PRODAT
líderes en protección de datos

GUIA BÁSICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Índice

1.1 Introducción

La Constitución Española, en su artículo 18 garantiza el derecho al honor, la intimidad personal y familiar y a la propia imagen. En particular, en su apartado cuarto, establece la necesidad de proteger estos derechos fundamentales, dentro del ámbito relacionado con el uso de la informática. De esta manera, el artículo 18.4 de nuestra Constitución dispone:

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

Como consecuencia de este mandato y para desarrollar el contenido del mismo, se promulgó la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal, más conocida como LORTAD.

En el ámbito europeo, el rápido desarrollo de las técnicas de tratamiento informático fue, igualmente, motivo de preocupación en los Organismos de ámbito internacional. Reflejo de esta preocupación, representa la promulgación del Convenio 108 (28/01/1981) del Consejo de Europa, que tenía como objetivo garantizar el respeto de los derechos y libertades fundamentales del individuo, concretamente su derecho a la vida privada con respecto al tratamiento automatizado de los datos de carácter personal. España ratificó este Convenio el 27 de Enero de 1984.

Posteriormente, se promulgó en el marco de la Unión Europea, la Directiva 95/46/CEE 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, que tenía como objetivo armonizar la legislación de los países miembros de la Unión en materia de protección de datos, garantizando, de esta manera, la protección y el respeto en todos los países de la Unión de este derecho fundamental del individuo, también conocido como "autodeterminación informativa". Para ello, el Parlamento Europeo elaboró la mencionada Directiva, en la que se recogen los principios mínimos de protección que todos los países de la Unión Europea deberían garantizar en su legislación nacional interna.

En cumplimiento de esta Directiva, España promulgó la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD), que supone la transposición de la Directiva 95/46/CE al derecho interno de nuestro país.

Nuestro Tribunal Constitucional en su Sentencia STC 292/2000, de 30 de noviembre, ha singularizado el derecho a la protección de los datos personales como un nuevo derecho fundamental independiente y desvinculado de los derechos fundamentales a la intimidad personal y familiar. Este nuevo derecho fundamental se define como un derecho autónomo consistente en el poder de control y disposición que cada ciudadano tiene de sus datos personales, sean éstos públicos o no.

El Tribunal Constitucional en su sentencia 292/2000, ha venido a reconocer la protección de datos de carácter personal como un derecho constitucionalmente autónomo e independiente a la intimidad, siguiendo así la línea de lo previsto en la Carta de Derechos Fundamentales de la Unión Europea firmada en Niza el 7 de diciembre de 2000, cuyo artículo 8 establece que toda persona tiene derecho a la protección de datos de carácter personal que la conciernen.

Así, el derecho fundamental a la protección de los datos personales presenta ya unos perfiles definidos por la jurisprudencia constitucional:

a) Su objeto va más allá de los datos íntimos, lo que significa que comprende en el ámbito protector del derecho fundamental los datos personales públicos, y en general a todos los que identifiquen o permitan la identificación de una persona.

   En este sentido, 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 (protegida por el artículo 18.1 CE), sino los datos de carácter personal. Asimismo, también alcanza a aquellos datos personales públicos (son accesibles al conocimiento de cualquiera).

   Que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados por este derecho son todos aquellos que identifiquen o permitan la identificación de la persona.

b) El objeto del nuevo derecho fundamental no se limita a los datos personales procesados o almacenados por sistemas informáticos, sino también a cualesquiera otros datos personales.

c) El ejercicio del derecho comporta un conjunto de facultades positivas relativas a la disposición y de control sobre los datos personales. Éstas no se limitan tampoco a garantizar la protección de la intimidad, pues aunque ambos derechos fundamentales –el derecho a la intimidad y el derecho a la protección de los datos personales- persiguen un objetivo común, su función, su objeto y su contenido son diferentes.

d) Estas facultades de disposición y control de los datos se concretan en el derecho a consentir y a conocer su posesión y su uso por parte de terceros (es un derecho fundamental consistente en el ejercicio de control por parte del titular de los datos sobre quién, cómo, para qué, dónde y cuándo son tratados los datos relativos a su persona). Este control y poder de disposición se hace efectivo a su vez a través del ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

Es por ello, que tal y como ha valorado y analizado el Tribunal Constitucional en su sentencia, el derecho fundamental a la protección de datos no puede ser entendido de una forma aislada, sino que debe quedar incardinado con el resto de los derechos fundamentales, sirviendo de límite y siendo limitado igualmente por ellos.

Las consecuencias que se derivan de la cualidad de derecho fundamental son las siguientes:

a) Es un derecho irrenunciable del individuo
b) Su desarrollo debe hacerse a través de Ley Orgánica (requiriendo para su aprobación mayoría absoluta del Congreso de los Diputados)
c) Prevalece sobre el ejercicio de otros derechos no fundamentales
d) Posee una protección reforzada, pudiendo ejercitarse ante los Tribunales Ordinarios por un procedimiento basado en los principios de preferencia y sumariedad, y a través del recurso de amparo ante el Tribunal Constitucional (artículo 53 CE)

La norma que desarrolla este derecho fundamental es la Ley Orgánica 15/1999 (LOPD). Se aplica a los datos de carácter personal registrados en soporte físico y a toda modalidad de uso posterior de esos datos por los sectores público y privado.

Los principios generales de la protección de datos constituyen el eje fundamental de la normativa. Partiendo de ellos, se desarrolla el resto de la regulación de obligado cumplimiento para todo aquél que trate datos de carácter personal y los correspondientes derechos otorgados a la persona titular de los mismos. En consecuencia, cualquier incumplimiento de estos principios o la falta de observancia de los mismos supondrán la comisión de una infracción y la consiguiente sanción por parte de la Agencia Española de Protección de Datos.

El pasado 19 de enero se publicó el Real Decreto 1720/2007, de 21 de diciembre, (en adelante, el "RDLOPD") por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. (en adelante, "LOPD").

El RDLOPD, que entró en vigor el 19 de abril de 2008, comparte con la LOPD la finalidad de hacer frente a los riesgos que para el derecho a la protección de la intimidad pueden suponer el acopio y tratamiento de datos personales.

Su aprobación tiene lugar con la vocación de no reiterar los contenidos de la norma superior y de desarrollar, no sólo los mandatos contenidos en la LOPD de acuerdo con los principios emanados 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 (en adelante, la "Directiva"), sino también aquellos que en estos años de vigencia de la LOPD se ha demostrado que precisaban de un mayor impulso normativo.

Los principales objetivos de éste RDLOPD es pretender dotar de seguridad jurídica al ordenamiento en materia de protección de datos de carácter personal y contribuir resolver las dudas interpretativa existentes así como al logro de una mayor claridad en su aplicación práctica, para lo cual consolida la doctrina y precedentes de la AEPD y la jurisprudencia de los Tribunales en la materia y aborda algunos aspectos (como el de empresas que prestan servicios de solvencia patrimonial y crédito o aquellas dedicadas al marketing) que, durante estos años de vigencia de la LOPD, requerían de una regulación expresa.

Las infracciones en materia de protección de datos aparecen tipificadas en el artículo 44 de la Ley. Se establece una clasificación en infracciones leves, infracciones graves e infracciones muy graves, tipificándose multas que ascienden hasta los 601.000 €.

Infracciones (art. 44 LOPD)		**Sanciones (art. 45 LOPD)**
Infracción Leve		**de 601,01 a 60.101,21 €**
Infracción Grave		**de 60.101,21 a 300.506,05 €**
Infracción Muy Grave		**de 300.506,05 a 601.012,10 €**

Tal y como se ha referenciado, la AEPD es el órgano estatal encargado de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación.

INFRACCIÓN	*Art. 44.2. Son infracciones leves:* *b) No proporcionar la información que solicite la Agencia Española de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.*
SANCIÓN	*Art. 45.1: Multa de 601,01 a 60101,21 €*
INFRACCIÓN	*Art. 44.3. Son infracciones graves:* *i) No remitir a la Agencia Española de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.* *j) La obstrucción al ejercicio de la función inspectora.*
SANCIÓN	*Art. 45.2: Multa de 60101,21 a 300506,05 €*
INFRACCIÓN	*Art. 44.4. Son infracciones muy graves:* *d) No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia Española de Protección de Datos o por las personas titulares del derecho de acceso.*
SANCIÓN	*Art.45.3: Multa de 300506,05 € a 601012,10 €*

De acuerdo con lo establecido en el artículo 41 LOPD, se prevé la creación de Agencias de Protección de Datos autonómicas que ejerzan determinadas funciones en la materia cuando afecte a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local en su ámbito territorial. Así, de una parte, existe una Agencia Española de Protección de Datos con competencias en todo el Estado Español, la Agencia Española de Protección de Datos, y de otra parte, existe una Agencia de Protección de Datos en cada Comunidad Autónoma que lo haya previsto legalmente.

La Comunidad Autónoma de Madrid, fue la primera que adoptó esta iniciativa (en 1995) y creó su propio órgano de control, tal y como dispone la actual Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal de la Comunidad de Madrid. La Agencia de Protección de Datos de la Comunidad de Madrid (en adelante APDCM) ejerce sus funciones respecto a los ficheros cuya responsabilidad está atribuida, básicamente, a Instituciones Autonómicas y Administraciones Públicas Autonómicas y Locales (además de Universidades Públicas y Colegios Profesionales de Madrid).

Las Comunidades Autónomas que no disponen de éste órgano, se encuentran bajo el control y fiscalización de la AEPD hasta su futura creación. En estos momentos, existen Agencias autonómicas, además de en Madrid, en la Comunidad Catalana y en la Comunidad Autónoma Vasca (y existen proyectos de Ley en Galicia y Andalucía).

1.2 Diposiciones generales

1.2.1 Ámbito de aplicación LOPD y RDLOPD 1720/2007

La L.O.P.D. es de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

El RDLOPD incluye dentro de su ámbito de aplicación los ficheros o tratamientos no automatizados (esto es, en soporte papel) o parcialmente automatizados. Particularmente, este nuevo texto regula de modo específico las medidas de seguridad aplicables a los mismos.

Dicha clase de ficheros o tratamientos, si bien no se encontraban excluidos del ámbito de aplicación de la LOPD, contaban con una vacatio legis de doce años a contar desde el 24 de octubre de 1995 para su adecuación a la citada norma (sólo los ficheros preexistentes), motivo por el cual no han quedado estrictamente sujetos a la normativa de referencia hasta el 24 de octubre de 2007. Por otro lado, las previsiones en materia de seguridad contenidas hasta la fecha en el derogado Real Decreto 994/1999, de 11 de junio, sobre las medidas de seguridad aplicables a los ficheros automatizados que contengan datos de carácter personal (en adelante, el "RDLOPD de medidas de seguridad"), no preveía la implantación de medidas de seguridad concretas para ficheros no automatizados.

En otro orden de cosas, el RDLOPD excluye expresamente de su ámbito objetivo de aplicación los tratamientos de datos referidos a personas jurídicas, así como los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas (entendemos que con el objetivo de realizar tratamientos cuya finalidad tenga relación con los cargos que dichas personas están desempeñando), consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.

En cualquier caso, los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la nueva norma en materia de protección de datos personales. Lo anterior ha de entenderse sin perjuicio del régimen previsto por la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información, en virtud del cual es preciso el consentimiento expreso para el envío de comunicaciones comerciales realizadas por correo electrónico o medios de comunicación electrónica equivalente, tanto a personas físicas como jurídicas.

Finalmente, debe destacarse que, no obstante el RDLOPD no sea de aplicación a los datos referidos a personas fallecidas, las personas a él vinculadas (ya sea por consanguinidad o afinidad) podrán dirigirse a los responsables de los ficheros o tratamientos que contengan tales datos personales para solicitar que los mismos sean cancelados.

1.2.2 Computo de plazos

En los supuestos en que este RDLOPD señale un plazo por días se computarán únicamente los hábiles. Cuando el plazo sea por meses, se computarán de fecha a fecha.

1.3 Principios generales de la protección de datos

La Ley orgánica 15/1999, de 13 de diciembre y el RDLOPD 1720/2007, regulan dentro de su título II los principios rectores que deben regir la protección de datos en España. La regulación gira entorno a los siguientes principios básicos que han de ser respetados en todas las fases del tratamiento de los datos, cuando resulten aplicables.

