

GUÍA

del Responsable de Ficheros

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



©AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
NIPO: 052-08-001-5

Diseño Gráfico: 

Imprime: NILO Industria Gráfica, S.A.

GUÍA

de Protección de Datos para Responsables de Ficheros

GUÍA

de Protección de Datos para los Responsables de Ficheros

índice

Introducción	4	
	4	¿ES IMPORTANTE!
	6	¿QUIÉN ES RESPONSABLE?
	8	¿QUIÉN ES EL ENCARGADO?
	10	¿CUÁNDO SE TRATAN DATOS PERSONALES?
	12	CONSEGUIR AYUDA
Mis Obligaciones	14	
	14	NOTIFICACIÓN DE FICHEROS
	14	Deber de notificar
	16	Requisitos ámbito público y privado
	18	Los ficheros no automatizados también
	19	AL RECOGER Y TRATAR DATOS
	19	Informar a los afectados
	21	Pedir su consentimiento
	24	DATOS ESPECIALMENTE PROTEGIDOS
	26	CALIDAD Y PROPORCIONALIDAD DE LOS DATOS
	27	¡ATENCIÓN DE LOS DERECHOS DE LOS CIUDADANOS!
	30	AL RECIBIR UN SERVICIO EN EL QUE SE ACCEDE A LOS DATOS
	32	AL COMUNICAR DATOS A TERCEROS
	34	EN TRANSFERENCIAS INTERNACIONALES
	36	MEDIDAS DE SEGURIDAD
	37	Niveles de seguridad
	40	Divulgar y controlar
	41	DEBER DE GUARDAR SECRETO
	42	SANCIONES
	43	DEBER DE COLABORAR CON LA AGENCIA
Anexo	44	Notificaciones telemáticas de la AEPD
	45	COMO NOTIFICAR
	47	PASOS PARA LA CUMPLIMENTACIÓN DEL FORMULARIO

¡ES IMPORTANTE!

Toda persona física tiene derecho a la protección de los datos de carácter personal que la conciernen y este derecho le atribuye la facultad de controlar sus datos

CONSTITUCIÓN ESPAÑOLA
LEY ORGÁNICA 15/1999 DE PROTECCIÓN DE DATOS
CARTA DE DERECHOS FUNDAMENTALES DE LA
UNIÓN EUROPEA
**RECONOCEN EL DERECHO FUNDAMENTAL A LA
PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.**

LAS EMPRESAS Y ORGANISMOS PÚBLICOS TRATAN DATOS DE CARÁCTER PERSONAL Y ESTÁN OBLIGADOS A GARANTIZAR EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS.

La Constitución Española en su artículo 10 reconoce el derecho a la dignidad de la persona. Por su parte, el artículo 18.4 dispone que la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

De ambos preceptos deriva el derecho fundamental a la protección de datos de carácter personal, que ha sido definido como autónomo e independiente por la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre.

En desarrollo del citado artículo 18.4, y como trasposición al ordenamiento jurídico español de la Directiva 95/46/CE (Directiva sobre protección de datos), fue aprobada la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD). La Ley tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor e intimidad personal y familiar.

La LOPD establece las obligaciones que los responsables de los ficheros y los encargados de los tratamientos, tanto de organismos públicos como privados, han de cumplir para garantizar la observancia del derecho a la protección de los datos de carácter personal.

La Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones (LGT) y la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI) atribuyen a la Agencia la tutela de los derechos y garantías de abonados y usuarios en el ámbito de las comunicaciones electrónicas, en relación con las comunicaciones comerciales remitidas por correo electrónico o medios equivalentes y sobre el empleo de dispositivos de almacenamiento de la información en equipos terminales.

Esta guía abordará los aspectos fundamentales que se deben tener en cuenta.

¿QUIÉN ES RESPONSABLE?

El responsable de un fichero o tratamiento es la entidad, persona o el órgano administrativo que decide sobre la finalidad, el contenido y el uso del tratamiento de los datos personales.

