



CURSO IMPLANTACIÓN

LOPD/LSSI

MÓDULO 1: LOPD CONCEPTOS LEGALES

Descripción breve

En este módulo vamos a tratar los conceptos básicos legales que debes conocer para el tratamiento de datos.

Eva González Mariscal
Emariscal@induscomp.com

Contenido

¿Qué es un dato personal?	3
¿El correo electrónico tiene la consideración de dato personal?	4
¿Si tengo un blog debo cumplir la LOPD?	4
¿Qué pasa con tu hosting, proveedores de datos y herramientas de mail marketing?	5
¿Qué ocurre en los casos en los que ese prestador de servicios está fuera del territorio del Espacio Económico Europeo?	5
¿Qué pasa si trabajo con empresas como MailChimp que están en EEUU y no tienen estos niveles de protección?	6
¿Qué pasa con el email?	7
Quién debe notificar	8
Obligaciones del titular de los ficheros	10
Inscripción de ficheros.....	10
Calidad de los datos	11
Deber de guardar secreto.....	11
Deber de información	11
Inscripción de ficheros.....	12
Calidad de datos.....	13
Deber de información	19
Tratamiento.....	24
Cesión.....	30
Deber de colaboración con la Agencia	35

Deber de guardar secreto.	38
Atención de los derechos de los ciudadanos.....	39
Glosario de términos.....	43

¿Qué es un dato personal?

Según la definición de la LOPD, un dato personal comprende cualquier información concerniente a **persona física identificada o identificable**. Por tanto debe existir una información o dato y que dicho dato pueda vincularse de forma directa o indirecta a una persona física identificada o identificable.

No serán considerados datos personales:

Aquellos **datos referidos a personas jurídicas** (empresas, sociedades, asociaciones, organismos)

Los ficheros que se limiten a incorporar los **datos de las personas físicas que presten sus servicios en empresas** (personas jurídicas) como nombre y apellidos, funciones o puestos desempeñados, la dirección postal o electrónica, teléfono y número de fax profesionales.

Datos relativos a empresarios individuales, cuando hagan referencia a ellos **en su calidad de comerciantes, industriales o navieros**.

¿El correo electrónico tiene la consideración de dato personal?

Sí, si es de una persona física y no de una empresa o asociación, por ejemplo. Por tanto una bandeja de entrada de un bloguero o de alguien que realice una actividad pública y por tanto tenga emails de persona, ya puede considerarse tratamiento de datos.

¿Si tengo un blog debo cumplir la LOPD?

Si solo publicas posts no. Pero si tienes formularios de suscripción al blog, de contacto o por cualquier otro medio a través de tu blog pides y tratas datos personales, tienes que cumplir con las previsiones legales en materia de protección de datos.

¿Qué pasa con tu hosting, proveedores de datos y herramientas de mail marketing?

Si se almacenan en el servidor de tu proveedor de hosting, sigues siendo el Responsable de Tratamiento, y tu proveedor de hosting será un Encargado de Tratamiento, en tanto en cuanto tiene acceso a esos datos personales que trata (aunque sólo los almacene) siguiendo las instrucciones del Responsable de Tratamiento (en este caso, tú mismo). Pasa lo mismo en el caso de proveedores de herramientas de Mailmarketing como Mailchimp, Mailrelay, Acumbamail o cualquier otro, se recaban datos a través de tu web que se almacenan en los servidores de estos proveedores de servicios. Son también, por tanto Encargados de Tratamiento.

¿Qué ocurre en los casos en los que ese prestador de servicios está fuera del territorio del Espacio Económico Europeo?