Los tres principios de la protección de datos, información, consentimiento, finalidad - constituyen, lo que se viene denominando por un sector de la doctrina, el eje de la protección de datos.

El conocimiento de los principios de consentimiento, información y finalidad permite adquirir pautas para analizar el resto de derechos y obligaciones que se encuentran reguladas en la normativa de protección de datos.

A efectos sistemáticos, vamos a analizar cada uno de estos principios de forma independiente si bien incluiremos las interrelaciones existentes entre los mismos, y las excepciones a cada uno de ellos, ya que una de las características de nuestra ley de protección de datos y el RDLOPD, es haber creado una rígida política de principios que excepciona de su cumplimiento a una serie de situaciones a las que el legislador ha querido dar un tratamiento especial.

De cada uno de los principios se van a ver las implicaciones normativas y el régimen de excepciones, cuyo conocimiento es fundamental para conocer los márgenes de actuación con los que cuenta el responsable del fichero.

1.3.1 Calidad de los datos (artículo 4 LOPD y 8 del RDLOPD)

Según lo dispuesto en el artículo 4 de la LOPD y 8 del RDLOPD, los datos de carácter personal deben cumplir tres características básicas tanto en el momento de su recogida como para su tratamiento posterior: ser adecuados, pertinentes, no excesivos, y tratados de forma leal y lícita en relación con el ámbito y finalidades legítimas para las que se hayan recabado.
La aplicación de este principio básico conlleva las siguientes consecuencias:

- Los datos obtenidos no podrán usarse para finalidades incompatibles con aquéllas para las que fueron recogidos. En este caso, el término incompatible debe ser interpretado como *distinto*, según lo dispuesto en la sentencia del Tribunal constitucional 292/2000, de 30 de noviembre.
- Los datos deberán ser exactos y puestos al día, respondiendo con veracidad a la situación actual del interesado. Esto significa que no podrán permanecer en el fichero por un tiempo superior al necesario para conseguir la finalidad para la que se recabaron. Si no son exactos, están incompletos, o dejan de ser necesarios o pertinentes, deberán ser cancelados o sustituidos por los correctos.

- Podrán ser conservados una vez dejen de ser útiles para la función prevista en los siguientes casos :

  - ✓ Cuando se decida su mantenimiento por valores históricos, científicos o estadísticos. "*Para la determinación de los fines a los que se refiere el párrafo anterior se estará a la legislación que en cada caso resulte aplicable y, en particular, a lo dispuesto en la Ley 12/1989, de 9 de mayo, reguladora de la Función Estadística Pública, la Ley 16/1985, de 25 junio, del Patrimonio Histórico Español y la Ley 13/1986, de 14 de abril de Fomento y Coordinación General de la Investigación Científica y Técnica, y sus respectivas disposiciones de desarrollo, así como a la normativa autonómica en estas materias".*
  - ✓ En atención al cumplimiento de obligaciones establecidas en la legislación específica prevista al efecto (obligaciones administrativas, fiscales, seguros, etc.). Se trata del denominado plazo o período de *bloqueo de datos* que lleva implícita la cancelación de los mismos en la mayoría de situaciones.

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

En resumen, dicho principio, lo que salvaguarda y protege es que la información que se obtenga y trate deberá ser adecuada, pertinente y no excesiva en relación con el ámbito y las finalidades determinadas, explicitas y legítimas para las que se haya obtenido; no podrán usarse los datos para una finalidad distinta, deberán ser exactos y puesto al día, respondiendo con veracidad a la situación actual del afectado debiendo a estos efectos ser corregidos de oficio, y además serán cancelados cuando dejen de ser necesarios para la finalidad para la que fueron recabados. Es decir, no se recabará más información de la necesaria para cumplir con la finalidad legítima del tratamiento.

INFRACCIÓN	*Art. 44.3. Son infracciones graves:* *d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.* *f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.*
SANCIÓN	*Art. 45.2: Multa de 60101,21 a 300506,05 €*
INFRACCIÓN	*Art. 44.4. Son infracciones muy graves:* *a) La recogida de datos en forma engañosa y fraudulenta.* *f) Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.*
SANCIÓN	*Art.45.3: Multa de 300506,05 € a 601012,10 €*

1.3.2 Derecho de información en la recogida de datos (artículo 5 LOPD)

De acuerdo con el artículo 5 LOPD, en el momento de la recogida de los datos personales se deberá informar al interesado de modo expreso, preciso e inequívoco de las siguientes circunstancias:

- De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
- Del carácter obligatorio o facultativo de su respuesta a las preguntas que le sean planteadas.
- De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
- De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- De la identidad o dirección del responsable del tratamiento o, en su caso, de su representante, en el caso de que el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento medios situados en territorio español.

En todo caso será necesario que exista conocimiento. A pesar de tener el consentimiento, sin el conocimiento, el tratamiento no sería leal. Según lo dispuesto en el Considerando 38 de la Directiva 95/46/CE del Parlamento Europeo y el 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 tratamiento leal de los datos supone que los interesados deben estar en condiciones de conocer la existencia de los tratamientos y, cuando los datos se obtengan de ellos mismos, contar con una información precisa y completa respecto a las circunstancias de dicha obtención. El problema surge en los casos en los que no es posible informar. Como solución se plantea la publicación de forma que el interesado esté en "*condiciones de conocer*". Este tratamiento leal también entra dentro de las exigencias normativas al establecer la Ley en el principio anteriormente analizado, que no podrán ser recabados los datos por "*medios fraudulentos, desleales o ilícitos*".

Este principio únicamente queda excepcionado si se da alguna de las siguientes circunstancias, establecidas en la LOPD de forma taxativa:

- Cuando lo establezca expresamente una Ley,
- 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 Española de Protección de Datos, en consideración del número de interesados, la antigüedad de los datos y las posibles medidas compensatorias.
- Cuando los datos procedan de fuentes accesibles la público y se destinen a la actividad de publicidad o prospección comercial. En este último 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.

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

A. del contenido del tratamiento
B. de la procedencia de los datos
C. de la existencia de un fichero o tratamiento
D. de la finalidad de la recogida
E. de los destinatarios de la información
F. de la posibilidad de ejercitar sus derechos
G. de la identidad y dirección del responsable del tratamiento o, en su caso de su representante.

Este derecho, como norma general, se deberá cumplir siempre, con independencia de que sea necesario o no la prestación del consentimiento por el afectado para el tratamiento de sus datos, dado que dicho consentimiento puede no ser necesario por estar sometido al régimen de excepciones.

Esta información debe estar incluida en los cuestionarios o impresos de recogida de datos. En el caso de utilizar internet como medio de recogida de los datos, también debe de facilitarse esta información a los usuarios que registran sus datos y debe de hacerse de modo que la información sea siempre previa al tratamiento. Además es recomendable que en el texto informativo resulte lo más claro y legible posible. En el caso de los menores de edad el RDLOPD exige que la información se exprese en un leguaje que sea fácilmente comprensible.

Cuando los datos se recojan directamente de los afectados, la información deberá facilitarse con carácter previo a la recogida de los datos.

No obstante apuntar, a modo de ejemplo, que al igual que el principio del consentimiento, este derecho también tiene una régimen de excepciones en virtud de las cuales existen determinadas situaciones en las que la ley exime del deber de información sobre algunos de estos aspectos cuando se deduzcan inequívocamente de la naturaleza de los propios datos y de las circunstancias en las que se produce la recogida. En algunos casos esta información, no es previa, sino posterior al tratamiento, así citar como ejemplo, el tratamiento de datos con fines de publicidad, prospección comercial o venta directa cuando los datos figuren en fuentes de acceso público regulado en el artículo 30 LOPD.

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

Se permite para el almacenamiento de los soportes, utilizar medios informáticos o telemáticos. En particular podrá proceder al escaneado de la documentación en soporte papel, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los soportes originales.

INFRACCIÓN	*Art. 44.2. Son infracciones leves:* *d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley.*
SANCIÓN	*Art. 45.1: Multa de 601,01 a 60101,21 €*
INFRACCIÓN	*Art. 44.3. Son infracciones graves:* *l) Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado.*
SANCIÓN	*Art.45.2: Multa de 60101,21 a 300506,05 €*
INFRACCIÓN	*Art. 44.4. Son infracciones muy graves:* *I) No Atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.*
SANCIÓN	*Art.45.3: Multa de 300506,05 € a 601012,10 €*

1.3.3 Consentimiento del interesado (artículo 6 LOPD)

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

Este consentimiento se podrá otorgar en cualquiera de las formas admisibles en Derecho. Salvo para aquellos casos en que la LOPD prevé que el consentimiento ha de otorgarse expresamente, puede establecerse de forma tácita. Además, el consentimiento así otorgado podrá revocarse en cualquier momento por causa justificada, sin que se atribuyan efectos retroactivos a dicha revocación.

Para que este consentimiento sea válido, como hemos expuesto en el principio relativo a la calidad de los datos, debemos tener en cuenta que la LOPD requiere que los datos no se recaben por medios fraudulentos, desleales o ilícitos.

En el tratamiento de datos especialmente protegidos, la Ley exige una serie de garantías adicionales. Requerirá un tipo de consentimiento u otro dependiendo del tipo de datos de que se trate.

El nivel de protección máxima lo establece la Ley para los datos referentes a ideología, afiliación sindical, religión y creencias. De acuerdo con el régimen establecido por la LOPD, nadie podrá ser obligado a declarar sobre estos datos. El propio interesado deberá consentir expresamente y por escrito. Además, existe una obligación de advertir al interesado sobre su derecho a no prestar su consentimiento (derivado del artículo 16 CE).

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

Sin el consentimiento del interesado, sólo podrán ser objeto de tratamiento datos sobre ideología, afiliación sindical, religión, creencias, salud, vida sexual y origen racial cuando sean absolutamente necesarios para los fines de una investigación concreta realizada por las Fuerzas y Cuerpos de Seguridad.

Con carácter general, establece la LOPD la prohibición de crear o mantener ficheros con la finalidad exclusiva de almacenar datos que revelen la ideología, religión, creencias, origen racial o vida sexual.

Por último, los datos relativos a comisión de infracciones penales o administrativas, únicamente podrán incluirse en los ficheros públicos por las Administraciones competentes de acuerdo con lo previsto en sus normas reguladoras.

La LOPD establece taxativamente aquellos casos en los que no es necesario el consentimiento del interesado para el tratamiento de datos de carácter personal:

- Cuando una Ley disponga otra cosa,
- Cuando los datos de carácter personal se recojan de fuentes accesibles al público, siempre que los datos provengan de ficheros de titularidad privada.
- Cuando se recojan para el ejercicio de las funciones propias de las Administraciones públicas.
- Cuando se refieran a personas vinculadas por una relación negocial, laboral, administrativa o un contrato o precontrato siempre que sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del mismo, o para proteger su interés vital.
- Que el tratamiento sea necesario para la protección de un interés vital del interesado (prevención o diagnóstico médico, prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios).

De las características del consentimiento no se infiere necesariamente su carácter expreso en todo caso, razón por la cual en aquellos supuestos en que el legislador ha pretendido que el consentimiento deba revestir ese carácter, lo ha indicado expresamente. Por tanto, el consentimiento podrá ser tácito, en el tratamiento de datos que no sean especialmente protegidos (artículo 7.2 y 7.3 LOPD) si bien para que ese consentimiento tácito pueda ser considerado inequívoco será preciso otorgar al afectado un plazo de 30 días para que pueda claramente tener conocimiento de que su omisión de oponerse al tratamiento implica un consentimiento al mismo, no existiendo al propio tiempo duda alguna de que el interesado ha tenido conocimiento de la existencia del tratamiento y de la existencia de ese plazo para evitar que se proceda al mismo.

El principio del consentimiento es el pilar central o piedra angular que enmarca la protección de datos. Lo que trata de proteger este principio como idea principal es, que toda la información relativa a cada individuo no puede salir de su entorno particular, de su vida privada, y ser utilizada por terceros, sin su consentimiento, sin su voluntad. En definitiva, toda la información (datos) de una persona, le pertenece a ella, y únicamente ella tendrá el poder de decisión sobre quien puede, o no, conocerlos y con qué finalidad.

En este sentido, para poder tratar la información personal de una persona, así como para poder ceder dicha información a terceros, será necesario su consentimiento

expresado de forma libre, inequívoca, específica e informada. Así lo establecen los artículos 6 y 11 de la LOPD, en relación con la definición del consentimiento contenida en el artículo 3 h) del mismo texto legal.

