del consentimiento expreso. Una interpretación acorde con la norma, supondría que el consentimiento igualmente deba ser expreso y por escrito, dado que es el tipo de consentimiento requerido para el tratamiento de dichos datos, englobando el concepto de tratamiento de datos, las cesiones que resulten de comunicaciones, consultas, etc.

Para la comunicación de los siguientes datos,será preciso, según marca el artículo 7.3 de la LOPD, que por razones de interés general **así lo disponga una ley** o el **afectado consienta expresamente:**

- Origen racial.
- Salud.
- Vida sexual.

Por tanto, en este supuesto, a diferencia de lo que ocurría en el supuesto anterior, cuando nos encontremos con una habilitación legal, podremos comunicar dichos datos sin consentimiento, pero debiendo tener en cuenta que, en caso de mínima duda respecto a la existencia o no de habilitación legal, se deberá optar por la obtención del consentimiento expreso.

Al igual que en el supuesto anterior, no serán de aplicación las excepciones generales al consentimiento para la cesión de datos recogidas en el artículo 6 ni 11.2 de la LOPD.

3.4 El cesionario de los datos

La persona o entidad que fuera a ser la cesionaria o destinataria de los datos de carácter personal, por el mero hecho de la comunicación de los mismos, quedará obligada a la observancia

de las disposiciones contempladas en la LOPD y su normativa de desarrollo (artículo 11.5 LOPD).

En concreto, y como obligación inicial, deberá informar a los afectados, según se establece en el artículo 5.4 de la LOPD dentro de los tres meses desde el registro de los datos (epígrafe 2.2.2).

Aunque la obligación de la obtención del consentimiento para la cesión de los datos de carácter personal debe corresponder a la entidad cedente, el riesgo en el tratamiento de los datos por parte del cesionario no queda difuminado por tal premisa.

El cesionario de los datos no puede ampararse en que el consentimiento para la cesión debió ser obtenido por el cedente de los datos, por ser esa la entidad que tenía todos los medios para la obtención del mismo. Como ya se ha indicado, por el mero hecho de ser cesionario de los datos, el cesionario ya se encuentra obligado a la observancia de todas las obligaciones contempladas en la LOPD. Entre las principales obligaciones, se encuentra el propio consentimiento para el tratamiento de los datos personales. Por tanto, ¿qué ocurriría si el cedente de los datos no obtuvo el consentimiento de los afectados para su cesión? Lo que ocurriría es que la persona o entidad que los recibió no tendría autorización o consentimiento para tratarlos y, por tanto, su tratamiento sería contrario a la LOPD.

En aquellos supuestos en los que se prevea que vayamos a ser cesionarios (receptores) de datos de carácter personal, deberemos verificar que el consentimiento para la cesión de datos de carácter personal ha sido efectivamente obtenido, dado que en caso contrario, podríamos ser sancionados por la cesión realizada por el cedente sin el debido consentimiento. Precisamente será el incumplimiento realizado por el cedente, el que arrastrará inevitablemente al cesionario a tratar los datos de carácter personal, sin la necesaria habilitación o cobertura para ello.

En concreto, para los supuestos en los que vayamos a ser cesionarios de los datos, se deberán establecer las siguientes cautelas:

- Establecer una cláusula contractual en la que la empresa cedente garantice la licitud y calidad (artículo 4 de la LOPD) de los datos cedidos, comprometiéndose a realizar la comunicación o cesión de datos con pleno respeto a las obligaciones reguladas por la LOPD y su normativa de desarrollo, garantizando la indemnidad patrimonial de la cesionaria en caso de incumplimiento de lo anterior.
- Que la empresa cedente garantice que la cesionaria, en virtud de la cesión de datos, estará habilitada para las finalidades que pretende perseguir a través del tratamiento de datos que se realizará de los datos cedidos.
- Recabar con carácter previo algún documento de la cedente en el que se justifique que realmente ha obtenido el consentimiento (algún cuestionario de los que utilice el cedente para recabar datos, etc.). Dicho documento se guardará y será el que pueda justificar, que de forma diligente, se verificó la existencia del consentimiento.

Si los datos que van a ser cedidos, son de los denominados **especialmente protegidos,** deberemos extremar las precauciones, ya que para tratar los mismos, necesitaríamos el consentimiento expreso o expreso y por escrito (en los términos ya vistos). Es por ello por lo que en dichos supuestos, se debe verificar diligentemente que cumplimos con dicho extremo.

Si vamos a recibir **datos personales** (alquiler o compra de una base de datos, etc.) debemos verificar que o bien no es necesario el consentimiento por ser de aplicación alguna de las excepciones ya vistas, o bien la entidad que nos vaya a remitir los datos nos debe garantizar la licitud de la cesión, debiendo comprobar diligentemente dicho extremo. En caso contrario, podríamos ser sancionados junto con el cedente de los datos.

Debemos asimismo verificar que podremos realizar los tratamientos de datos que tenemos previstos, debiendo garantizar el cedente los tratamientos y finalidades habilitados por los afectados.