Es un supuesto de **transferencia internacional de datos**. En caso que los datos se transfieran a un país que ofrezca un nivel adecuado de protección. Los países con nivel

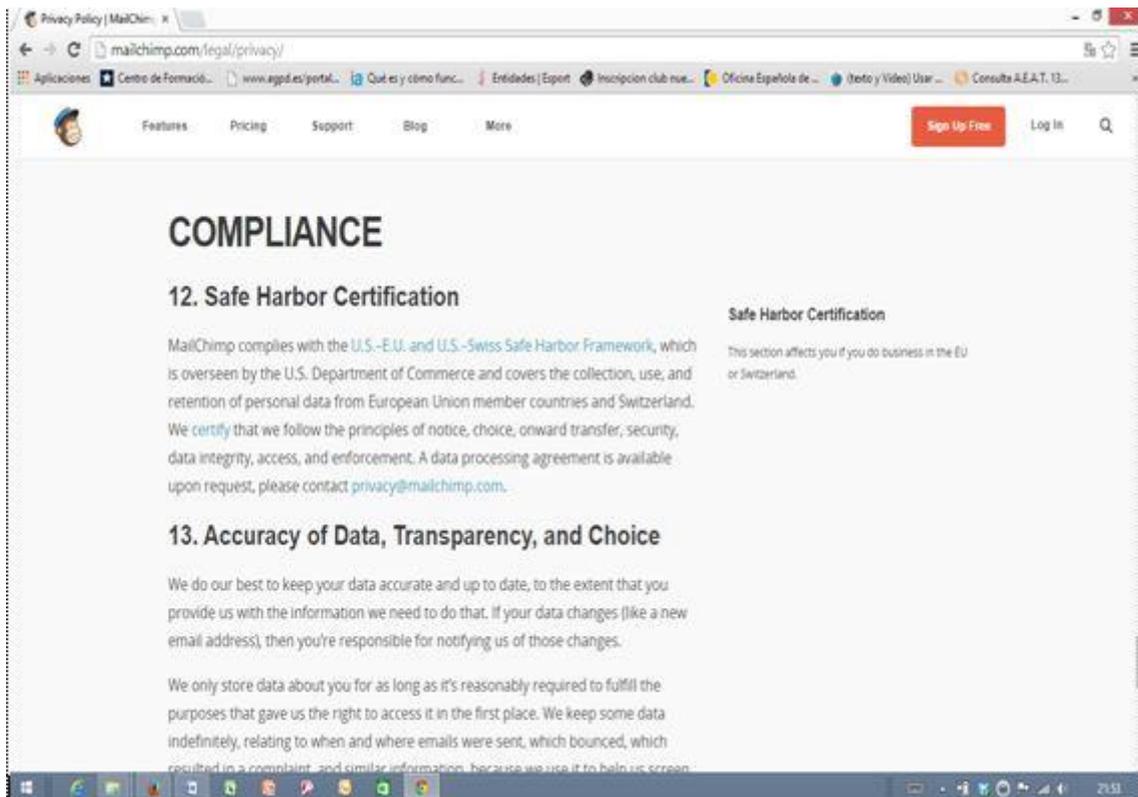
adecuado de protección son los siguientes según la Agencia Española de Protección de Datos:

Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay y Nueva Zelanda.

Si no es así, necesita una **Autorización del Director de la Agencia Española de Protección de Datos. Este trámite dura unos tres meses.**

¿Qué pasa si trabajo con empresas como MailChimp que están en EEUU y no tienen estos niveles de protección?

Puede que se hayan adherido al Convenio de Puerto Seguro (Safe Harbor). Entonces no habría problema en que tus datos pasaran por ella.



¿Qué pasa con el email?

También puede suceder que el contacto que tienes en la web genere un correo electrónico a la dirección de correo que hayas configurado y que por tanto te vayan llegando mails de las diferentes personas que desean contactar contigo. No se está generando un fichero de forma automática, pero puedes ir guardando y ordenando esos datos personales. En ese caso estás generando un fichero.

Esta es la definición de Fichero de la Agencia Española de Protección de Datos: "todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso".

En cualquier caso, tu bandeja de entrada ya podría ser considerada como un fichero, porque de alguna manera puedes sistematizar la búsqueda de esos contactos.

No olvides que también deberías disponer de un documento de seguridad.

Quién debe notificar

Están obligados a notificar la creación de ficheros para su inscripción en el RGPD, de acuerdo con lo dispuesto en la LOPD, aquellas personas físicas o jurídicas, de naturaleza

pública o privada, u órgano administrativo, que procedan a la creación de ficheros que contengan datos de carácter personal. También aquellos entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados y sean responsables de ficheros de datos de carácter personal.