INFRACCIÓN	*Art. 44.3. Son infracciones graves:* *c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en los que éste sea exigible.*
SANCIÓN	*Art. 45.2: Multa de 60101,21 a 300506,05 €*
INFRACCIÓN	*Art. 44.4. Son infracciones muy graves:* *c) Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7.*
SANCIÓN	*Art.45.3: Multa de 300506,05 € a 601012,10 €*

1.3.4 Obtención del Consentimiento del interesado y el deber de información (Capitulo II. "consentimiento para el tratamiento de datos y deber de información del RDLOPD)

Con relación a la exigencia de obtener el consentimiento del afectado o interesado para efectuar el tratamiento de sus datos personales, merece especial atención el hecho de que el nuevo RDLOPD incluye dos nuevas excepciones: cuando el tratamiento o cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o cesionario o cuando sean necesarios para el cumplimiento de un deber jurídico, en ambos casos amparados por una norma con rango de Ley o de Derecho Comunitario.
Salvo cuando sea necesario el consentimiento expreso, el consentimiento puede recabarse dirigiéndose al afectado y concediéndole un plazo de 30 días para manifestar su negativa al tratamiento. Por otra parte, para asegurar el correcto cumplimiento de esta disposición, paralelamente se exige al responsable comprobar que la comunicación en la que se pone en conocimiento del afectado o interesado que se está procediendo al tratamiento de sus datos personales, no ha sido objeto de devolución. Al mismo tiempo, se obliga al responsable a facilitar un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos (por ejemplo, mediante un envío prefranqueado, una llamada a un número de teléfono gratuito o a los servicios de atención al cliente de los que disponga el responsable).

No podrá solicitarse nuevamente el consentimiento del interesado respecto de los mismos tratamientos y para las mismas finalidades en el plazo de un año a contar de la fecha de la anterior solicitud.

El responsable que haya solicitado el consentimiento del afectado durante el proceso de formación en un contrato para finalidades que no guarden relación directa con la relación contractual, deberá permitir al afectado que manifieste expresamente su

negativa al tratamiento o cesión de datos. En particular, esta obligación se entiende satisfecha si se le permite al afectado la marcación de una casilla o un procedimiento equivalente que le permita manifestar su negativa al tratamiento.

En particular, cuando se trate de responsables que presten al afectado un servicio que genere información periódica o reiterada, o facturación periódica, la comunicación podrá llevarse a cabo de forma conjunta a esta información o a la facturación del servicio prestado, siempre que se realice de forma claramente visible.

En el caso de los menores de edad hay que distinguir entre los mayores de catorce años que puedan prestarlo, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela, y los menores de catorce, caso que requerirá el consentimiento de los padres o tutores.

1.3.5 Deber de secreto (artículo 10 LOPD)

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

En la práctica, este principio implica que las personas que deban operar sobre los ficheros, o tengan acceso a datos personales, aunque sólo sea a modo de consulta, deberán estar sometidos por medidas o normas estrictas de conducta relativas al mantenimiento de la confidencialidad (compromiso de confidencialidad) en el desempeño de su labor diaria (por ejemplo, personal del Departamento de RR.HH., Comercial, etc.).

Asimismo, el nuevo RDLOPD establece que aquellas personas que vayan a prestar servicios en las instalaciones del responsable del fichero (ej. personal de limpieza) y no deban acceder a la información deberán asegurarse la confidencialidad, respecto a la información que pudieran tener acceso por la prestación de los mismos.

Por otra parte, el Código Penal ha tipificado en su artículo 197 el delito de apoderamiento o uso sin consentimiento de ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado, de modo que, exista o no infracción de LOPD, cabrá plantear la existencia de un delito.

INFRACCIÓN	*Art. 44.2. Son infracciones leves:* *e) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave.*
SANCIÓN	*Art. 45.1: Multa de 601,01 a 60101,21 €*

INFRACCIÓN	*Art. 44.3. Son infracciones graves:* *g) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.*
SANCIÓN	*Art. 45.2: Multa de 60101,21 a 300506,05 €*
INFRACCIÓN	*Art. 44.4. Son infracciones muy graves:* *g) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.*
SANCIÓN	*Art.45.3: Multa de 300506,05 € a 601012,10 €*

1.3.6 Cesión o Comunicación de datos y supuestos que lo legitiman (artículo 11 LOPD y 10 del RDLOPD)

La comunicación de datos es un punto conflictivo, cuando se trata de proteger los datos de carácter personal, debido a que mediante la cesión de datos a otros ficheros se posibilita el cruce de los mismos, desarrollando todas las posibilidades de tratamiento de información que permite la informática. Además, a través de la comunicación de datos se suele incurrir en el error de la utilización de los datos con otro uso o finalidad distinta para el que se habían recabado.

En el artículo 11 LOPD se establecen las condiciones en las que podrá o no realizar la cesión o comunicación de datos de carácter personal, determinando, que sólo se podrán ceder datos de carácter personal "para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario".

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

No obstante lo anterior, existen en la vida cotidiana muchas situaciones donde no podrían realizarse las cesiones de datos con los mencionados requisitos del consentimiento previo. Así, por ejemplo, no podría accederse a información clínica de un accidentado para atenderle de urgencia y salvarle la vida, no podría accederse por la Agencia Tributaria a los datos de las nominas o datos patrimoniales de los ciudadanos para realizar una inspección sin su consentimiento etc.

En la LOPD y en el RDLOPD se establecen excepciones a este principio determinando los casos en los que no es necesario dicho consentimiento (excepciones a la regla general del consentimiento):

a) Lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los supuestos siguientes:

- El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre.
- El tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas.

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

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

c) Los datos de carácter personal podrán cederse sin necesidad del consentimiento del interesado cuando:

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

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

c) El tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del apartado 6 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre.

d) Será posible la cesión de los datos de carácter personal sin contar con el consentimiento del interesado cuando:

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

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

c) La cesión entre Administraciones públicas cuando concurra uno de los siguientes supuestos:

- Tenga por objeto el tratamiento de los datos con fines históricos, estadísticos o científicos.
- Los datos de carácter personal hayan sido recogidos o elaborados por una Administración pública con destino a otra.

- La comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias.

5. Los datos especialmente protegidos podrán tratarse y cederse en los términos previstos en los artículos 7 y 8 de la Ley Orgánica 15/1999, de 13 de diciembre.

En particular, no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

El responsable del fichero o tratamiento deberá informar al titular en el momento en que efectúe la primera cesión indicando la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario. No será necesario informar de esta cesión cuando venga impuesta por una Ley, cuando se trate de una cesión sin consentimiento basada en la existencia de una relación jurídica previa que la justifique, cuando el destinatario sea el Ministerio Fiscal, los jueces y Tribunales, el Defensor del pueblo o el Tribunal de Cuentas, o sus análogos autonómicos, ni cuando se trate de cesiones entre Administraciones Públicas con fines históricos o estadísticos.

Interesa señalar que, respecto a un grupo empresarial, entendiendo que la vinculación que puede existir entre las sociedades que integran un mismo grupo empresarial no puede ser tenida en consideración respecto al tema de inscripción de ficheros y al análisis de las circunstancias que concurren en una cesión de datos.

En definitiva, debe entenderse que la existencia de un grupo de empresas no impide que cada una de las sociedades integradas en el mismo mantenga diferenciada y plena su personalidad jurídica. Por tanto, a todos los efectos jurídicos, la circunstancia de que una sociedad esté participada por otra no afecta al hecho de que cada una de ellas tenga su propia personalidad jurídica, de modo que cada empresa integrante será responsable del fichero o tratamiento de cada uno de sus ficheros con datos de carácter personal (tal y como se regula en la definición del artículo 3.d) LOPD): *"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.".* En resumen, lo anteriormente expuesto significa que cada empresa deberá inscribir sus ficheros de manera independiente ante la Agencia Española de Protección de Datos y las comunicaciones de datos entre ellas constituirán una cesión de datos del artículo 11.

Se introduce en el nuevo RDLOPD el supuesto de la modificación del responsable del fichero, como consecuencia de una operación de fusión, escisión, cesión global de activos y pasivos etc. indicando que no se producirá cesión de datos. No obstante, no exime del deber de informar al interesado del cambio del nuevo responsable del fichero.

INFRACCIÓN	*Art. 44.4. Son infracciones muy graves:* *b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.*
SANCIÓN	*Art.45.3: Multa de 300506,05 € a 601012,10 €*

1.3.7 Acceso a los datos por cuenta de terceros (artículo 12 LOPD y 20 del RDLOPD)

La relación contractual que se contempla en el artículo 12 LOPD y 20 del RDLOPD, es la de un arrendamiento de servicios (contrato por el que una persona se compromete a prestar algún servicio a otra a cambio de un precio), donde su característica principal es que quien los presta actúa por cuenta de quien lo encarga, de modo que el riesgo o beneficio de los resultados del servicio siempre recaerá sobre el arrendatario (quien encarga el servicio). Es decir, lo esencial de este contrato es que el responsable del fichero (arrendatario de los servicios), continúa teniendo la dirección y la responsabilidad del tratamiento, de modo que el encargado del tratamiento (o arrendador de los servicios) sólo está legitimado para realizar aquello que se le encomienda por medio del contrato.

la figura del *"encargado del tratamiento"*, definido en el artículo 3g) LOPD y 5 k) del RDLOPD, como la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del inicial responsable (se estima que el prestador de servicios del artículo 12 LOPD es una modalidad de la figura del encargado del tratamiento).

No se considerará comunicación siempre que el acceso sea necesario para la prestación de un servicio al responsable del tratamiento. No obstante, en todo caso, dicha prestación tendrá que estar regulada en un contrato, por escrito o en alguna otra forma que permite acreditar su celebración y contenido, que establezca expresamente los siguientes aspectos:

- Que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento.
- Que el encargado del tratamiento no aplicará o utilizará los datos con fin distinto al que figure en dicho contrato.
- Que el encargado del tratamiento no comunicará los datos, ni siquiera para su conservación, a otras personas.
- Las medidas de seguridad a las que se refiere el artículo 9 de la LOPD que el encargado del tratamiento está obligado a implementar, y que están recogidas en el art. 81 del RDLOPD.
- Que una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

  Art. 22 del RDLOPD, "1.- No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.

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

En caso de incumplimiento de las estipulaciones del contrato, el encargado del tratamiento será responsable de las infracciones en que hubiera incurrido personalmente.

Así, como el acceso del prestador de servicios no supone una cesión o comunicación de datos del artículo 11 LOPD, no le será aplicable el artículo 11.5. LOPD, en el sentido que el tercero no se encuentra sometido a la Ley, salvo en las especificaciones marcadas por el artículo 12 del mismo texto legal.

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

El problema más frecuente y riesgo más grave que se ha planteado en la práctica es la del uso ilegítimo de los datos por parte del encargado que presta el servicio, que se sirve de los datos para cederlos o alquilarlos en su propio beneficio, sin el consentimiento del responsable del fichero.

Tal y como se ha analizado, el supuesto de deslealtad del prestador del servicio, está previsto en el artículo 12.4. LOPD Y 20.3 del RDLOPD, al establecer que, en tal caso, el prestador del servicio (encargado del tratamiento) será considerado como responsable del fichero y, en caso de denuncia ante la Agencia Española de Protección de Datos por uso no previsto ni autorizado, la única responsabilidad que podrá exigirse será frente al encargado del tratamiento desleal.

En todo caso, siempre podrán exigirse responsabilidades por parte del responsable del fichero frente al encargado del tratamiento por el incumplimiento del contrato, exigiéndose tanto la indemnización de los daños que pudieran derivarse del uso ilegítimo, como del lucro cesante, los beneficios obtenidos o debidos percibir por parte del encargado en los usos que realizó ilegalmente.

La falta de regulación en un contrato de prestación de servicios con los requisitos que de forma expresa deben estipularse para el acceso a los datos por cuenta de terceros, de acuerdo con lo establecido en el mencionado artículo, supone la comisión de una infracción grave para la entidad tercera que presta el servicio (prestador de servicios) por tratar datos sin consentimiento del titular, e infracción muy grave para la entidad a la que se presta el servicio (responsable del fichero) por realizar una cesión de datos sin el consentimiento del titular.

Se traslada al responsable del tratamiento la obligación de velar por que el encargado reúna las garantías para el cumplimiento de la normativa de protección de datos de carácter personal.