Modelo de obtención del consentimiento para la cesión de datos

De conformidad con lo recogido en el artículo 5, 6 y 11 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de Datos de Carácter Personal, quedo informado y consiento, que los datos que voluntariamente facilite a través del presente documento *(si de la relación que surja, se van a recibir o tratar más datos, se deberá igualmente indicar. Por ejemplo: así como todos los datos e informaciones que nos facilite a durante la gestión, mantenimiento y desarrollo de la relación* _____ *(laboral, contractual, etc)*), quedarán registrados en el fichero _____ *(introducir nombre del fichero y código de inscripción en la AEPD)* responsabilidad de _____ *(datos identificativos de la persona responsable, ya sea persona física o jurídica),* única destinataria de los datos salvo lo recogido en la presente cláusula para la cesión de los mismos, con la finalidad de _____ *(indicar la finalidad o finalidades del tratamiento, no indicando finalidades incomprensibles, vagas, imprecisas, etc. Igualmente, habrá que tener en cuenta que las finalidades que no se indiquen, no podrán realizarse).*

Quedo informado de la obligatoriedad de las respuestas a las preguntas planteadas que se encuentran marcadas con un asterisco (*) en el documento *(habrá que indicar en el documento los campos obligatorios con un asterisco)*, en caso de no facilitar dichos datos, no se podrá atender mi solicitud.

Una vez facilite los datos, éstos serán tratados por el responsable anteriormente indicado, y de acuerdo a las finalidades determinadas, explícitas y legítimas que se indican en la presente cláusula.

Quedo informado que podré ejercitar los derechos de acceso, rectificación, cancelación y oposición, mediante comunicación al domicilio del responsable del tratamiento, sito en _____ *(indicar todos los datos del domicilio. Igualmente, si se hubiese habilitado un teléfono de información respecto a protección de datos, indicarlo).*

Continúa

Los datos personales de _____ *(indicar los datos que será objeto de la cesión)* serán cedidos a _____, *(identificar entidad cesionaria y su dirección)* entidad dedicada a _____ *(identificar tipo de actividad de aquel a quien se van a ceder los datos)* con la finalidad de _____ *(indicar la finalidad a que destinarán los datos cuya comunicación se autoriza)*. En caso de no consentir la citada cesión de datos, marcar la siguiente casilla _____.

Si se produjese algún cambio en los datos personales facilitados, quedo informado de mi obligación de notificar dicho extremo al responsable, a los efectos de su correcta actualización.

Con la firma del presente documento, y su remisión a _____ autorizo de forma expresa los anteriores tratamientos de datos indicados en la anterior cláusula de protección de datos de carácter personal.

Acceso a datos de carácter personal

4.1 Concepto de acceso a datos de carácter personal

Se encuentra regulada dicha figura en el artículo 12 de la LOPD, que establece:

"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.

Continúa

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."*

Existen casos en los que se revelan datos a una persona distinta del interesado, definición dada respecto al término comunicación de datos en el artículo 3, apartado i), y que realmente no nos encontramos ante una comunicación de datos, quebrando por tanto la referida definición en los supuestos de accesos a datos de carácter personal.

La LOPD, a los efectos de poder flexibilizar el modo de organización empresarial, y permitir determinadas contrataciones de servicios relacionados con el tratamiento de datos ha concebido la figura del encargado del tratamiento. Viene a solventar los problemas que se podrían dar en los supuestos, por ejemplo, en los que fuéramos a contratar una auditoría fiscal con una tercera entidad. La Auditora, a los efectos de poder realizar su trabajo, necesariamente tendría que entrar a ver determinados datos de carácter personal de los que la entidad auditada es responsable. Si no existiera el concepto jurídico de acceso a datos, en el momento en que la Auditora conociese cualquier dato personal responsabilidad de la Auditada, estaríamos ante un claro supuesto de comunicación de datos a tercero, dado que comunicación de datos viene definida como toda revelación realizada a una persona distinta del interesado.

Dado que la Auditora es indudablemente una entidad distinta, estaríamos ante una cesión de datos y, por tanto, sería de aplicación

el riguroso régimen establecido en la LOPD para dichos supuestos (consentimiento previo a la cesión, información de los destinatarios, comunicación de la primera cesión, etc.). Igualmente, la entidad auditora tendría que solventar varios problemas respecto a dicha cesión. En concreto debería informar en el plazo de tres meses desde el registro de los mismos y verificar que ostenta el consentimiento para el tratamiento de los datos cedidos.

Lo mismo ocurre en el caso en que encargáramos a una gestoría, que llevase, por ejemplo, las nóminas de la empresa o los aspectos fiscales, o si contratásemos con un tercero la destrucción de los soportes en que consten datos personales (DVD, CD, papel, etc.) o si encargáramos a un tercero el ensobrado de cartas para una determinada campaña publicitaria.

Por tanto, si se tuviese que aplicar el régimen de la cesión en dichos casos, se estaría coartando la posibilidad de organización empresarial del responsable en el tratamiento de datos, por lo que el artículo 12 de la LOPD viene a suplir dichas dificultades.

En último lugar, indicar que el responsable del tratamiento deberá velar por que el encargado del tratamiento cumpla estrictamente las instrucciones y las garantías impuestas por el primero.

4.2 Requisitos

Que el acceso a datos de carácter personal sea necesario para la prestación de un servicio al responsable del tratamiento.

En primer lugar, indicar que serán cuatro las figuras fundamentales en un acceso a datos de carácter personal:

- El responsable del tratamiento.
- El encargado del tratamiento.