La creación, modificación o supresión de los ficheros de las Administraciones Públicas sólo podrán hacerse por medio de [disposición general](#) publicada en el "Boletín Oficial del Estado" o diario oficial correspondiente.

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

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

Cualquier modificación posterior en el contenido de la inscripción de un fichero en el RGPD, deberá comunicarse a

la Agencia Española de Protección de Datos, mediante una solicitud de modificación o de supresión de la inscripción, según corresponda. En ambos casos será necesario citar el Código de Inscripción asignado por el RGPD al fichero.

La no notificación de la existencia de un fichero supondría una infracción leve, tal y como señala el art. 44.2.b) de la LOPD, quedando sujeto al régimen sancionador previsto en esta Ley.

Obligaciones del titular de los ficheros

Sobre el responsable del fichero o tratamiento recaen las principales obligaciones establecidas por la LOPD y le corresponde velar por el cumplimiento de la Ley en su organización. Entre otros debe:

Inscripción de ficheros

Notificar los ficheros ante el Registro General de Protección de Datos, para que se proceda a su inscripción.

Calidad de los datos

Asegurarse de que los datos sean adecuados y veraces, obtenidos lícita y legítimamente y tratados de modo proporcional a la finalidad para la que fueron recabados.

Deber de guardar secreto

Garantizar el cumplimiento de los deberes de secreto y seguridad.

Deber de información

Informar a los titulares de los datos personales en la recogida de éstos.

Obtener el consentimiento para el tratamiento de los datos personales.

Atención de los derechos de los ciudadanos

Facilitar y garantizar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

Asegurar que en sus relaciones con terceros que le presten servicios, que comporten el acceso a datos personales, se cumpla lo dispuesto en la LOPD.

Cumplir, cuando proceda, con lo dispuesto en la legislación sectorial que le sea de aplicación.

Inscripción de ficheros

Siempre que se proceda al tratamiento de datos personales, definidos en el art. 3.a) de la Ley Orgánica 15/1999, como "cualquier información concerniente a personas físicas identificadas o identificables", que suponga la inclusión de dichos datos en un fichero, considerado por la propia norma, artículo 3.b), como "conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso", el fichero se encontrará sometido a la Ley, siendo obligatoria su inscripción en el Registro General de Protección de Datos (RGPD).

De conformidad con lo dispuesto en el artículo 55 del RLOPD, todo fichero de datos de carácter personal de titularidad pública o privada, con excepción de aquellos ficheros que están expresamente excluidos de la aplicación de la LOPD en su artículo 2.2, como los ficheros mantenidos por las personas físicas en el ejercicio de actividades exclusivamente personales o domésticas (p.e.: agendas de familiares y amigos, ficheros de fotografías personales), serán notificados

a la Agencia Española de Protección de Datos para su inscripción en el Registro General de Protección de Datos.

No solicitar la inscripción de los ficheros de datos de carácter personal en el RGPD constituye infracción leve, con arreglo a lo dispuesto en el artículo 44.2.b) de la LOPD.

Según el artículo 58 del RLOPD, la inscripción de los ficheros deberá encontrarse actualizada en todo momento, por lo que cualquier modificación que afecte al contenido de la inscripción, así como su supresión deberá ser notificada a la AEPD para proceder a la inscripción de la modificación o a la cancelación del fichero.

Calidad de datos

La Ley Orgánica 15/1999 contiene entre sus principios generales, el principio de calidad de los datos, que exige que los mismos sean adecuados a la finalidad que motiva su recogida.

La recogida y tratamiento de datos de carácter personal debe efectuarse también desde su subordinación a la

proporcionalidad en su tratamiento, tal y como establece la Ley.