Se permite, asimismo, que el encargado del tratamiento conserve bloqueados los datos a los que ha tenido acceso en tanto pudieran derivarse responsabilidades de su relación con el responsable.

Se introduce en el nuevo RDLOPD la posibilidad de la subcontratación de los servicios, recogiéndose, expresamente la necesidad de obtención de autorización para la subcontratación y siempre y cuando se cumplan además, los siguientes requisitos:

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

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

c) Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior 20 del RDLOPD.

En este caso, el subcontratista será considerado encargado del tratamiento, siéndole de aplicación lo previsto en el artículo 20.3 de este RDLOPD.

Si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del tratamiento los extremos señalados en el apartado anterior.

Así, por un contrato de prestación de servicios donde no se refleje los requisitos señalados por el artículo 12 LOPD y 21 del RDLOPD (caso de subcontratación), o no se encontrase recogido en un contrato, supondría por un solo dato de carácter personal objeto de dicha prestación de servicios:

- Para el Responsable del fichero una sanción multa de 300506,05 € a 601012,10 €.
- Para los encargados del tratamiento (empresas prestadoras del servicios) una sanción con multa de 60101,21 € a 300506,05 €.

1.4 Ejercicio de derechos

Como complemento de los principios analizados, la LOPD establece una serie de derechos del titular de los datos, que representan la concreción individual de los principios enunciados. Se garantiza a las personas los derechos para que puedan acceder, rectificar, cancelar y oponerse al tratamiento de la información que les afecte.

Así, dentro de los derechos incluidos en la LOPD, deben distinguirse dos tipos de derechos: los derechos que constituyen el contenido esencial del derecho fundamental a la protección de datos, de acuerdo con la doctrina del Tribunal Constitucional (derecho de acceso, rectificación, cancelación y oposición); y por otro lado, el derecho a impugnación, el derecho a indemnización y el derecho a la consulta del Registro General de Protección de Datos.

El derecho fundamental a la protección de los datos de carácter personal persigue garantizar a la persona un poder de control y disposición sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad derecho del afectado. Dicho poder de disposición y control se concreta jurídicamente en la facultad de consentir su recogida, la obtención, el acceso a los datos personales y su rectificación y cancelación cuando los datos no sean exactos o hayan dejado de ser necesarios para la finalidad para la cual fueron recabados. La regulación de tales derechos se encuentra estipulada en los artículos 15, 16, 23 y 24 LOPD, artículos 23 al 36 del RDLOPD.

Además de los derechos de acceso, rectificación, cancelación y oposición que a continuación se detallan, se reconoce a las personas los derechos de consulta al Registro General de Protección de Datos consistente en la posibilidad de acudir a dicho registro para obtener información sobre los ficheros tanto de naturaleza pública como privada inscritos en él (el nombre del responsable del fichero y la finalidad del mismo), y el de impugnación de valoraciones, que permite impugnar las decisiones que tengan efectos jurídicos, basadas únicamente en una evaluación de sus características o personalidad resultado de un tratamiento de datos de carácter personal. Asimismo, podrán ser impugnados "*los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento*" si el único fundamento es un perfil obtenido a través del tratamiento de sus datos (art. 36 del RDLOPD).

El ejercicio de los derechos tiene carácter de personalísimo (sólo pueden ser ejercitados por el titular), no pudiendo ejercerlos una persona en nombre de otra, excepto cuando lo

realice el representante legal del interesado en dos supuestos tasados: cuando éste se encuentre en una situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de los mismos (artículo 23 del RDLOPD) y gratuitos (no se podrá cobrar por atender el ejercicio de los derechos)

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

- El procedimiento para el ejercicio de derechos se regula en el art. 25 del RDLOPD. Dicho precepto establece que el ejercicio de los derechos deberá llevarse a cabo:

  a) Nombre y apellidos del interesado; fotocopia de su documento nacional de identidad, o de su pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación. La utilización de firma electrónica identificativa del afectado eximirá de la presentación de las fotocopias del DNI o documento equivalente.

  El párrafo anterior se entenderá sin perjuicio de la normativa específica aplicable a la comprobación de datos de identidad por las Administraciones Públicas en los procedimientos administrativos

  b) Petición en que se concreta la solicitud.

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

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

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

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

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

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

1.4.1 Derecho de acceso

El Derecho de acceso, regulado en el artículo 15 LOPD y 27 del RDLOPD, consiste básicamente, en la posibilidad que tiene el interesado de dirigirse al titular del fichero para solicitar y obtener gratuitamente información sobre sus datos de carácter personal que están siendo sometidos a tratamiento, sobre su origen y las comunicaciones realizadas o que se prevean realizar de los mismos.

El derecho de acceso se ejercerá mediante petición o solicitud dirigida al responsable del fichero, formulada por cualquier medio que garantice la identificación del afectado y en la que conste el fichero o ficheros a consultar (artículo 27 del RDLOPD).

El afectado podrá optar por uno o varios sistemas de consulta, siempre que la configuración e implantación material del fichero lo permita. Así, ésta información se podrá obtener mediante:

1. Al ejercitar el derecho de acceso, el afectado podrá optar por uno o varios de los siguientes sistemas de consulta del fichero:

a) Visualización en pantalla.

b) Escrito, copia o fotocopia remitida por correo, certificado o no.

c) Telecopia.

d) Correo electrónico u otros sistemas de comunicaciones electrónicas.

e) Cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable.

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

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

- Los datos de base del afectado y los resultantes de cualquier elaboración o proceso informático.
- 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.

El Responsable del fichero deberá adoptar las medidas necesarias 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 este sentido, el responsable del fichero está obligado a proporcionarle la información de forma gratuita en el plazo máximo de un mes, a contar desde la recepción de la solicitud. Si en este plazo no se ha resuelto de forma expresa, se entenderá que la solicitud ha sido denegada. En el supuesto de que la solicitud fuera estimatoria, el acceso se hará efectivo en el plazo de los diez días siguientes a la notificación de aquella (artículo art. 29.1 del RDLOPD).

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

Este derecho podrá ejercitarse a intervalos no inferiores a doce meses salvo que se acreditase un interés legítimo por parte del interesado, pudiendo en este caso

ejercitarse antes. A excepción de la limitación temporal referenciada, únicamente se denegará el acceso cuando la solicitud sea formulada por persona distinta del afectado.

1.4.2 Derecho de rectificación y cancelación

La LOPD establece en su artículo 16 LOPD y 32.2. del RDLOPD, que "*el responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días*".

El titular de los datos podrá ejercitar estos derechos cuando los datos sean inexactos, o incompletos o cuando el tratamiento a que están siendo sometidos no se ajuste a lo dispuesto en la LOPD (en particular cuando tales datos resulten inadecuados o excesivos).

También el responsable del fichero podrá modificar por propia iniciativa los datos que resulten incompletos o inexactos, tal y como establece el artículo 4 LOPD (principio de calidad de datos).

El derecho del ciudadano a ejercer sus derechos de rectificación y cancelación, no implica que el titular del fichero tenga la obligación de rectificar o cancelar los datos. Únicamente tendrá que hacerlo, en el caso de que efectivamente proceda su rectificación o cancelación. No obstante, cuando se trate de datos que reflejen hechos constatados en un procedimiento administrativo, aquellos se consideran exactos siempre que coincidan con estos.

La solicitud de rectificación deberá indicar el dato que es erróneo y la corrección que debe realizarse y deberá ir acompañada de la documentación justificativa de la rectificación solicitada, salvo que la misma dependa exclusivamente del consentimiento del interesado. En cuanto a la solicitud de cancelación, el interesado deberá indicar si revoca el consentimiento del otorgado en los casos en que la revocación proceda.

Una vez recibida la solicitud, el responsable del fichero puede estimarla o no. En el caso de que la estime deberá hacer efectivo la cancelación o rectificación en el plazo de 10 días desde la recepción de la solicitud. En el supuesto de que considere que no procede a la cancelación o rectificación solicitada por el interesado, deberá comunicárselo motivadamente dentro del mismo plazo de 10 días. Si transcurridos 10 días desde la recepción de la solicitud el responsable del fichero no se pronuncia al respecto de forma expresa se entenderá desestimada.

Además, la cancelación no supone su eliminación o el borrado, sino el bloqueo, ya que en caso de posterior conflicto pueden ser requeridos.

Las entidades afectadas deberán proceder al bloqueo de todos aquellos datos de carácter personal incluidos en sus sistemas de información que hayan dejado de ser necesarios al fin para el que fueron recabados o registrados y proceder a su cancelación definitiva una vez cumplidos los plazos de prescripción derivados de las obligaciones o responsabilidades nacidas del tratamiento. Por tanto, quedarán a disposición de las Administraciones públicas y Tribunales durante el plazo de prescripción previsto para la exigencia de responsabilidades nacidas del tratamiento de los datos. Una vez transcurrido dicho plazo deberán suprimirse.

Si los datos rectificados o cancelados hubieran sido comunicados o cedidos previamente, el responsable del tratamiento deberá notificar en el mismo plazo de 10 días, la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso

de que se mantenga el tratamiento por este último, que deberá también proceder a la rectificación y cancelación.

1.4.3 Derecho de oposición

Supone el derecho del interesado a que sus datos no lleguen a ser tratados con una finalidad determinada o introducidos en un fichero. En la legislación sobre protección de datos puede distinguir dos clases de derecho de oposición:

A. Una que se refiere a la posibilidad que los titulares tienen a oponerse a que sus datos sean tratados con la finalidad de marketing y prospección comercial.

B. La segunda se refiere a los supuestos en que no siendo necesario el consentimiento de los afectados para el tratamiento de sus datos, el interesado se podrá oponer al tratamiento de sus datos cuando existan motivos fundados y legítimos relativos a una concreta situación personal, siempre que la Ley no disponga lo contrario.

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

Este derecho se tramita igual que el resto de derechos, en cuanto a la forma de solicitarlo.

Cuando en el derecho de oposición no sea necesario el consentimiento del afectado para el tratamiento, en la solicitud deberán hacerse constar los motivos fundados y legítimos, relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho.

El responsable del fichero resolverá sobre la solicitud de oposición en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición, ésta podrá entenderse desestimada a los efectos de la interposición de la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

Ejemplos de derecho de oposición: oposición a que los datos de dirección y teléfono de un abonado no figure en la guía telefónica, o que los datos registrados en el padrón municipal no consten en el futuro censo promocional.

INFRACNCIÓ	*Art. 44.2. Son infracciones leves:* *a) No atender por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.*
SANCIÓN	*Art. 45.1: Multa de 601,01 a 60101,21 €*
INFRACCIÓN	*Art. 44.3. Son infracciones graves:* *e) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.*

SANCIÓN	*Art. 45.2: Multa de 60101,21 a 300506,05 €*
INFRACCIÓN	*Art. 44.4. Son infracciones muy graves:* *h) No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.*
SANCIÓN	*Art.45.3: Multa de 300506,05 € a 601012,10 €*

1.4.4 Otros Derechos del afectado

Tal y como ha sido referenciado, el titular interesado dispone de otros derechos reconocidos por la normativa. A continuación, se reflejan los más significativos:

- Derecho de Impugnación de valoraciones:

  La LOPD establece en su artículo 13, el derecho de impugnación del interesado a determinados actos. En concreto, impugnar aquellas decisiones que tengan efectos jurídicos y cuya base sea únicamente un tratamiento de datos de carácter personal que ofrezca una definición de sus características o de su personalidad.

- Derecho de consulta al Registro General:

  El derecho de consulta al Registro General de Protección de Datos, regulado en el artículo 14 LOPD, permite al interesado cuyos datos hayan sido objeto de tratamiento, proceder a recabar información del Registro General de Protección de Datos (de la Agencia Española de Protección de Datos) relativa a conocer la existencia de tratamientos de datos de carácter personal, la finalidad del mismo y la identidad del responsable del fichero. Dicho Registro se configura legalmente como de consulta pública y gratuita, no existiendo limitación alguna para las consultas efectuadas por parte del interesado.

  La información existente en el Registro se limita a determinadas características de los ficheros: su identificación, quien es el responsable del mismo, donde se ubican y el tipo de datos que tratan, entre otras.

  Actualmente, la Agencia Española de Protección de Datos ha habilitado la posibilidad de consultar el registro a través de su web site (www.agpd.es) en Internet.