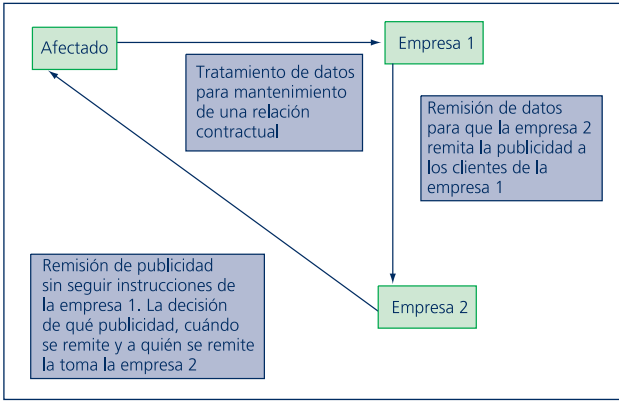
- El afectado o interesado.
- Los datos de carácter personal.

El encargado, será la persona o entidad que accederá a los datos de carácter personal responsabilidad de la persona o entidad a la que prestará el servicio (el responsable), siendo dicho servicio, el que motivará el acceso a datos de determinados afectados.

En muchas ocasiones, determinadas operaciones con incidencia en materia de protección de datos de carácter personal se regulan de forma sistemática por los responsables como acceso a datos, dado que es aparentemente lo más sencillo, bastando para ello la inclusión de una determinada cláusula en el contrato en la que se recogiese el contenido mínimo establecido en el artículo 12 de la LOPD. Ahora bien, se están dando muchos supuestos en los que en la realidad, tras un contrato de acceso a datos, realmente lo que se ha producido es una comunicación de los mismos, dado que el "supuesto" encargado del tratamiento no lo es, siendo responsable en el tratamiento de los datos a los que "ha accedido", estando por tanto el encargado en dichos supuestos realizando funciones independientes de las que motivaron dicho contrato de acceso a datos, tomando decisiones que afectan al tratamiento de los datos de carácter personal con total autonomía, surgiendo en la mayoría de estos casos un nuevo vínculo entre el afectado y el encargado del tratamiento, siendo dicho vínculo independiente del que tenía el afectado con el responsable.

Aunque una operación se articule como un acceso a datos, la AEPD podrá entender que dicho acceso no es real, siendo la consecuencia inevitable una fuerte sanción dado que en la mayoría de las ocasiones, al entender el responsable (erróneamente) que se encontraba ante un acceso a datos, consecuentemente no obtuvo los consentimiento para la comunicación de los datos. En el momento en que la AEPD entienda que no es un acceso a datos, la consecuencia inevitable es que se trata de una comunicación de datos y, por tanto, se debería haber cumplido con el régimen establecido para la cesión de datos (principalmente, el consentimiento previo).

Figura 4.1. Cesión de datos.

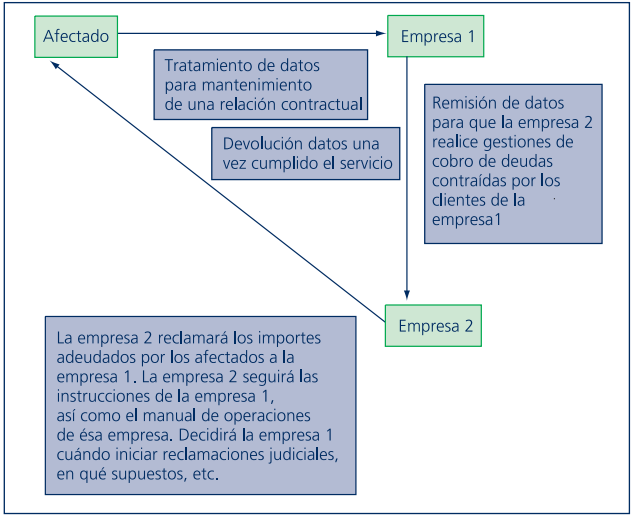


En el supuesto anterior, se puede advertir que la empresa 2 no va a seguir las instrucciones de la empresa 1, dado que la empresa 2 se dedicará a la comercialización de sus productos entre los clientes de la empresa 1. Quien decidirá sobre la finalidad, contenido y uso de los datos cedidos, será la empresa 2, por lo que aunque se hubiese firmado un contrato de acceso a datos entre la empresa 1 y la empresa 2, la AEPD podría entender que se trata de una cesión de datos y no un acceso. Si se trata realmente dicho supuesto de una comunicación de datos, la empresa 2 queda obligada al cumplimiento de todas las obligaciones derivadas de la LOPD (información, consentimiento, etc.).

Igualmente, no encajaría el anterior caso en un supuesto de acceso a datos, dado que el acceso no parece que sea necesario para la prestación de un servicio al responsable. Más bien, al contrario. El servicio parece que lo estaría prestando la empresa 1 a la 2. Por tanto, la empresa 2 no seguirá las instrucciones del responsable, no le estaría prestando un servicio y, por tanto, en principio, no sería susceptible de articularlo como un acceso a datos.

En el anterior caso será necesario el consentimiento de los afectados para llevar a cabo dicha operación.

Figura 4.2. Acceso a datos.



En este segundo supuesto, según está planteado, la empresa 2 sí que seguirá las instrucciones de la empresa 1, por lo que sí que *a priori* sería susceptible de acceso a datos de carácter personal. Igualmente, se puede ver como claramente la empresa 2 va a prestar un servicio real al responsable del tratamiento, estando dicho servicio vinculado al tratamiento de datos de responsabilidad de la empresa 1, y teniendo dicha empresa habilitación legal para tratarlos, para la finalidad del mantenimiento y desarrollo de la relación contractual que existiría entre el afectado y la empresa 1. Al seguir las instrucciones de la empresa 1, la empresa 2 no tratará los datos con autonomía propia, no decidiendo, por tanto, sobre la finalidad, contenido y usos del tratamiento de datos.