No puede obviarse que estamos tratando de un auténtico derecho fundamental, cuyo contenido el Tribunal Constitucional ha terminado de perfilar en la Sentencia 292/2000, de 30 de noviembre, denominándolo derecho de autodeterminación informativa o de libre disponibilidad de los datos de carácter personal. Así, en dicha sentencia se indica que este derecho fundamental "persigue garantizar a esa persona el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado", estableciendo, en cuanto a su ámbito, que '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 tercero pueda afectar a sus derechos sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello esta la protección

que el artículo 18. 1 CE otorga, sino los datos de carácter personal".

Concretando más el contenido del derecho, se establece que el poder de disposición y control sobre los datos personales que tal derecho implica "se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos"

Principios relativos a la Calidad de datos (artículos 4 LOPD y 8 RLOPD).

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

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

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

Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las

facultades que a los afectados reconoce el artículo 16 (derechos de rectificación y cancelación).

Cuando los datos hubieran sido comunicados previamente, el responsable del fichero o tratamiento deberá notificar al cesionario, en el plazo de diez días, la rectificación o cancelación efectuada, siempre que el cesionario sea conocido. En el plazo de diez días desde la recepción de la notificación, el cesionario que mantuviera el tratamiento de los datos, deberá proceder a la rectificación y cancelación notificada.

Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados. Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la

legislación específica, se decida el mantenimiento íntegro de determinados datos.

También podrán conservarse los datos durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de la una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado. Una vez cumplido este período los datos sólo podrán ser conservados previa disociación de los mismos, sin perjuicio de la obligación de bloqueo prevista en la LOPD y en su reglamento de desarrollo.

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

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

Constituye infracción de carácter grave, de acuerdo con lo dispuesto en el artículo 44.3.c) de la LOPD "Tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en el artículo 4 de la

presente Ley y las disposiciones que lo desarrollan, salvo cuando sea constitutivo de infracción muy grave", por su parte "La recogida de datos en forma engañosa o fraudulenta" está tipificada como infracción muy grave en el artículo 44.4.a).

Deber de información

El deber de información a las personas de las cuales se vaya a obtener cualquier tipo de datos personales, previo al tratamiento de sus datos de carácter personal, es uno de los principios fundamentales sobre los que se asienta la LOPD y así viene encuadrado dentro de su Título II.

Este principio es, a la vez que una obligación para los responsables de los tratamientos, un derecho de los titulares de los datos y, muchas veces, constituye la primera ayuda que tiene el ciudadano para poder ejercitar el resto de derechos que marca la Ley (Acceso, Rectificación, Cancelación y Oposición). El artículo 5 de la LOPD señala lo siguiente:

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

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

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

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

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

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

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

previsto en las letras a), d) y e) del apartado 1 del presente artículo.

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

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

Por tanto, cada persona de la que se pretenda recabar sus datos personales deberá ser informada previamente de todo

el contenido del artículo 5.1 para que así conozca para qué finalidad se van a tratar, y por quién, pudiendo además en cualquier momento ejercitar sus derechos de acceso, rectificación, cancelación u oposición.

Si la recogida de los datos se ha realizado sin el conocimiento del interesado se le deberá de informar en el plazo de los tres meses siguientes al tratamiento, del contenido de cada uno de los puntos del artículo 5.1, quedando únicamente exceptuados de esta información aquellos supuestos en que una ley expresamente así lo establezca, o cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados a criterio de esta Agencia.

A este respecto, el artículo 19 del RLOPD recoge los siguientes supuestos especiales:

"En los supuestos en los que se produzca una modificación del responsable del fichero como consecuencia de una operación de fusión, escisión, cesión global de activos y pasivos, aportación o transmisión de negocio o rama de actividad empresarial, o cualquier operación de

reestructuración societaria de análoga naturaleza, contemplada por la legislación mercantil, no se producirá cesión de datos, sin perjuicio del cumplimiento por el responsable de lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre".

El incumplimiento del deber de información que contiene el precepto transcrito se encuentra tipificado como falta leve en el artículo 44.2.d) de la Ley Orgánica 15/1999: "El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos sean recabados del propio interesado" y como falta grave en el artículo 44.3.c): "El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos no hayan sido recabados del propio interesado".