Una empresa, será la responsable de los ficheros que contienen datos relativos a sus empleados y a sus clientes; un autónomo o empresario individual será responsable del tratamiento de los datos personales de sus clientes, un hotel será responsable del fichero de sus huéspedes; un gimnasio será responsable del fichero de sus socios; un centro educativo será responsable del fichero de sus alumnos, un Ayuntamiento será responsable del fichero del padrón...

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

- Notificar los ficheros ante el Registro General de Protección de Datos para que se proceda a su inscripción.
- 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.
- Garantizar el cumplimiento de los deberes de secreto y seguridad.
- Informar a los titulares de los datos personales en la recogida de éstos.
- Obtener el consentimiento para el tratamiento de los datos personales.
- 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.

Información para el responsable en www.agpd.es -> Canal del Responsable

¿QUIÉN ES EL ENCARGADO?

El encargado del tratamiento es 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.

Una empresa que preste servicios para la realización de envíos postales; el informático ajeno a la organización del responsable que realiza tareas de mantenimiento de software o hardware; el gestor administrativo que confecciona nóminas y gestiona el fichero de personal...

Asociada a la figura del responsable, está la figura del encargado, que es la persona o entidad, autoridad pública, servicio o cualquier otro organismo que, sólo o con otros, trate datos por cuenta del responsable del fichero.

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

No se considera encargado del tratamiento a la persona física que tenga acceso a los datos personales en su condición de empleado dentro de la relación laboral que mantiene con el responsable del fichero.

Ambos, encargado y responsable del tratamiento, pueden ser sancionados de acuerdo a la LOPD si incumplen sus obligaciones.

¿CUÁNDO SE TRATAN LOS DATOS PERSONALES?

Los datos personales permiten identificar a una persona

Si se recogen y tratan el nombre, los apellidos, la fecha de nacimiento, la dirección postal o la dirección de correo electrónico, el número de teléfono, el número de identificación fiscal, la huella digital, el ADN, una fotografía, el número de seguridad social, ... se están usando datos que identifican a una persona, ya sea directa o indirectamente.

Se están tratando datos personales y se deben cumplir las obligaciones que impone la LOPD salvo que sea en el ejercicio de actividades exclusivamente personales o domésticas.

Es habitual que prácticamente para cualquier actividad sea necesario que los datos personales se recojan y utilicen en la vida cotidiana. La LOPD regula el tratamiento de cualquier tipo de dato personal con independencia de que éste pertenezca o no a la vida privada del titular. La LOPD se aplica a los tratamientos de datos personales privados y públicos.

Una persona facilita sus datos personales cuando abre una cuenta en el banco, cuando se matricula en un curso de idiomas, cuando se apunta al gimnasio, cuando solicita participar en un concurso, cuando reserva un vuelo o un hotel, cuando pide hora para una consulta médica, cuando busca trabajo, cada vez que efectúa un pago con su tarjeta de crédito, cuando navega por Internet.....

Si se tratan estos datos, se deben seguir las recomendaciones de esta guía. No obstante existen excepciones a las obligaciones fijadas por la LOPD. Según su artículo 2.2 la LOPD no será de aplicación :

- A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
- A los ficheros sometidos a la normativa sobre protección de materias clasificadas.
- A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos.

Por otra parte, según lo dispuesto por el artículo 2.3 de la LOPD determinados tratamientos se registrarán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por la LOPD. Se trata de los ficheros regulados por la legislación de régimen electoral; los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública; los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas; los derivados del Registro Civil y del Registro Central de penados y rebeldes; los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

CONSEGUIR AYUDA

LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) protege los derechos de los ciudadanos. Es el ente de derecho público que vela por el cumplimiento de la normativa sobre protección de datos personales en todos los ámbitos, público y privado, por lo que actúa con plena independencia de las Administraciones Públicas

INFORMA sobre el contenido, los principios y las garantías del derecho fundamental a la protección de datos regulado en la LOPD.

AYUDA al ciudadano a ejercitar sus derechos.

AYUDA a los responsables y encargados de tratamientos a cumplir las obligaciones que establece la LOPD y a resolver sus dudas.