Requisito formal

Se recoge en el artículo 12 de la LOPD 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.

Hay que señalar, que el Código Civil en su artículo 1.278, dispone: "*los contratos serán obligatorios, cualquiera que sea la forma en que se hayan celebrado, siempre que en ellos concurran las condiciones esenciales para su validez*". Por su parte, el artículo 1.279 del mismo texto legal establece: "*Si la Ley exigiese el otorgamiento de escritura u otra forma especial para hacer efectivas las obligaciones propias de un contrato, los contratantes podrán compelerse recíprocamente a llenar aquella forma desde que hubiese intervenido el consentimiento y demás requisitos necesarios para su validez*".

De lo recogido en los anteriores artículos, se deduce el principio de libertad de forma en los contratos. Ahora bien, el citado artículo 12 de la LOPD establece que deberá constar la prestación de servicios en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido.

Para poder acreditar la existencia del contrato, su celebración y contenido, deberá constar, ineludiblemente por escrito, dado que en caso contrario, no se podrá acreditar ante la AEPD la existencia y contenido del mismo, pudiendo ser, por tanto, sancionados.

El artículo 12.1 de la LOPD prevé un contenido mínimo, indispensable, como, por ejemplo, que el encargado del tratamiento deberá seguir las instrucciones del responsable del tratamiento, la no utilización de los datos para un fin distinto al que figure en el contrato, su no comunicación a otras personas, así como el establecimiento de las medidas de seguridad del artículo 9 de la LOPD y que, cumplida la prestación, se destruyan los datos o sean devueltos al responsable del tratamiento. Si no es por escrito, difícilmente se podría acreditar la existencia de dichos elementos en la relación entre el responsable y el encargado del

tratamiento. Tanto la jurisprudencia como la propia AEPD entienden que se trata de un requisito imprescindible el que conste el contrato en forma escrita.

Contenido mínimo del contrato

El contrato deberá recoger inexcusablemente, los siguientes puntos:

- **Que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento.**

  Es ésta una de las características principales de la figura del encargado del tratamiento. Si precisamente a los accesos a datos por cuenta de terceros no se les aplica el régimen de la cesión, es porque el encargado debe tratar los datos conforme a las instrucciones del responsable del tratamiento. Si la entidad que los recibe, no puede tratarlos decidiendo sobre la finalidad, contenido o uso del tratamiento, no podrá ser considerado responsable, dado que estos aspectos son característicos de la figura del responsable del fichero o tratamiento.

  Precisamente, el encargado del tratamiento, tratará los datos actuando en nombre y por cuenta del responsable, actuando en cumplimiento de sus instrucciones.

  El punto cuarto del artículo 12 de la LOPD establece que 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 hubiere incurrido personalmente.

- **Que no los aplicará o utilizará con fin distinto al que figure en dicho contrato.**

  Al igual que en el supuesto anterior, el encargado del tratamiento no puede utilizar los datos con una finalidad distinta a la que figure en el contrato, dado que se estaría separando de las instrucciones del responsable y tratando los datos para unas finalidades distintas de las que motivaron el acceso a

datos por parte del encargado. En caso de que se produjera dicha separación respecto a la finalidad recogida en el contrato, el encargado sería considerado responsable del tratamiento, respondiendo personalmente de las infracciones en que hubiera incurrido.

- **Que el encargado del tratamiento no comunicará los datos, ni siquiera para su conservación, a otras personas.**

  Se ha discutido la posibilidad de que por parte del encargado, se puedan subcontratar aspectos que conforman el acceso a datos que éste pudiera realizar. La finalidad de la presente prohibición es que el responsable pueda perder el control sobre los datos, debido a las posibles cadenas de subcontrataciones que se podrían producir entre los distintos encargados del tratamiento.

  Pese a que de los términos del artículo 12 de la LOPD, se deduce necesariamente que el encargado del tratamiento no puede subcontratar con un tercero, la AEPD, en su informe 2004-0513 (www.agpd.es), admite la subcontratación, pero debiendo mantenerse las siguientes cautelas:

  "Por otro lado, de preverse o producirse por parte del prestador de un servicio una subcontratación que implique tratamiento de datos personales deberá reflejarse en el contrato los requisitos exigidos por la normativa de protección de datos haciendo constar expresamente, además de las prescripciones del citado artículo 12 que, o bien el contratista del servicio actúa en nombre y por cuenta del responsable del fichero o tratamiento o, alternativamente, se especifiquen los siguientes requisitos acumulativos, que deberán figurar en el contrato:

  a. *Que los servicios a subcontratar se hayan previsto expresamente en la oferta o en el contrato celebrado entre el responsable del fichero y el encargado del tratamiento.*
  b. *Que el contenido concreto del servicio subcontratado y la empresa subcontratista conste en la oferta o en el contrato.*

c. *Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.*

En consecuencia, la subcontratación de terceras entidades encargadas del tratamiento será posible siempre y cuando o bien el contratista del servicio actúe en nombre y por cuenta del responsable del fichero o tratamiento o, alternativamente, se especifiquen los requisitos que se acaban de indicar."