  Este derecho es ejercitable también ante el Registro de Datos Personales perteneciente a la Agencia de Protección de Datos de la Comunidad de Madrid (APDCM), aunque la LOPD se refiere únicamente al Registro General de Protección de Datos. La información, en este caso, se limitará al ámbito competencial del Órgano autonómico.

- Derecho de indemnización:

  El artículo 19 LOPD establece para los interesados, que como consecuencia del incumplimiento de lo prescrito en la normativa por parte del responsable del fichero o por el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos

tienen derecho a ser indemnizados. Para obtener dicha indemnización, cuando el incumplimiento provenga de ficheros de titularidad privada, deberán ejercitar la correspondiente acción ante los órganos de la jurisdicción ordinaria, y cuando el incumplimiento provenga de un fichero de titularidad pública, la responsabilidad se exigirá conforme a lo dispuesto en la legislación reguladora del régimen de responsabilidad de las Administraciones públicas.

1.4.5 Ejercicio de derechos ante un encargado del tratamiento. (art. 26 RDLOPD).

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

1.5 Tratamiento para actividades de publicidad y prospección

Ya ha sido comentado en el principio del consentimiento que junto al principio de finalidad e información, son el eje sobre el que gira toda la regulación de protección de datos. La regulación del consentimiento se consolida a su vez en tres de los principios regulados en el Titulo II de la LOPD y del RDLOPD que son:

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

Por ello, antes de utilizar los datos con finalidad de publicidad, (proveedores, clientes...) deberá comprobarse siempre, que se ha recabado el consentimiento de los afectados o que provienen de fuentes de acceso público.

En una primera aproximación al principio del consentimiento, se puede afirmar que todo tratamiento de datos requiere el consentimiento del interesado, así como su comunicación a un tercero, y que cuando el tratamiento o la comunicación afectan a datos especialmente protegidos, el consentimiento tiene que estar dotado de unas garantías especiales, en este supuesto deberá ser expreso.

La entidad que pretenda comunicar los datos de sus clientes, proveedores, empleados, a terceras empresas con la finalidad de que éstas los traten con fines de publicidad, deberá previamente comprobar que se ha informado y recabado el consentimiento de los afectados para dicha comunicación. La empresa cesionaria de los datos informará en dicha comunicación de la procedencia de los mismos, del responsable del fichero y domicilio donde podrá ejercitar los derechos de acceso, rectificación, cancelación y oposición.

A los efectos anteriores las entidades deben conocer que las compañías del grupo a efectos de protección de datos tienen la consideración de tercero, y por tanto, son supuestos de comunicación o cesión de datos.

Se deben incluir en sus procedimientos formulas de recogida del consentimiento de forma que respondan a una manifestación de voluntad libre, inequívoca, especifica e informada, para aquellos supuestos que hayan determinado como necesarios.

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

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

Por lo tanto, las fuentes para la actividad de marketing se encontrarían en:

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

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

Estos supuestos son:

a) El censo promocional, regulado conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, actualmente no está existe dicho censo.

b) Las guías de servicios de comunicaciones electrónicas, en los términos previstos por su normativa específica.

c) Las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección profesional e indicación de su pertenencia al grupo. La dirección profesional podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica. En el caso de Colegios profesionales, podrán indicarse como datos de pertenencia al grupo los de número de colegiado, fecha de incorporación y situación de ejercicio profesional.

d) Los Diarios y Boletines oficiales

e) Los medios de comunicación social. (Podrán considerarse incluidos los datos que hayan sido objeto de difusión a través de prensa, radio y televisión (convencional o digital)

Internet no es, a los efectos de protección de datos un “medio de comunicación social”, sino un “canal de comunicación”, por lo que no es fuente accesible al público.

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

Si para la realización de una campaña de publicidad se decidiera adquirir los datos a través de una empresa proveedora de bases de datos, deberá exigir siempre en el contrato un compromiso sobre el origen de los datos (procedentes de fuentes de acceso público o recabados con el consentimiento del interesado).

A tenor del artículo 11.1 LOPD los datos de carácter personal objeto de tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de los fines directamente relacionados con las funciones legítimas del cedente y cesionario, con el previo consentimiento del interesado. Es decir, cuando el responsable del fichero pretenda realizar un arrendamiento de datos (entregar a otra empresa un listado en una promoción de marketing-con o sin segmentación previa-) y comercializar la información, deberá recabar el consentimiento previo para realizar dichas cesiones de datos.

No obstante, la empresa responsable del fichero que ceda el fichero, deberá cumplir lo establecido en la LOPD, en el sentido de informar en el momento en el que se efectúe la primera cesión de datos de los siguientes aspectos:

- Notificación de la cesión.
- La finalidad del fichero.
- La naturaleza de los datos cedidos
- Nombre y dirección del cesionario.

La adquisición de listados de personas físicas con datos procedentes de una empresa externa, se considerará cesión de datos a los efectos de la vigente Ley Orgánica 15/1999. Por tanto, en ningún caso supondrá una prestación de servicios del artículo 12 LOPD (resulta necesario identificar ambas figuras).

Nos referimos a los mailing dirigidos a personas que no son clientes ni solicitantes de información o catálogos, y por tanto no se encuentran registrados en ficheros propios de la entidad. En esta actividad se utilizan listados de personas, adquiridos a empresas especializadas en marketing, publicidad directa y prospecciones comerciales, realizando sobre ellos segmentaciones derivadas de hábitos de consumo, contestación a encuestas de opinión, etc. Los datos en concreto, deberán haber sido obtenidos de fuentes accesibles al público o facilitados por los propios interesados u obtenidos con su consentimiento.

Los contratos de arrendamiento de direcciones que se establezcan con los proveedores para obtener listados de potenciales clientes a los que se dirigen acciones de Marketing, situarán a la empresa como entidad cesionaria de la comunicación de datos.

Cuando la empresa, se plantee la necesidad de alquilar listados de direcciones, bien para un solo uso o bien para varios, deberán tenerse en cuenta los siguientes aspectos:

- Fuentes de información de las que se nutre el listado.
- Datos que incluye dicho listado.
- Actualización de los datos (mensual, anual, etc.).
- Inscripción del fichero de donde proviene el listado en el Registro General de Protección de Datos.
- Posibles duplicidades de datos y tratamientos informáticos a realizar.
- Posibles variables de segmentación que se ofrecen (sexo, geográficas, renta, edad, formación, capacidad de compra, etc.).

Si una vez analizados los apartados anteriores, se establece la viabilidad del alquiler del listado, deberá elaborarse un contrato que se ajuste a los requerimientos que establece la LOPD. Por tanto, la empresa, en caso de no figurar, deberá regular los siguientes aspectos en el contrato:

- Se ha de diferenciar la cesión de datos de las prestaciones de servicios que se regulen (tanto si son prestadas por el mismo proveedor, como si se regulan los requisitos generales de la prestación que debe cumplir una tercera empresa, ya sea contratada por el proveedor o por el beneficiario de la información).

- Respecto a la cesión de datos, se ha de detallar el objeto, finalidad, datos que se ceden, plazo, nº de usos, inserción de códigos o registros de control, fecha de la devolución o destrucción del soporte entregado.
- Se ha de identificar el fichero/s inscritos en el Registro General de Protección de Datos que se van a utilizar en la elaboración del listado y la procedencia específica de los datos que componen dicho fichero/s.

- Asimismo, se ha de garantizar por parte del proveedor el cumplimiento de todos los requisitos que le impone la LOPD y el RDLOPD, respecto a sus datos, incluida la procedencia u origen de los datos, su actualización, derechos de oposición y listas Robinson.

- Los datos que incluyan el listado deben haber sido recabados de las fuentes accesibles al público, anteriormente señaladas, o con el consentimiento de los afectados para la cesión de los datos, así como que se ha procedido a informar a los interesados de los aspectos recogidos en el artículo 5 LOPD. Si los datos proceden de las fuentes accesibles al público (incluidas en el artículo 3j) LOPD), deberá observarse lo dispuesto en el artículo 28 LOPD, en lo relativo a la caducidad de las mismas:

    - Si la fuente accesible al público de la que provienen los datos se edita en forma de libro o algún otro soporte físico, ésta perderá el carácter de fuente de acceso público con la nueva edición que se publique (los datos del listado pertenecen a la última edición).
    - Si los datos provienen de una copia de la lista en formato electrónico, perderá el carácter de fuente accesible al público en el plazo de un año desde su obtención.
    - Que los datos incluidos en el listado no son excesivos o inadecuados, en relación con la finalidad de dicho listado (acciones de marketing) como que contenga datos calificados como sensibles por el artículo 7 LOPD.

- Los datos deben estar actualizados de forma que respondan a la situación real de los titulares de los mismos.

- Se ha de establecer la cláusula informativa.

- Suscripción de una cláusula de compromiso, donde se recoja que la empresa no realizará uso diferente al pactado o ilícito de los datos.

- Recoger en el contrato, de acuerdo a lo establecido en el RDLOPD, que la comunicación realizada por empresas externas, debe garantizar el nivel de seguridad correspondiente al tipo de información tratada.

- Compromiso genérico por parte del proveedor del cumplimiento de todos los deberes y obligaciones que le impone la Ley Orgánica 15/1999 y reconocimiento expreso de la exención de cualquier tipo de responsabilidad a la empresa cesionaria, motivada por cualquier posible reclamación de particulares y/o Agencia Española de Protección de Datos.

Cuando acabe el plazo determinado o la campaña para la que los datos fueron cedidos, es necesario que dichos datos sean devueltos o suprimidos por el cesionario.

La empresa cesionaria que solicitó el alquiler de listados de direcciones, deberá guardar el original de dicho contrato a efectos de prueba.

Además de lo anterior, el nuevo RDLOPD establece que cuando se pretenda contratar a terceros la realización de una determinada campaña publicitaria de sus productos encomendándole el tratamiento de determinados datos se aplicaran las siguientes normas:

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

Se considerará cesión de datos cuando dos o mas responsables pretendan, sin consentimiento de los interesados, con fines de promoción o comercialización de sus productos o servicios y mediante un tratamiento cruzado conocer quien ostenta la condición de cliente de una u otra.

Se podrán conservar los mínimos datos imprescindibles para identificar a la persona que haya manifestado su negativa a recibir publicidad.

El actual RDLOPD, contempla la posibilidad de creación de ficheros comunes de exclusión de carácter general o sectorial. Los únicos ficheros que podríamos consultar, como se está haciendo hasta ahora, son los de la FECEMD. Asimismo se determina que, cuando el interesado manifieste su oposición a que sus datos sean tratados con fines de publicidad el responsable del fichero deberá informarle de la existencia de los ficheros comunes de exclusión así como la identidad de su responsable, su domicilio y la finalidad del tratamiento.

Siempre que se quiera realizar un tratamiento relacionado con actividades de publicidad habrá que consultar previamente los ficheros comunes mencionados a día de hoy el de la FECEMD.

Cuando un interesado se dirija a la empresa ante la que se ha encargado la realización de una campaña publicitaria estará obligada en el plazo de diez días desde la recepción de la solicitud a comunicárselo al responsable del fichero para que éste en el plazo de diez días desde la recepción de la comunicación dando cuenta de ello al afectado.

Para el ejercicio de los derechos de oposición, especifica el RDLOPD que deberá concederse al interesado un medio sencillo y gratuito para oponerse al tratamiento. Se considerará cumplido cuando los derechos puedan ejercitarse mediante la llamada a un número telefónico gratuito o la remisión de un correo electrónico. Asimismo si el responsable del fichero dispone de servicios de cualquier índole para la atención de sus clientes deberá concederse la posibilidad al afectado de ejercer su oposición a través de dichos servicios. Igualmente se recogen los plazos establecidos en el punto anterior cuando es un tercero quien realiza una campaña publicitaria.

1.6 Ficheros de titularidad pública y titularidad privada

La LOPD y el actual RDLOPD, establecen una normativa de carácter general aplicable a todo tipo de ficheros (Título IV de la LOPD) que dedica su Capítulo primero (artículos 20 al 24) a los ficheros de titularidad pública y el Capítulo segundo (artículos 25 al 32) a los ficheros de titularidad privada. El Título V capitulo I. del RDLOPD (artículos 49, 52 a 64) dedica a las inscripciones de ficheros públicos y privados.
Los de titularidad pública serán la consecuencia del ejercicio de una función pública, mientras que los privados pueden ser creados según las necesidades de la persona, empresa o entidad titular, para el logro de su actividad u objeto legítimos.
La diferencia entre unos y otros estriba principalmente en la forma de creación, modificación o supresión de los mismos, y en las sanciones impuestas en caso de infracción. Para ambos tipos de ficheros existe la obligación de notificación e inscripción en la Agencia Española de Protección de Datos, y el régimen de infracciones es el mismo.