Tratamiento

El artículo 5.1.f) del RLOPD define al tratamiento de datos como "cualquier operación o procedimiento técnico, sea o

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

Como regla general, la inclusión de datos de carácter personal en un fichero supondrá un tratamiento de datos de carácter personal, que requerirá, en principio, el consentimiento del afectado.

"Artículo 6. Consentimiento del afectado.

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

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones

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

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

4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos

fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado".

En cuanto al consentimiento, el artículo 3.h) de la Ley Orgánica 15/1999 lo define como tal "toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen". De ello se desprende la necesaria concurrencia para que el consentimiento pueda ser considerado conforme a derecho de los cuatro requisitos enumerados en dicho precepto.

A juicio de esta Agencia la interpretación que ha de darse a estas cuatro notas características del consentimiento, siguiendo a tal efecto los criterios sentados en las diversas recomendaciones emitidas por el Comité de Ministros del Consejo de Europa, será las siguientes:

Libre, lo que supone que el mismo deberá haber sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por el Código Civil.

Específico, es decir, referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento, tal y como impone el artículo 4.2 de la LOPD.

Informado, es decir que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que el mismo se produce. Precisamente por ello el artículo 5.1 de la LOPD impone el deber de informar a los interesados de una serie de extremos que en el mismo se contienen.

Inequívoco, lo que implica que no resulta admisible deducir el consentimiento de los meros actos realizados por el afectado (consentimiento presunto), siendo preciso que exista expresamente una acción u omisión que implique la existencia del consentimiento.

De lo que se ha indicado se desprende que 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; así sucede en el caso de tratamiento de datos especialmente protegidos, indicando el artículo 7.2 la necesidad de consentimiento expreso y escrito para el tratamiento de los datos de ideología, religión, creencias y afiliación sindical, y el artículo 7.3 la necesidad de consentimiento expreso aunque no necesariamente escrito para el tratamiento de los datos relacionados con la salud, el origen racial y la vida sexual.

Por tanto, el consentimiento podrá ser tácito, en el tratamiento de datos que no sean especialmente protegidos (artículo 7.2 y 7.3 de la Ley Orgánica 15/1999) si bien para que ese consentimiento tácito pueda ser considerado inequívoco será preciso otorgar al afectado un plazo prudencial para que pueda claramente tener conocimiento de que su omisión de oponerse al tratamiento implica un consentimiento al mismo, 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 tratamiento de datos sin consentimiento previo del afectado en aquellos supuestos no exceptuados legalmente, puede ser motivo de infracción grave de acuerdo con lo dispuesto en el artículo 44.3.b) de la Ley Orgánica 15/1999.

Cesión.

En cuanto a la cesión de datos, si la misma comporta identificación de concretas personas físicas constituye una comunicación de datos de carácter personal, definida en el artículo 3.i) de la Ley Orgánica 15/1999, como "toda revelación de datos realizada a persona distinta del interesado".

El régimen de las cesiones de datos se contiene en el artículo 11 de la citada Ley Orgánica:

"Artículo 11. Comunicación de datos.

1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento

de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

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

a) Cuando la cesión está autorizada en una Ley.

b) Cuando se trate de datos recogidos de fuentes accesibles al público.

c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

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

destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

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

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

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

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

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

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

La comunicación de datos entre Administraciones públicas se regula en el artículo 21 de la LOPD.

"Artículo 21. Comunicación de datos entre Administraciones públicas.

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

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

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

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

A tenor del artículo 44.4.k) de la LOPD se considera infracción grave "La comunicación o cesión de datos de carácter personal sin contar con legitimación para ello en los términos previstos en esta Ley y sus disposiciones reglamentarias de desarrollo, salvo que la misma sea constitutiva de infracción muy grave". La consideración como infracción muy grave tendría lugar cuando se llevase a cabo una transferencia internacional de datos a países que no proporcionan un nivel de protección adecuado sin la autorización del Director de la

Agencia Española de Protección de Datos (artículo 44.4.d) LOPD).