- **Las medidas de seguridad que deba incorporar el encargado del tratamiento.**

  Establece el artículo 12 de la LOPD, que se deberán estipular las medidas de seguridad a que se refiere el artículo 9 de la LOPD, que el encargado está obligado a implementar.

  En concreto, el artículo 9 de la LOPD establece:

  "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."

Actualmente, las medidas de seguridad que se han aprobado y desarrollado reglamentariamente son las recogidas en el Real Decreto 994/1999, que ya ha sido analizado en el epígrafe 2.4. Faltaría el desarrollo reglamentario respecto a las medidas de seguridad para los ficheros no automatizados. El responsable deberá indicar en el contrato las medidas de seguridad que corresponderá implantar al encargado, de acuerdo a los datos que éste último fuera a acceder. Si el acceso únicamente se produce respecto a datos que requieren un nivel de seguridad básico, se deberá recoger la obligación del encargado de implementar dichas medidas de seguridad en el propio contrato, con indicación a las medidas que corresponden a dicho nivel (o al menos, una remisión a los artículos en que consten estas medidas).

- **Cumplimiento del deber de secreto.**

  El artículo 10 de la LOPD establece que todos los que intervengan en cualquier fase del tratamiento de datos de carácter personal, están obligados al secreto profesional 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.

  Esta obligación va dirigida, fundamentalmente, a los trabajadores de la entidad que presten sus servicios para el responsable del fichero o tratamiento. Ahora bien, tanto el encargado como sus empleados deberán cumplir con dicha obligación de guardar secreto profesional, durante la prestación de los servicios, como una vez finalizados.

  Por tanto, sería aconsejable que en el mismo contrato de prestación de servicios, se estableciera que sus trabajadores y quienes intervengan en el acceso a los datos de carácter personal, tienen suscritos los compromisos de confidencialidad.

- **Obligaciones una vez efectuado el encargo de tratamiento de datos.**

  Una vez finalice la prestación al responsable que motivó el acceso a datos de carácter personal, deberá el encargado

destruir o devolver los datos personales, así como cualquier soporte o documento en que pudieran constar dichos datos.

El responsable deberá decidir si solicita la devolución de los datos o su destrucción, variando por lo general en función de la causa que motivó el acceso a ellos. Si, por ejemplo, el acceso se produjo como consecuencia de la realización de determinadas encuestas telefónicas a los clientes del responsable, los datos a los que hubiera accedido el encargado lo normal es que fueran devueltos, dado que en este caso el encargado habría accedido a los datos de contacto de los clientes del responsable para poder contactar con éstos (estos datos podrían perfectamente ser destruidos, si así lo indicase el responsable) y los datos que se hubieran obtenido a través de las encuestas deberían ser entregados al responsable, dado que es el motivo principal del acceso a datos.

Si de la realización del encargo se derivase la obtención de nuevos datos, de carácter personal de los afectados, el encargado debería, siguiendo instrucciones del responsable, informar a las personas con las que contacte y de las que va a obtener nuevos datos (datos de satisfacción, calidad de los productos, etc.) del concreto tratamiento de datos que se irá a realizar de esos nuevos datos que van a ser obtenidos, indicando como responsable de los mismos al responsable del tratamiento. La información y consentimiento para el tratamiento de dichos datos debería obtenerse de conformidad con lo que ya se ha analizado a lo largo de la presente obra.

- **Responsabilidad del encargado del tratamiento.**

  Si el encargado se desliga del contenido del contrato de acceso a datos, destinándolos a otra finalidad, incumpliendo las obligaciones del contrato (medias de seguridad, obligación de seguir las instrucciones del responsable, etc.), perderá ese estatus de encargado, siendo considerado también responsable, respondiendo por tanto de las infracciones en que hubiere incurrido.

Dicha responsabilidad surge dado que en el momento en que el encargado se desligue del contenido del contrato, no estará tratando los datos conforme a lo previsto y ordenado por el responsable, adquiriendo, por tanto, autonomía en las decisiones que tome, las cuales no podrán imputarse al responsable, respondiendo de éstas personalmente.

4.3 Supuestos más habituales en una PYME

Los supuestos que a continuación se indican serían los que con más frecuencia se suelen dar respecto al tratamiento de datos que realizan las empresas. En todos ellos, un tercero accederá a los datos que son responsabilidad de la empresa, debiendo ésta, por tanto, dar pleno y eficaz cumplimiento a lo previsto en el artículo 12 de la LOPD a los efectos de evitar que se pierda el poder de control sobre los dato

Supuestos más habituales en una PYME:

- Gestoría.
- Manipulado de datos (cartas, etc.).
- Asesoría jurídica externa.
- Realización de encuestas.
- Apoyos en la contratación (call centres externos, etc.).
- Seguridad (grabaciones de seguridad y control de acceso al edificio).
- Gestión de recobros.
- Prestaciones de servicios a otras empresas del grupo empresarial.
- Imprenta (elaboración de tarjetas de visita de empleados, etc.).
- Auditorías externas.