1.6.1 Ficheros de titularidad pública

Los ficheros de titularidad pública serán aquellos cuyo titular sea la Administración pública. El derecho de las Administraciones públicas a recabar datos de los ciudadanos se basa en la necesidad de éstas de defender el interés público, que en ocasiones puede entrar en colisión con el derecho a la intimidad de las personas. Como punto de partida se admite que para la gestión pública, las Administraciones Públicas tengan que disponer de la información necesaria de los ciudadanos, pero dicha información debe ser la estrictamente necesaria para una gestión eficaz.
Entre las excepciones a la necesidad de consentimiento, está la del tratamiento por parte de la Administración Pública. A pesar de que el tratamiento de los datos debe depender principalmente del interesado, en caso de que la Ley, atendiendo a la existencia de un interés prevalente, autorice el tratamiento, no será necesario dicho consentimiento.

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

- La finalidad del fichero y los usos previstos para el mismo.
- Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
- El procedimiento de recogida de los datos de carácter personal.
- La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
- Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.
- Los órganos de las Administraciones responsables del fichero.
- Los servicios o unidades ante los que pudiesen ejercitarse los derechos reconocidos en la Ley (acceso, rectificación, cancelación y oposición).
- Las medidas de seguridad con indicación del nivel básico, medio o alto exigible en el RD 1720/2007, de 21 de diciembre.

- Respecto a las disposiciones que se dicten para la supresión de los ficheros, habrá que indicarse el destino de los mismos, o en su caso, la forma de destrucción.
- De lo dispuesto en el artículo 41 de la LOPD, se deriva la posibilidad de crear Agencias de Protección de Datos en las Comunidades autónomas u órganos correspondientes. Este artículo sirve de fundamento a la Ley 13/1995, de 21 de abril, de regulación del uso de la informática en el tratamiento de datos personales por la comunidad de Madrid, por la que se crea la Agencia de Protección de Datos de la Comunidad de Madrid (APDCM) como autoridad de control respecto de los tratamientos y usos de datos contenidos en ficheros creados o gestionados por las instituciones de la Comunidad de Madrid, y por los órganos, organismos, entidades de derecho público y demás entes públicos, así como de las Administraciones locales de su ámbito competencial. Dicha Ley se sustituye por la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid (LPDCM).

Las sanciones previstas para los titulares de ficheros públicos se caracterizan por no ser de carácter económico, a diferencia de las previstas para los titulares de ficheros privados. En estos supuestos, el Director de la Agencia Española de Protección de Datos dictará una resolución que establezca las medidas a adoptar para que cesen o se corrijan los efectos producidos por dicha infracción. Ésta será notificada al Responsable del fichero, al órgano del que dependa jerárquicamente y a los interesados en caso de que los hubiera. También puede proponer la iniciación de actuaciones disciplinarias si éstas procediesen. Será el régimen disciplinario de las Administraciones Públicas el que establezca el procedimiento y las sanciones que se deben aplicar. Las resoluciones que recaigan en relación con estas medidas y actuaciones deben ser comunicadas a la Agencia Española de Protección de Datos, y el Director de la Agencia debe comunicar al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte en este sentido.

La diferencia estriba en el estímulo que prevé la ley para promover su cumplimiento. Cuando se trata de ficheros de titularidad privada, la Ley establece unas elevadas sanciones, por lo que el estímulo es de tipo económico. Sin embargo, en el caso de las Administraciones, só se trataría de una sanción disciplinaria.

1.6.2 Ficheros de titularidad privada

Los ficheros de titularidad privada están sometidos a un régimen distinto. La Ley prevé para este tipo de ficheros un sistema de control a priori, dada la necesidad de inscripción y notificación registral. Podrán ser creados cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad. A diferencia de los ficheros de titularidad pública, los ficheros de titularidad privada deben tener unas finalidades determinadas, acordes con los fines institucionales o con el objeto social de la entidad o empresa.

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

Asimismo, deberá comunicarse cualquier cambio en la finalidad, el responsable o la dirección de ubicación del fichero. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia hubiera resuelto sobre la misma, se entenderá inscrito el fichero a todos los efectos.

El procedimiento para la inscripción de ficheros consiste en la presentación de los modelos o formularios electrónicos, y en soporte papel, de notificación de creación, modificación o supresión de ficheros, así como los formatos para la comunicación telemática de ficheros públicos por las autoridades de control autonómicas, de conformidad con lo establecido en los artículos 55 y 58 del RDLOPD.

1.- Iniciación del procedimiento (art. 130 RLOPD)

-Notificación mediante cumplimentación del formulario disponible en www.agpd.es, presentación telemática o en papel.

2.- Notificación titularidad pública (art. 131 RLOPD).

•Acompañar copia de la norma o acuerdo regulador o dirección electrónica que permita su localización.

•En caso de requerimiento. Plazo de subsanación o mejora: 3 meses.

3.- Duración del procedimiento. 1 mes (art. 134 RLOPD).

El Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, dictará resolución acordando, en su caso, la inscripción.

La inscripción contendrá el código asignado por el Registro, la identificación del responsable del fichero, la identificación del fichero o tratamiento, la descripción de su finalidad y usos previstos, el sistema de tratamiento empleado en su organización, en su caso, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, y la indicación del nivel de medidas de seguridad exigible conforme a lo dispuesto en el artículo 81 del RDLOPD.

Asimismo, se incluirán, en su caso, la identificación del encargado del tratamiento en donde se encuentre alojado el fichero y los destinatarios de cesiones y transferencias internacionales.

La inscripción de un fichero en el Registro General de Protección de Datos, no exime al responsable del cumplimiento del resto de las obligaciones previstas en la Ley Orgánica 15/1999, de 13 de diciembre, y demás disposiciones reglamentarias.

En los casos de que existan más de un responsable del fichero, es decir se prevea crear un fichero del que resulten responsables varias personas o entidades simultáneamente, cada una de ellas deberá notificar, a fin de proceder a su inscripción en el Registro General de Protección de Datos y, en su caso, en los Registros de Ficheros creados por las autoridades de control de las Comunidades Autónomas, la creación del correspondiente fichero.

INFRACCIÓN	*Art. 44.2. Son infracciones leves:* *c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.*
SANCIÓN	*Art. 45.1: Multa de 601,01 a 60101,21 €*
INFRACCIÓN	*Art. 44.3. Son infracciones graves:* *a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el "Boletín Oficial del Estado" o Diario Oficial correspondiente.* *b) Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.* *k) No inscribir el fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando haya sido requerido para ellos por el Director de la Agencia de Protección de Datos.*
SANCIÓN	*Art. 45.2: Multa de 60101,21 a 300506,05 €*

1.7 Transferencia internacional de datos

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

En particular, se consideran como tales las que constituyan una cesión o comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable de fichero".

En cuanto a las transferencias internacionales de datos, se regulan en los artículos 33 y 34 LOPD, y en el RD. 1720/2007 (arts. 65 a 70).

Respecto al régimen jurídico aplicable, las transferencias internacionales de datos efectuadas desde España están sometidas, en principio, a la previa autorización del Director de la Agencia Española de Protección de Datos.

La LOPD, diferencia los casos en los que la transferencia tiene como país de destino uno que proporcione un nivel de protección adecuado, de aquellos en los que no ocurra así.

Se consideran países que proporcionan un nivel de protección adecuado, los estados miembros de la Unión Europea, Islanda, Liechtenstein, Noruega o un Estado respecto del cual la Comisión de las Comunidades Europeas haya declarado que ganrantiza un nivel de protección adecuado, estando incluidos, hasta la fecha, entre esto últimos, Suiza, Argentina, las entidades estadounidenses adheridas a los "principios del puerto seguro", Guernsey, Isla de Man y Canadá, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos.

Así, las transferencias internacionales de datos de carácter personal a países que no proporcionen un nivel de protección equiparable al nacional están prohibidas, salvo en los casos en los que se obtenga autorización previa del Director de la AEPD.

La LOPD también recoge una serie de supuestos en los que la transferencia estaría permitida sin necesidad de solicitar dicha autorización:

A. Cuando la transferencia resulte de la aplicación de tratados o convenios en los que sea parte España.
B. Cuando se haga a efectos e prestar auxilio judicial internacional.
C. Cuando sea necesaria para la prevención o el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.
D. Cuando se refiera a transferencias dinerarias conforme a su legislación específica.
E. Cuando el afectado haya dado su consentimiento inequívoco.
F. Cuando 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 sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar por el responsable del fichero y un tercero.
H. Cuando sea necesaria o legalmente exigida para la salvaguarda de un interés público (transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias).
I. Cuando sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
J. Cuando se efectúe a petición de persona con interés legítimo desde un registro público y aquella sea acorde con la finalidad del mismo.
K. Cuando tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas haya declarado que garantiza un nivel de protección adecuado.

La no aplicación del régimen de autorización previa del artículo 33 LOPD en modo alguno excluye, en primer lugar, que la transferencia deba sujetarse al régimen general de comunicación de datos de carácter personal establecido en el artículo 11, donde se exige para la misma (salvo los supuestos exceptuados por el apartado segundo), que dicha cesión se efectúe a un tercero para el cumplimiento de fines directamente relacionados con las funciones legitimas del cedente y cesionario, así como el previo consentimiento del interesado, suficientemente informado de la finalidad a que se destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar.

A lo anterior no afecta que la cesión se efectúe entre sociedades integradas en un mismo grupo empresarial, desde el momento en que estamos en presencia de una entidad diferente de aquella a la que los interesados cedieron los datos, siendo indiscutible que el cesionario tiene en tal caso la condición de tercero a que alude el artículo 3.i) LOPD. Esta interpretación, se aplica también a cesiones que se verifiquen entre empresas de un mismo grupo siendo todas ellas de nacionalidad española.

Cuando se prevean hacer transferencias internacionales con los datos de los afectados, deberá notificarse a la Agencia Española de Protección de Datos e informar al interesado.

INFRACCIÓN	*Art. 44.4. Son infracciones muy graves:* *e) La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia Española de Protección de Datos.*
SANCIÓN	*Art.45.3: Multa de 300506,05 € a 601012,10 €*

1.8 Medidas de seguridad.

El artículo 9 LOPD establece otro de los principios generales de la Ley: principio de seguridad de los datos y en el RD. 1720/2007 de desarrollo de la LOPD.

1.8.1 Seguridad de la Información

Según lo dispuesto en el artículo 9 de la LOPD, es responsabilidad del Responsable del Fichero y en su caso, del Encargado del Tratamiento, el implantar las medidas de seguridad técnicas y organizativas que garanticen la seguridad de los datos, es decir:

- la confidencialidad: evitar accesos no autorizados,
- la disponibilidad: evitar su pérdida,
- la integridad: evitar su alteración no deseada.

Las medidas a adoptar dependerán tanto de la naturaleza de los datos almacenados, como de los riesgos a los que están expuestos y al estado de la tecnología.

Tal y como se ha comentado, se indica que las medidas adoptadas deberán de ser acordes con el estado de la tecnología. Esto supone la obligación por parte del Responsable del Fichero de mantener una actualización constante de las medidas no sólo a cambios organizativos en la entidad o en el marco legal, sino también al progreso que se produzca en la tecnología y en los sistemas de tratamiento de información. Por tanto, se deduce que es necesario mantener los sistemas de tratamiento actualizados periódicamente.

Lo anterior incide en la reconocida idea de que **la seguridad no es un estado sino un proceso**. De nada sirve proteger unos sistemas si no se mantiene y se analiza a que nuevos riesgos se puede enfrentar y que nuevas medidas se han de adoptar para reducirlos.

1.8.2 Sanciones

La LOPD tipifica los incumplimientos en materia de seguridad como infracciones graves:

INFRACCIÓN	*Art. 44.3. Son infracciones graves:* *h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.*
SANCIÓN	*Art. 45.2: Multa de 60101,21 a 300506,05 €*

1.8.3 RDLOPD 1720/2007.

Lo dispuesto en el artículo 9 LOPD ha sido desarrollado por vía reglamentaria. El 21 de Diciembre de 2007. Este nuevo RDLOPD, deroga el anterior RD. 994/1999 que desarrolló el artículo 9 de la Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD).