Deber de colaboración con la Agencia

Entre las funciones que el artículo 37 de la LOPD atribuye a la Agencia Española de Protección de Datos se encuentra la de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos (artículo 37.1.a), así como las de:

Requerir a los responsables y los encargados del tratamiento, previa su audiencia, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de la LOPD y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones (artículo 37.1.f).

Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones (artículo 37.1.g).

Ejercer la potestad sancionadora en los términos previstos en la LOPD (artículo 37.1.g).

Artículo 40. "Potestad de inspección.

1. Las autoridades de control podrán inspeccionar los ficheros a que hace referencia la presente Ley, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos. A tal efecto, podrán solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados"

Régimen sancionador

La falta de colaboración está considerada como infracción según el artículo 44 de la LOPD, conforme a los siguientes tipos:

Como infracción leve

No remitir a la Agencia Española de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo.

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

Como infracción grave

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

La obstrucción al ejercicio de la función inspectora.

Como infracción muy grave

No cesar en el tratamiento ilícito de datos de carácter personal cuando existiese un previo requerimiento del Director de la Agencia Española de Protección de Datos para ello.

Artículo 49. "Potestad de inmovilización de ficheros

En los supuestos constitutivos de infracción grave o muy grave en que la persistencia en el tratamiento de los datos de carácter personal o su comunicación o transferencia

internacional posterior pudiera suponer un grave menoscabo de los derechos fundamentales de los afectados y en particular de su derecho a la protección de datos de carácter personal, el órgano sancionador podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido, el órgano sancionador podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas".

Deber de guardar secreto.

El artículo 10 de la Ley Orgánica 15/1999 exige a quienes intervengan en cualquier fase del tratamiento de los datos, en el amplio sentido en que lo define el artículo 3,c), guardar secreto profesional sobre los datos, subsistiendo la obligación aun después de finalizar su relación con el responsable del fichero.

"Artículo 10. Deber de secreto.

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

El incumplimiento del deber de secreto constituye infracción grave de acuerdo con lo previsto en el artículo 44.3.d) de la LOPD: "La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la presente Ley".

Atención de los derechos de los ciudadanos

La LOPD establece como derechos de los ciudadanos de carácter personalísimo, cuyo ejercicio habrá de hacerse efectivo por los responsables del tratamiento de los datos, los siguientes:

Derecho de acceso

Derecho de rectificación y cancelación

Derecho de oposición

Es competencia de la Agencia Española de Protección de Datos la tutela de los derechos de acceso, rectificación, cancelación y oposición (ARCO). Ante una denegación del ejercicio de estos derechos queda abierta la posibilidad, de la que deberán informar los responsables de los ficheros, de solicitar dicha tutela formulando la correspondiente reclamación en la forma prescrita en el Capítulo I del Título III del RLOPD (artículos 23 y siguientes).

Según el artículo 44.3.e) de la LOPD constituye falta grave "El impedimento o la obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación y oposición"

El artículo 23 de la LOPD establece las

"Excepciones a los derechos de acceso, rectificación y cancelación.

Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior (datos personales recogidos para fines policiales por las Fuerzas y Cuerpos de Seguridad sin consentimiento de los afectados, así como los relativos a la ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual recogidos y tratados cuando sea absolutamente necesario para fines de una investigación concreta) podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o

la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

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

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

Glosario de términos

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

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

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

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

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

Responsable del fichero o del tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

En el caso de entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados, se considerará responsable del tratamiento a la persona o personas integrantes de los mismos.

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

En el caso de entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados, se considerará encargado del tratamiento a la persona o personas integrantes de los mismos.

Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento.

Tercero: la persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.

En el caso de entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados, se considerará tercero a la persona o personas integrantes de los mismos.

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

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

Transcurrido ese plazo deberá procederse a la supresión de los datos.

Datos de carácter personal relacionados con la salud: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se

consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.

Cesión o comunicación de datos: tratamiento de datos que supone su revelación a una persona distinta del interesado.

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

En el caso de entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados, se considerará destinatario a la persona o personas integrantes de los mismos.

Transferencia internacional de datos a países terceros: 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.

Exportador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español y responsable del tratamiento de los datos de carácter personal que son objeto de transferencia internacional a un país tercero.