4.4 Modelo de cláusula de acceso a datos de carácter personal

La siguiente cláusula, se debe incorporar en aquellos contratos, en los que un tercero vaya a acceder a datos de carácter personal de los que seamos responsable:

Modelo de acceso de datos de carácter personal

Para la prestación de los servicios regulados y recogidos en el presente contrato, es imprescindible que "A" (encargado del tratamiento) acceda a datos de carácter personal responsabilidad de "B" (responsable del tratamiento). *(A, será la entidad que nos va a prestar los servicios. Por ejemplo, los de ensobrado y remisión de cartas a correos, o los de recobros frente a terceros, etc. Las condiciones del contrato, obligaciones de las partes, etc. deberán constar en el contrato)*. Dicho acceso a datos no tendrá la consideración de comunicación de datos de carácter personal, siendo por tanto de aplicación lo recogido en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, "LOPD").

"A" declara conocer las obligaciones que se derivan del tratamiento de datos de carácter personal, entendiendo por éstos a lo recogido en el artículo tercero, apartado c) de la citada LOPD.

"A" en su calidad de encargado del tratamiento se obliga a:

1. Tratar los datos únicamente conforme a las instrucciones del responsable del tratamiento ("B").
2. No aplicar o utilizar los datos personales a los que acceda con un fin distinto al que figura en el presente contrato.
3. No comunicar a otras personas, ni siquiera para su conservación, los datos personales a los que acceda.
4. Implementar las medidas de seguridad, tanto de índole técnica y organizativas necesarias que garanticen la seguridad

Continúa

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.
En concreto, las medidas de seguridad que deberá implementar, serán las recogidas 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 (en adelante, "RMS"), de acuerdo con la aplicación de los niveles de seguridad a los que se hace referencia en el artículo tercero y cuarto del citado Reglamento, o las medidas de seguridad que se indiquen en cualquier norma que pudiera sustituir o modificar a la anterior.

El nivel de seguridad que deberá implementar "A" será el nivel _____ (indicar nivel básico, básico/medio o básico/medio/alto). Las medidas de seguridad que corresponderán a dicho nivel de seguridad, serán las recogidas en los artículos _____ a _____ del "RMS" *(indicar los artículos que corresponda. Para las medidas de seguridad de nivel básico, artículos 8 a 14 y 5 a 7, para nivel básico/medio 8 a 22 y 5 a 7, y para básico/medio/alto, artículos 8 a 26 y 5 a 7)*.

"A" declara conocer el alcance y contenido del citado "RMS", así como de las medidas de seguridad que corresponden a cada nivel de seguridad de acuerdo con lo anterior.

"A" se compromete a dejar inspeccionar al personal de "B" el cumplimiento de las anteriores medidas de seguridad.

5. Guardar el debido secreto profesional respecto a los datos a los que tuviere acceso en cumplimiento y ejecución del presente contrato, subsistiendo dicha obligación de secreto profesional incluso después de finalizar su relación con "B". Asimismo informará a su personal y colaboradores de las obligaciones de confidencialidad, garantizando a

Continúa

"B" que tiene suscritos documentos de confidencialidad con sus empleados y colaboradores, a fin de garantizar y asegurar el tratamiento de la información a la que acceda con las debidas garantías de confidencialidad y secreto profesional.

Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos a "B", al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto de tratamiento, debiendo emitir "A" a simple requerimiento de "B" un certificado acreditativo de lo anterior *(se deberá indicar la opción deseada. Sería aconsejable que el encargado emita un certificado, una vez se extinga la relación contractual, de devolución o destrucción de los datos)*.

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

Derechos de los afectados

5.1 Caracteres básicos de los derechos de acceso, rectificación, cancelación y oposición

La nota principal de los derechos es su carácter de personalísimos. Por tanto, deberán ser ejercitados directamente por los interesados. Tiene gran importancia que el responsable verifique quién está ejercitando el derecho, guardando prueba documental de ello, a los efectos de evitar facilitar el ejercicio de un derecho a persona distinta del interesado, lo que consecuentemente supondría una sanción por parte de la AEPD.

El artículo 11 del Real Decreto 1332/1994, respecto a la posibilidad de ejercicio de los derechos por medio de representante legal, establece que: *"Los derechos de acceso a los ficheros automatizados, así como los de rectificación y cancelación de datos son personalísimos y serán ejercidos por el afectado frente al responsable del fichero.* (...) *Podrá, no obstante, actuar el representante legal del afectado cuando éste se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de los mismos*".

La solicitud que se dirija al responsable deberá contener, de conformidad con lo establecido en el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, que continúa en vigor de conformidad con lo establecido en la Disposición Transitoria Tercera de la Ley

Orgánica 15/1999, así como en la Instrucción 1/1998, de 19 de enero, de la Agencia Española de Protección de Datos:

- Nombre, apellidos, fotocopia del documento nacional de identidad del interesado, en los casos que excepcionalmente se admita, de la persona que lo represente, así como el documento acreditativo de tal representación. La fotocopia del documento nacional de identidad podrá ser sustituida siempre que se acredite la identidad por cualquier otro medio válido en derecho.
- Petición en que se concreta la solicitud.
- Domicilio a efectos de notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición que formula, en su caso.
- El interesado deberá utilizar cualquier medio que permita acreditar el envío y la recepción de la solicitud.

Es importante que formule el acceso por cualquier medio que garantice la identificación del afectado y en la que conste el fichero, o ficheros, a consultar.

El responsable del fichero deberá contestar la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado en sus ficheros, debiendo utilizar cualquier medio que permita acreditar el envío y la recepción. En el caso de que la solicitud no reúna los requisitos mínimos, el responsable del fichero deberá solicitar la subsanación de los mismos.

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.