El Real Decreto 1720/2007, debe de aplicarse tanto a los ficheros automatizados como a los no automatizados.

En consecuencia, desde la entrada en vigor del RDLOPD 19 de Abril 2008, resulta aplicable a los ficheros en soporte no automatizado. Los ficheros manuales que existieran antes de dicha fecha, dispondrán a estos efectos, de un plazo de adaptación.

No obstante, cuando resulte de aplicación el RDLOPD de medidas de seguridad, conforme a los criterios expuestos, sólo deberán implantarse las medidas de seguridad, que pese a estar previstas para ficheros automatizados, por su naturaleza sean también aplicables a ficheros no automatizados (por ejemplo, la elaboración e implantación del Documento de Seguridad).

1.8.4 Niveles de seguridad

El RDLOPD de Medidas de Seguridad establece los requisitos y condiciones que deben reunir los ficheros y las personas que intervengan en el tratamiento de los datos. El RDLOPD viene a establecer tres niveles de seguridad, atendiendo a la naturaleza de la información tratada en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la misma, con independencia de la finalidad en virtud de la cual se haya procedido al tratamiento de los datos personales.

Interesa señalar que se trata de un RDLOPD de mínimos (se establecen las medidas mínimas exigibles al tipo de datos tratados). Es decir, corresponde a cada responsable de fichero, en virtud de su criterio, establecer medidas de seguridad más severas de las establecidas en el RDLOPD.

A continuación se expone un cuadro resumen de las medidas de seguridad aplicable en virtud del tipo de datos de carácter personal objeto de tratamiento:

DATOS	NIVEL DE SEGURIDAD
Ficheros con datos de carácter personal.	**Medidas de seguridad de nivel básico**, establecidas en los artículos 105 al 108 del RDLOPD. Cualquier fichero o tratamiento de datos de carácter personal. Ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando: - transferencia dineraria - entidades de las que los afectados sean asociados o miembros. - tratamiento manual de forma incidental o accesoria, sin guardar relación con la finalidad. Salud - grado o condición de discapacidad o invalidez - cumplimiento de deberes públicos.
Ficheros con datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y a la prestación de servicios de información sobre solvencia patrimonial y de crédito.	Además de las de nivel básico, **medidas de seguridad de nivel medio**, establecidas en los artículos 109 a 110 del RDLOPD. - Infracciones administrativas o penales - Servicios de información sobre solvencia patrimonial y crédito. - Administraciones Tributarias - potestades tributarias. - Entidades financieras - servicios financieros - Seguridad Social, Mutuas. - Elaboración de perfiles. - MEDIO (+ registro de accesos) Operadores TELECO – tráfico y localización
Ficheros con datos de ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual, así como los que contengan datos recabados con fines policiales sin consentimiento de las personas afectadas.	Además de las de nivel básico y medio, **medidas de seguridad de nivel alto**, establecidas en los artículos 111 - 114 del RDLOPD. - Datos especialmente protegidos. - Fines policiales sin consentimiento de las personas afectada. - Violencia de género.

De acuerdo con lo expuesto anteriormente, el tratamiento de datos personales obliga a la empresa a tener implementadas las medidas de seguridad a cualquier fichero o tratamiento con independencia de:

1.- Quién realice el tratamiento, como es el supuesto de las prestaciones de servicios realizadas por el encargado del tratamiento y los diferentes modos de la prestación del servicio (art. 82 del RDLOPD).

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

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

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

3. En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en este RDLOPD.

2.- La prestación de servicios sin acceso a datos personales (art. 83) en éste caso deberá establecerse en el contrato una cláusula informativa donde se recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

Cabe destacar que en el supuesto de las prestaciones de servicio, se establecerá por contrato escrito las medidas de seguridad a implantar por el encargado del tratamiento. Asimismo, se tendrá en cuenta que la implantación de las medidas de un cierto nivel implica necesariamente la implantación de todas las medidas de niveles inferiores.

Asimismo se deberá tener en cuenta que es habitual que un fichero sea tratado por diversas herramientas y que los datos asociados a un mismo titular almacenados en cada una de estas herramientas podrían ser distintos en cuanto a su tipología. Así pues, a cada una de las herramientas se les deberá de dotar de las medidas de seguridad que les corresponda por la tipología de los datos que trata.

1.8.5 Documento de Seguridad

El eje sobre el que gira toda la normativa del RDLOPD sobre medidas de seguridad de los datos de carácter personal es el Documento de Seguridad. En el RDLOPD se establecen los requerimientos técnicos y organizativos mínimos exigibles, y estos se recogerán en el Documento de Seguridad.

El Documento de seguridad no tiene que presentarse en la Agencia Española de Protección de Datos, si bien deberá estar a disposición de ésta, en el supuesto de requerimiento o inspección. Igualmente, en caso de implantar medidas de nivel medio o alto, deberá ser auditado cuando se proceda a realizar la preceptiva auditoría que será de carácter bienal.

En caso de haber contratado la prestación de servicios por terceros para determinados ficheros, en el documento de seguridad se debe hacer constar esta circunstancia, indicando una referencia al contrato y su vigencia así como los ficheros objeto de este tratamiento.

Si se ha contratado la prestación de servicios en relación con la totalidad de los ficheros y tratamientos de datos del responsable, y dichos servicios se prestan en las instalaciones del encargado del tratamiento se podrá delegar en éste la llevanza del documento de seguridad.

1.8.5.1 Medidas para todos los tratamientos:

Medidas Generales:

Formalizar por escrito en el Documento de Seguridad las posibles delegaciones de funciones del Responsable del Fichero en otra persona. Formalizar por escrito en el Documento de Seguridad las autorizaciones para el tratamiento de datos fuera de los locales del Responsable. Estas autorizaciones se podrán establecer por usuario o por perfil de usuario, determinando el periodo de validez de la autorización. Garantizar la aplicación de las medidas de seguridad correspondiente a los ficheros temporales, borrándolos o destruyéndolos una vez que cumplan su función.

1.8.5.2 Medidas de seguridad de Nivel Básico

Funciones y obligaciones del personal:

Definir las distintas funciones y obligaciones del personal para el tratamiento de datos de carácter personal, bien por usuario o por perfiles de usuario, incluyendo las autorizaciones delegadas por el Responsable del fichero o tratamiento, debiendo informar a todo el personal de forma comprensible de las normas de seguridad que afecten al desarrollo de sus funciones.

Registro de incidencias: Establecer y documentar un procedimiento de notificación y gestión de incidencias, incluyéndolo en el Documento de Seguridad, y habilitando un registro de las mismas.

Control de acceso a datos: Limitar el acceso de los usuarios (propios o ajenos a la organización) únicamente a aquellos recursos necesarios para la realización de sus funciones, debiendo mantener un registro actualizado de usuario y perfiles de usuarios con los accesos autorizados de cada uno. Establecer mecanismos que eviten el acceso de los usuarios a recursos a los que no estén autorizados, reflejando en el documento de seguridad el usuario o perfil de usuarios que pueden modificar los accesos sobre los recursos.

Medidas de seguridad de Nivel Medio:

Responsable de seguridad: Designar uno o varios Responsables de Seguridad, reflejándolo en el Documento de Seguridad, que serán los encargados de coordinar y controlar las medidas de seguridad establecidas.

Auditoría: Realizar una auditoría al menos bianual de los sistemas de información e instalaciones de tratamiento y almacenamiento de datos, que dictamine sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario. Estas auditorías serán analizadas por el/los Responsables de Seguridad, que deberán implantar las medidas correctoras o complementarias y elevar las conclusiones al Responsable del Fichero. Se realizará una auditoría extraordinaria siempre que existan modificaciones sustanciales en el sistema de tratamiento de los datos.

Gestión de soportes y documentos: Establecer un sistema que registre las entradas y salidas de soportes o documentos con datos de carácter personal.

1.8.5.3 Medidas para el tratamiento de datos automatizado

Medidas Generales:

Garantizar un nivel de seguridad equivalente al acceso local a los accesos a datos automatizados a través de redes de comunicaciones (públicas o no).

1.8.5.4 Medidas de seguridad de Nivel Básico

Gestión de soportes y documentos:

Los soportes que contengan datos de carácter personal deben permitir identificar el tipo de información que contienen, (a menos que las características del soporte lo imposibiliten), constar en un inventario, y permitir el acceso a los mismos exclusivamente al personal autorizado. La salida de soportes y documentos, así como los correos electrónicos con datos de carácter personal deberá ser autorizada por el Responsable del fichero o constar como autorizada en el Documento de Seguridad. Para el traslado de los documentos de deben implantar medidas que eviten el acceso, perdida o sustracción de los mismos. Los soportes que vayan a ser desechados deben ser destruidos o borrados para que nadie pueda acceder o recuperar la información contenida en ellos.

Identificación y autenticación: Implantar un sistema de identificación y autenticación inequívoca y personalizada para cada usuario, verificando la autorización para el acceso a los datos. Si el método de identificación se realiza mediante contraseñas, se debe establecer y documentar un procedimiento para la asignación, almacenamiento y comunicación confidencial de la contraseña, estableciendo el periodo de validez de las contraseñas (no superior a un año) y reflejándolo en el Documento de Seguridad

Copias de respaldo y recuperación de datos: Establecer procedimientos de realización de copias de seguridad, cuya periodicidad no sea superior a 7 días, (salvo que no exista modificación de los datos en dicho periodo), y procedimientos de recuperación de datos que garanticen la recuperación de los mimos. El Responsable del fichero, o en su caso la persona o perfil designado en el Documento de Seguridad, se encargará de la verificación de la correcta definición, funcionamiento y aplicación de los procedimientos de copia y recuperación de datos. Las pruebas realizadas con datos reales deberán cumplir las medidas de seguridad correspondientes, realizando previamente una copia de seguridad de dichos datos.

1.8.5.5 Medidas de seguridad de Nivel Medio

Identificación y autenticación: Establecer medidas que impidan el intento de acceso no autorizado de manera reiterada al sistema de información.

Control de acceso físico a servidores de datos: Implantar medidas que restrinjan el acceso a los lugares donde se encuentren los servidores al personal no autorizado.

Registro de incidencias: Las recuperaciones de datos deberán ser autorizadas por el Responsable del Fichero y ser registradas en el registro de incidencias.

1.8.5.6 Medidas de seguridad de Nivel Alto

Gestión y distribución de soportes: La identificación de soportes se debe realizar de forma no comprensible para el personal no autorizado. La distribución de soportes se debe realizar utilizando mecanismos que eviten el acceso o manipulación no autorizado de la información, como el cifrado de los mismos, igualmente se cifrarán los datos contenidos en dispositivos portátiles que se saquen fuera de los locales de la organización, debiendo evitar el tratamiento en dispositivos portátiles que no lo permitan.

Copias de respaldo y recuperación de datos: Almacenar una copia de seguridad de los datos y de los procedimientos de recuperación fuera de los locales de la organización.

Registro de accesos: Configurar un registro que almacene los intentos de acceso a los datos, así como las acciones realizadas por los usuarios que hayan accedido, manteniendo dicho registro al menos durante dos años, y debiendo ser revisado por el Responsable de Seguridad mensualmente, quien deberá emitir un informe de la revisiones realizadas.

Telecomunicaciones: Las comunicaciones de datos a través de redes públicas o inalámbricas se realizaran con algún mecanismo que evite el acceso o manipulación por terceros, como por ejemplo cifrándolas.

1.8.6 Medidas de seguridad para el tratamiento de datos no automatizado:

1.8.6.1 Medidas de seguridad de Nivel Básico:

Criterios de archivo de soportes: El archivo de soportes o documentos deberá garantizar la correcta conservación de los mismos, la localización y consulta de la información contenida. **Dispositivos de almacenamiento:** Implantar mecanismos que eviten la apertura de los dispositivos que contengan datos de carácter personal.

Custodia de los soportes: Establecer normas para que el personal que trate los soportes con datos antes de su almacenamiento, custodie e impida el acceso a los mismos por parte de personal no autorizado.

1.8.6.2 Medidas de seguridad de Nivel Alto:

Almacenamiento de la información: Los elementos de almacenaje de documentos o soportes no automatizados con datos deben encontrase en áreas de acceso restringido, con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente, que deberán permanecer cerradas cuando no se acceda a la información.