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

Dato disociado: aquél que no permite la identificación de un afectado o interesado .

Procedimiento de disociación: todo tratamiento de datos personales que permita la obtención de datos disociados.

Bloqueo: la identificación y reserva de datos de carácter personal con el fin de impedir su tratamiento excepto por parte de las Administraciones públicas, Jueces y Tribunales para la atención de las posibles responsabilidades nacidas

del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades.

Supresión: la eliminación física de los datos de carácter personal bloqueados una vez cumplido el plazo de prescripción de las posibles responsabilidades nacidas del tratamiento durante el cual se guardaron bloqueados.

Ficheros de titularidad pública: los ficheros de los que sean responsables los Órganos constitucionales o con relevancia constitucional del Estado o las Instituciones Autonómicas con funciones análogas a las mismas, las Administraciones Públicas Territoriales, las entidades u organismos dependientes de las mismas con personalidad jurídica pública y sometidas al derecho administrativo y las Corporaciones de derecho público, exclusivamente en cuanto dichos ficheros se encuentren estrictamente vinculados al ejercicio de las potestades de derecho público que a las mismas atribuye su normativa específica.

Ficheros de titularidad privada: los ficheros de los que sean responsables las entidades sometidas al derecho privado, no vinculados en ningún caso con el ejercicio de potestades de

derecho público, incluyendo aquellos de los que sean responsables las fundaciones no sanitarias del sector público, las sociedades del sector público empresarial del Estado, Comunidades Autónomas, Provincias o Municipios, con independencia de su estructura accionarial, y las Corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de las potestades de derecho público que a las mismas atribuye su normativa específica.

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

pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación.

Sistema de información: conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.

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

Identificación: procedimiento de reconocimiento de la identidad de un usuario.

Autenticación: procedimiento de comprobación de la identidad de un usuario.

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

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

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

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

Transmisión de documentos: cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.

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

DNI electrónico: es el documento que acredita física y digitalmente la identidad personal de su titular y permite la firma electrónica de documentos.

Firma electrónica: es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación personal.

Firma electrónica avanzada: es aquella firma electrónica que permite establecer la identidad personal del suscriptor respecto de los datos firmados y comprobar la integridad de los mismos, por estar vinculada de manera exclusiva tanto al suscriptor, como a los datos a que se refiere, y por haber sido creada por medios que mantiene bajo su exclusivo control.

Firma electrónica reconocida: es aquella firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

Clave Pública y Clave Privada: la criptografía asimétrica en la que se basa la PKI emplea un par de claves en la que lo que se cifra con una de ellas sólo se puede descifrar con la otra y viceversa. A una de esas claves se la denomina pública y se la incluye en el certificado electrónico, mientras que a la otra se la denomina privada y únicamente es conocida por el titular del certificado.

Clave Personal de Acceso (PIN): secuencia de caracteres que permiten el acceso a los certificados.

Dispositivo seguro de creación de Firma: instrumento que sirve para aplicar los datos de creación de firma cumpliendo con los requisitos que establece el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

Documento electrónico: conjunto de registros lógicos almacenado en soporte susceptible de ser leído por equipos electrónicos de procesamiento de datos, que contiene información.

Función hash: es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es imposible encontrar dos mensajes distintos que generen el mismo resultado al aplicar la Función hash.

Hash o Huella digital: resultado de tamaño fijo que se obtiene tras aplicar una función hash a un mensaje y que cumple la propiedad de estar asociado unívocamente a los datos iniciales.

Listas de Revocación de Certificados o Listas de Certificados Revocados: lista donde figuran exclusivamente las relaciones de certificados revocados o suspendidos (no los caducados).

Prestador de Servicios de Certificación: persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

Con independencia de los términos citados anteriormente, para obtener más información sobre determinados conceptos podrá consultar en las siguientes direcciones:

- Glosario de Términos sobre Internet y SPAM, en la página web de esta AEPD, (www.agpd.es),

- Glosario de Términos sobre DNI electrónico (www.dnielectronico.es)