En último lugar, la Ley configura los derechos de acceso, rectificación y cancelación como derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

5.2 Acceso

El responsable debe almacenar los datos de forma que se permita el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

El contenido del derecho de acceso, viene recogido en el artículo 15 de la LOPD, pudiéndose concretar dicho derecho en la posibilidad de solicitar y obtener el interesado, de forma gratuita información de:

- Sus datos de carácter personal sometidos a tratamiento.
- El origen de dichos datos.
- Las comunicaciones realizadas.
- Las comunicaciones que se prevén hacer de los mismos.

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

La información que se proporcione, cualquiera que sea el soporte en que fuere facilitada, se dará en forma legible e inteligible, previa transcripción en claro de los datos del fichero, en su caso, y comprenderá todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático.

En el caso de que los datos provengan de fuentes diversas, deberán especificarse las mismas, identificando la información que proviene de cada una de ellas.

La posibilidad de solicitar el acceso a los datos se encuentra limitada temporalmente, pudiéndose ejercitar dicho derecho en intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.

El responsable, una vez reciba la solicitud deberá:

- Contestar a la solicitud que se le dirija, con independencia de que figuren, o no, datos personales del afectado en sus ficheros, debiendo utilizar cualquier medio que permita acreditar el envío y la recepción.
- En el caso de que la solicitud no reúna los requisitos especificados en el apartado tercero, el responsable del fichero deberá solicitar la subsanación de los mismos.

Los plazos que deberá cumplir el responsable serán los siguientes:

- Plazo máximo de un mes a contar desde la recepción de la solicitud, con independencia de que no se dispongan de datos personales. En caso de no responder de forma expresa la solicitud en el plazo anterior, se entenderá desestimada, pudiendo el afectado solicitar tutela a la AEPD.
- Una vez estimada la solicitud en el anterior plazo, se deberá hacer efectivo el acceso en el plazo de 10 días desde la notificación de la estimación del acceso.
- En caso de que se hubiere ejercitado el derecho de acceso por el interesado en un intervalo inferior a 12 meses y no se acredite un interés legítimo al efecto, o en el supuesto de que la solicitud la formule persona distinta del afectado, se podrá denegar el acceso.

5.3 Rectificación y cancelación

La rectificación y cancelación de datos están regulados en el artículo 16 de la LOPD.

El plazo marcado por la Ley para dar efectivo cumplimiento a los derechos de rectificación y cancelación instados por los interesados es de 10 días. En caso de que la solicitud deba ser

subsanada, se deberá notificar al interesado, así como en el supuesto de desestimación de su solicitud, debiendo motivarse la contestación, a los efectos de que el interesado pueda instar un procedimiento de tutela de derechos ante la AEPD. Ahora bien, en la solicitud de cancelación, el interesado deberá indicar si revoca el consentimiento otorgado, en los casos en que la revocación proceda, o si, por el contrario, se trata de un dato erróneo o inexacto, en cuyo caso deberá acompañar la documentación justificativa.

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.

La rectificación y/o cancelación se deberá producir:

- Cuando los datos personales objeto de tratamiento no se ajuste a la LOPD.
- Cuando los datos personales objeto de tratamiento sean inexactos o incompletos.

La cancelación da 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 (la supresión definitiva se deberá producir una vez hayan prescrito las posibles responsabilidades del tratamiento, acciones de reclamación de los afectados, etc.). 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 pudiendo ser conservados en forma que permitan la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados. Se daría dicho supuesto,

por ejemplo, en el caso en que un determinado interesado revoque los consentimientos en su día otorgados para el tratamiento de sus datos, ya sea de forma total (todos los tratamientos autorizados) o parcial (los datos sujetos a determinada finalidad cuyo consentimiento vaya a ser revocado por el interesado). Dado que el responsable ya no tendría habilitación para dicho tratamiento, debería proceder a su cancelación.

Hay que tener en cuenta que en determinados supuestos, no se podrá proceder a la cancelación de los datos, dado que podrían ser, por ejemplo, necesarios para un determinado tratamiento legítimo por parte del responsable (por ejemplo, si el interesado ha contratado determinado servicio por un plazo de 1 año. No podría en principio instar la cancelación de sus datos hasta que finalizase ese vínculo jurídico consentido, que existe entre interesado y responsable, de conformidad con lo dispuesto en el artículo 6.3 de la LOPD, dado que no habría causa justificada para ello).

Los datos de carácter personal deben 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.

Por su parte, la rectificación, se podrá instar, a los efectos de que el responsable cumpla con el principio de calidad, en el supuesto en que los datos que se estén tratando sean inexactos o incompletos. Por tanto, dicho derecho se encuentra estrechamente relacionado con el principio de calidad de los datos, y, en concreto, con la obligación del responsable de mantener actualizada la información tratada. Ya se vio que el artículo 5.3. de la LOPD establece que los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación del afectado. Si los datos resultan ser inexactos o incompletos, deberán cancelarse y sustituirse de oficio por los correspondientes datos rectificados o completados.

5.4 Oposición

Se trata de un derecho introducido por la LOPD, el cual se encuentra pendiente de desarrollo reglamentario, de conformidad con lo dispuesto en el artículo 17 de la LOPD.

Los titulares de los datos pueden solicitar la oposición al tratamiento de datos, de conformidad con lo previsto en el artículo 6.4 de la LOPD, el cual establece que e*n 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.

Por su parte, el artículo 30.4 de la LOPD, al regular los tratamientos con fines de publicidad y de prospección comercial, dispone que 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 aquel a su simple solicitud.