Copia o reproducción de soportes o documentos: Las copias de los soportes o documentos deberán realizarse bajo control de personal autorizado, debiendo destruir las copias desechadas de forma que se evite el acceso a la información que contenían.

Registro de accesos a información automatizada: Configurar un registro que almacene los intentos de acceso a los datos, así como las acciones realizadas por los usuarios que hayan accedido, debiendo ser revisado este registro por el Responsable de Seguridad mensualmente, quien deberá emitir un informe de dicho registro.

Acceso a la información: Implantar medidas que permitan identificar los accesos realizados cuando los documentos se puedan utilizar por varios usuarios, debiendo quedar constancia en un registro del acceso de personas no autorizadas formalmente en el Documento de Seguridad.

Traslado de documentación: Implantar medidas que impidan el acceso o manipulación por terceros cuando se trasladen soportes o documentos con datos.

1.8.7 Disposición transitoria segunda. Plazos de implementación

- Ficheros nuevos manuales y/o automatizados

  Aplicación del nivel básico, medio o alto correspondiente desde su creación.

- Ficheros existentes:

Automatizados:

- Seguridad Social, Mutuas, Perfiles → 1 año (Medio)
- Violencia de género → 1 año (Medio) → 18 meses (Alto)
- Telecomunicaciones (tráfico, localización) → 1 año (Medio) → 18 meses (Registro de accesos).
- Adaptación resto de ficheros → 1 año (arts. 93, 94, 101, 104)

No automatizados

- Básico (1 año)
- Medio (18 meses)
- Alto (2 años)

1.9 Introducción: funciones de la Agencia Española de Protección de Datos.

La Agencia Española de Protección de Datos, es el ente independiente que debe garantizar el cumplimiento de las previsiones y mandatos establecidos en la Normativa existente y vigente en materia de Protección de Datos. Actualmente la LOPD y el RDLOPD.

Artículo 120 del RDLOPD. Ámbito de aplicación.
1. Las disposiciones contenidas en el presente capítulo serán de aplicación a los procedimientos relativos al ejercicio por la Agencia Española de Protección de Datos de la potestad sancionadora que le viene atribuida por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal, en la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico, y en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.
2. No obstante, las disposiciones previstas en el artículo 121 y en la sección cuarta de este capítulo únicamente serán aplicables a los procedimientos referidos al ejercicio de la potestad sancionadora prevista en la Ley Orgánica 15/1999, de 13 de diciembre.

Se le asignan las competencias necesarias para su ejercicio, clasificándolas en dos tipos de funciones:

- Funciones inspectoras.
- Funciones instructoras.

Las funciones inspectoras, abarcan las actuaciones de examen, análisis y prueba de sistemas, ficheros, documentos, dispositivos y, en general, de todos aquellos elementos relacionados con los posibles tratamientos automatizados de datos personales objeto de investigación.

Las funciones instructoras, relacionadas con el ejercicio de la potestad sancionadora, incluyen la tramitación de los expedientes administrativos iniciados como consecuencia de reclamación o denuncias recibidas en la Agencia Española y relacionadas con la protección de datos personales.

Estas actuaciones instructoras, están estructuradas en torno a tres procedimientos diferenciados según se trate de tutelar los derechos reconocidos por la Ley, instruir y resolver expedientes sancionadores o tramitar expedientes derivados de infracciones cometidas en ficheros cuyo responsable es una Administración Pública.

La práctica ha puesto de manifiesto que los escritos recibidos en la Agencia requieren frecuentemente un proceso previo de análisis de contenido y obtención de información adicional, antes de ser encaminados hacia uno de los procedimientos. En ocasiones, estas actuaciones previas permiten determinar la no procedencia de iniciar procedimiento alguno, por faltar alguno de los supuestos que determinan la competencia de la Agencia para iniciar actuaciones o bien por no haberse cumplido algún requisito previo.

1.9.1 Procedimientos de la Agencia Española de Protección de Datos.

a) Procedimiento de Tutela de Derechos

El ejercicio de los derechos que otorga a los ciudadanos la LOPD, se lleva a cabo mediante un procedimiento de tutela de derechos. El artículo 18 de la LOPD, indica en su apartado primero, que las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los afectados ante la Agencia Española de Protección de Datos, en la forma en que reglamentariamente se determine, (actualmente el RDLOPD).

Se encuentra regulado en el artículo 117 del Real Decreto 1720/2007, indicando que se debe iniciar siempre a instancia del afectado, mediante escrito de reclamación ante la Agencia Española de Protección de Datos; en el referido escrito el afectado debe indicar con claridad el contenido de su reclamación y los preceptos de la Ley Orgánica 15/1999 que se consideren vulnerados.

Recibida la reclamación en la Agencia Española de Protección de Datos, se da traslado de la misma al responsable del fichero para que en el plazo de 15 días, formule las alegaciones que considere convenientes y, tras audiencia al afectado y de nuevo al responsable del fichero, el Director de la Agencia Española de Protección de Datos resolverá dando traslado a los interesados de la resolución, cabiendo recurso contencioso-administrativo contra la misma.

Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su reclamación por silencio administrativo positivo.

Se puede resumir brevemente los pasos del procedimiento de Tutela de Derechos:

- Apertura del procedimiento
- Traslado del procedimiento a la entidad por parte de la Agencia Española de Protección de Datos
- Período de alegaciones en el plazo de 15 días
- Traslado de alegaciones de la entidad al afectado para su contestación
- Nuevo traslado a la entidad para la apertura de un segundo período de alegaciones por 15 días, contestando al afectado.
- Resolución. será de seis meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la reclamación del afectado o afectados.

Si la resolución es desestimatoria, se procederá a su archivo.

Si por el contrario nos encontramos con una resolución estimatoria, la entidad objeto del procedimiento, deberá dar cumplimiento a la misma se requerirá al responsable del fichero para que, en el plazo de diez días siguientes a la notificación, haga efectivo el ejercicio de los derechos objeto de la tutela, debiendo dar cuenta
por escrito de dicho cumplimiento a la Agencia Española de Protección de Datos en idéntico plazo.

También puede resolver con la apertura de un Procedimiento Sancionador.

b) Procedimiento sancionador.

La potestad de inspección de la Agencia Española de Protección de Datos, derivada de la propio Ley Orgánica de Protección de Datos, viene atribuida por el Estatuto de la Agencia y en el Título IX del RDLOPD en su capitulo I, se recoge en el ***Artículo 115. Régimen aplicable.*** *"Los procedimientos tramitados por la Agencia Española de Protección de Datos, se regirán por lo dispuesto en el presente título, y supletoriamente, por la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.*
2. Específicamente serán de aplicación las normas reguladoras del procedimiento administrativo común al régimen de representación en los citados procedimientos.

El Procedimiento Sancionador se encuentra regulado en los artículos 120 a 128 del R.D. 1720/2007. Se inicia siempre de oficio por la Agencia Española de Protección de Datos, bien haya tenido conocimiento por denuncia del afectado o de un tercero, o por otros motivos o actos, como puede ser el ejercicio de la actividad inspectora.

Inspecciones de la Agencia Española de protección de datos.

Las actuaciones previas serán llevadas a cabo por el personal del área habilitado para el ejercicio de funciones inspectoras. Los funcionarios que ejercen estas funciones, tendrán la consideración de autoridad pública, podrán recabar cuantas informaciones precisen para el cumplimiento de sus cometidos.

Las inspecciones podrán realizarse en el domicilio del inspeccionado, en la sede o local concreto relacionado con el mismo o en cualquiera de sus locales, incluyendo aquéllos en que el tratamiento sea llevado a cabo por un encargado.

Funciones de los Inspectores:

- Examinar los soportes de información que contengan datos de carácter personal.
- Examinar los equipos físicos.

- Requerir el pase de programas y examinar la documentación pertinente al objeto de determinar los algoritmos de los procesos de que los datos sean objeto.
- Examinar los sistemas de transmisión y acceso a los datos.
- Realizar auditorías de los sistemas informáticos, para determinar su conformidad con la Ley.
- Requerir la exhibición de los documentos que considere pertinentes.
- Requerir el envío de la información necesaria para el ejercicio de las funciones inspectoras.
- Puede avisar o no previamente a la entidad que va a ser inspeccionada de la realización de la misma.
- Deberán aportar ante la Entidad objeto de la inspección, la autorización que a tal efecto expida el Director de la Agencia.

Los Inspectores, pueden solicitar la presencia de determinados responsables de la Organización, para que puedan responder determinadas cuestiones objeto de la inspección. La organización puede designar a una persona responsable de mantener las relaciones con la Agencia Española de Protección de Datos, siendo esta persona la que asista a las inspecciones, sin que esto haya sido considerado por los inspectores obstrucción a la inspección. De esta forma, una sola persona permanecerá con los inspectores, trasladando las preguntas que no pueda contestar a las personas de la organización correspondientes. A esta persona la designaremos como responsable en protección de datos.

Una vez consultados los datos por la Agencia, procederán a levantar acta de toda la información obtenida, debiendo ser firmada por los responsables de la Entidad inspeccionada, así como por los inspectores de la Agencia de Protección de Datos.

De una inspección realizada por la Agencia Española de Protección de Datos puede derivarse la apertura de un procedimiento de Tutela de Derechos o Procedimiento Sancionador. De no ser así, la Agencia normalmente procederá al archivo de actuaciones, que comunicará por escrito.

La Agencia Española de Protección de Datos puede enviar escritos solicitando información. Estos escritos consisten en la solicitud de información por parte de la Agencia sobre algún aspecto relativo al fichero, o sobre los datos de un afectado en concreto.

La contestación a estos escritos tiene un plazo de diez días, aunque el plazo puede ampliarse, en caso de ser necesario y solicitándolo la entidad destinataria del escrito. Lo normal es que la ampliación sea de un tiempo igual al de la mitad del otorgado inicialmente.

Los Escritos Informativos, pueden ser previos a la apertura de un Procedimiento sancionador, aunque también pueden referirse a una inspección realizada con anterioridad.

Algo más complejo en su desarrollo que el procedimiento de Tutela de Derechos, se inicia mediante acuerdo del Director de la Agencia de Protección de Datos, en el que se designará instructor con indicación de la posibilidad de recusación y se identificará al presunto responsable o responsables, concretando los hechos y la infracción que, supuestamente, ha cometido, así como la sanción o sanciones que se pueden imponer y las medidas cautelares a adoptar en su caso.

Una vez que se notifique al presunto responsable la incoación del expediente, ofreciéndole la posibilidad de efectuar alegaciones y de emplear los medios de prueba de que se quiera valer, se ordenará por el instructor la práctica de las mismas y volverá a poner de manifiesto el expediente al presunto responsable para que, a la vista del resultado de las pruebas, pueda alegar nuevamente, incluso aportando documentos, lo que considere de interés.

Por último, el instructor formulará una propuesta de resolución motivada que notificará al presunto responsable para que, en un nuevo plazo de quince días, pueda formular nuevas alegaciones si lo considera oportuno.

Termina el procedimiento con la notificación al responsable de la resolución que determinará con precisión los hechos imputados, la infracción cometida, el responsable de la misma y la sanción impuesta, o la declaración de no existencia de responsabilidad, expresando también el derecho de interponer contra la misma el correspondiente recurso contencioso-administrativo. Normalmente, la resolución suele confirmar la propuesta de resolución. No obstante, en algunos casos el Director de la Agencia Española de Protección de Datos, ha dictado una resolución de contenido distinto. Esto es especialmente problemático en aquellos casos en los que el instructor, en la propuesta de resolución declara la ausencia de responsabilidad y posteriormente el Director en la resolución, determina la responsabilidad y sanciona.

El plazo para dictar resolución será el que determinen las normas aplicables a cada procedimiento sancionador y se computará desde la fecha en que se dicte el acuerdo de inicio hasta que se produzca la notificación de la resolución sancionadora, o se acredite debidamente el intento de notificación. El vencimiento del citado plazo máximo, sin que se haya dictada y notificada resolución expresa, producirá la caducidad del procedimiento y el archivo de las actuaciones.

Como ya se ha dicho antes, contra la resolución de un procedimiento sancionador, dictada por el Director de la Agencia Española de Protección de Datos, cabe interponer recurso contencioso-administrativo en el plazo de dos meses desde la notificación de la resolución indicada ante la Audiencia Nacional.