5.5 Consulta al registro general de protección de datos

Según establece el artículo 14 de la LOPD, 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.

5.6 Impugnación de valoraciones

Recoge el artículo 13 de la LOPD que 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.

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

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

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

5.7 Derecho a indemnización

En el artículo 19 de la LOPD se regula el derecho que tiene todo interesado a ser indemnizado, en el supuesto en que como consecuencia de un incumplimiento por parte del responsable o del encargado del tratamiento de las disposiciones recogidas en la LOPD, sufra un daño o lesión en sus bienes o derechos.

Si el daño o lesión fuese causado o derivado de un fichero de titularidad pública, la reclamación se deberá exigir de acuerdo con la legislación reguladora de la responsabilidad de las Administraciones públicas, mientras que si se trata de un fichero de

titularidad privada, la reclamación se deberá instar en los órganos de la jurisdicción ordinaria.

Se suelen plantear solicitudes de indemnizaciones, en los casos en que una determinada entidad remite los datos de alguno de sus clientes a los ficheros de "morosos". En estos casos, se puede producir una vulneración de la LOPD, así como un daño moral del interesado y una vulneración de su derecho al honor susceptible de indemnización (se trataría de una divulgación, la de la existencia de la deuda, realizada de forma indebida, haciendo que terceros, puedan desmerecer el aspecto de dicha persona como cumplidora de sus obligaciones económicas que asuma frente a terceros). Igualmente, a parte de ese daño moral, se podría derivar un daño material, económico, patrimonial, que sería la imposibilidad de concluir un determinado negocio jurídico, precisamente por la inclusión indebida de sus datos personales en el fichero de morosos.

5.8 Tutela de derechos

El artículo 18 de la LOPD establece que las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la AEPD.

Cuando se deniegue, de forma total o parcial, el ejercicio de sus derechos (acceso, rectificación, cancelación y oposición) puede 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.

Bibliografía

Normativa

- Constitución Española de 2 de diciembre de 1978.
- Convenio de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.
- Directiva 95/46/CE, del Parlamento y del Consejo, 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 de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior.
- 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.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- 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.
- 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.

- Instrucción 1/1998 de 19 de enero, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.
- Instrucción 1/2000, de 1 de diciembre, relativa a las normas por las que se rigen los movimientos internacionales de datos.
- Instrucción 1/2006, de 12 de diciembre, de la Agencia Española de Protección de Datos sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

Recursos web

- Revista de la Agencia de Protección de Datos de la Comunidad de Madrid, en la que se desarrollan importantes aspectos jurídicos y prácticos derivados de la normativa de protección de datos de carácter personal, ofreciendo respuestas jurídicas a problemas derivados de dicha normativa (www.datospersonales.org).
- Página web de la Agencia Española de Protección de Datos de Carácter Personal (www.agpd.es). Se puede encontrar numerosa información acerca de las obligaciones y derechos derivados del tratamiento de datos personales, así como resoluciones, tanto sancionadoras, como de archivo, de los procedimientos que se siguen por dicho organismo.
- Página web de la Agencia de Protección de Datos de la Comunidad de Madrid (www.madrid.org/apdcm).
- Página web de la de la Agencia Vasca de Protección de Datos (www.avpd.euskadi.net/s04-4319/es).
- Página web de Supervisor Europeo de Protección de Datos (www.edps.eu.int).
- Página web del Grupo del artículo 29, de la Comisión Europea (http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm).

OTROS TÍTULOS DE LA SERIE

BUSINESS POCKET

ISBN 978-84-9745-163-5

eLearning easy
Cómo aprovechar la teleformación en la empresa sin meterse en un lío

ISBN 978-84-9745-160-4

Respuesta eficiente al consumidor
Gestione con éxito las relaciones entre fabricantes y distribuidores

ISBN 978-84-9745-095-9

Coaching sobre el terreno
Desarrolle a sus colaboradores y beneficiénse ambos

ISBN 978-84-9745-068-3

Prevención, gestión y resolución de conflictos
Para qué discutir pudiendo arreglarlo a golpes

ISBN 978-84-9745-124-6

Motivar con la acción social
El voluntariado corporativo como herramienta de gestión de personas

netbiblo

ISBN 978-84-9745-083-6

Marketing del ego
Utilice lo ya inventado para venderse mejor

ISBN 978-84-9745-168-0

Gestión de la publicidad
Haga de su empresa de publicidad un buen socio para su empresa

ISBN 978-84-9745-092-8

Dirección de personas
Escuchar, influenciar y desarrollar a los colaboradores

ISBN 978-84-9745-184-0

Marketing relacional
Cree un plan de incentivos eficaz

ISBN 978-84-9745-187-1

La empresa creativa
Una organización diseñada para triunfar

ISBN 978-84-9745-200-7

La gestión de costes en lean manufacturing
Cómo evaluar las mejoras en costes en un sistema lean

ISBN 978-84-9745-195-6

Protocolo y estrategia para PYMES
La imagen y excelencia de los pequeños

ISBN 978-84-9745-194-9

Comunicación con la clientela
Entrevistas con clientes, postventa y reclamaciones

ISBN 978-84-9745-196-3

Aumente su cartera de clientes
Entrevistas con clientes, postventa y reclamaciones

Para títulos de próxima publicación, consulte nuestra web:
www.netbiblo.com

netbiblo