GARANTIZA el derecho a la protección de datos investigando aquellas actuaciones de los responsables o encargados de ficheros que puedan ser contrarias a los principios y garantías contenidos en la LOPD, bien de oficio, o por denuncia de un particular. Impone, en estos casos, las correspondientes sanciones.

La Agencia Española de Protección de Datos (en adelante AEPD), emite dictámenes jurídicos sobre las cuestiones de mayor complejidad en esta materia.

La Agencia facilita el derecho de consulta de los ciudadanos permitiendo acceder a información básica relativa a todos los ficheros públicos y privados inscritos en el Registro General de Protección de Datos.

Con naturaleza preventiva, la Subdirección General de Inspección de la AEPD realiza también Inspecciones Sectoriales de Oficio, que se caracterizan por suponer una evaluación de todas las garantías previstas en la normativa de protección de datos. El objetivo es posibilitar que se constaten todas las deficiencias que existan en el cumplimiento de la citada normativa y que se formulen las oportunas recomendaciones para su corrección.

La Agencia cuenta con un área de Atención al Ciudadano que informa y asesora a la ciudadanía sobre todos los aspectos relacionados con la LOPD.

Dirígete a la Agencia:

al teléfono **901 100 099**
a través de correo electrónico **ciudadano@agpd.es**
visitando la página web **www.agpd.es**
por correo a la
Agencia Española de Protección de Datos,
Jorge Juan 6 - 28001 Madrid
o al fax **91 445 56 99**

En el canal de documentación se encuentran recomendaciones e informes jurídicos:
www.agpd.es -> Canal de Documentación

NOTIFICACIÓN DE FICHEROS

DEBER DE NOTIFICAR

LA CREACIÓN DE FICHEROS SE DEBE NOTIFICAR PARA SU INSCRIPCIÓN EN EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS (RGPD) DE LA AEPD

¿QUIÉN LO HACE?

El responsable del fichero

¿CUÁNDO?

- Con anterioridad al uso de los ficheros.
- Cuando se producen cambios respecto a la inscripción inicial.
- Cuando cesa el uso del fichero.

¿QUÉ IMPLICA?

El compromiso por parte del responsable de que el fichero declarado para su inscripción cumple con todas las exigencias legales

¿QUÉ COSTE TIENE?

Ninguno

¿PARA QUÉ?

Permite que los titulares de los datos puedan conocer quienes son los responsables de los ficheros ante los que ejercitar directamente los derechos de acceso, rectificación, cancelación y oposición

La no notificación de la existencia de un fichero supondría una infracción leve o grave, tal y como señala el art. 44 de la LOPD, quedando sujeto al régimen sancionador previsto en esta Ley.

El Registro General de Protección de Datos es el órgano al que corresponde velar por la publicidad de la existencia de los ficheros que contengan datos de carácter personal, con miras a hacer posible el ejercicio de los derechos de acceso, rectificación, oposición y cancelación, regulados en los artículos 14 a 16 de la LOPD. Por ello es el encargado de la gestión de las inscripciones. El acceso al Registro es público y gratuito y puede consultarse en la web de la Agencia.

De conformidad con el artículo 39 de la citada Ley serán objeto de inscripción en el Registro:

- Los ficheros de los que sean titulares las Administraciones Públicas.
- Los ficheros de titularidad privada.
- Las autorizaciones de transferencias internacionales.
- Los códigos tipo.
- Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

Consulta de ficheros inscritos en el Registro General de Protección de Datos
en:www.agpd.es -> Ficheros y tratamientos inscritos

REQUISITOS ÁMBITO PUBLICO Y PRIVADO

PRIVADO

Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulten necesarios 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.

PÚBLICO

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 (art. 20.1 de la LOPD).

El artículo 20.2 de la LOPD indica los contenidos de la disposición general que también concreta el artículo 54 del Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre de protección de los datos de carácter personal (RDLOPD). La disposición deberá contener:

- La identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos.

- El origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia.
- La estructura básica del fichero mediante la descripción detallada de los datos especialmente protegidos y los datos identificativos, así como las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización.
- Las comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios.
- Las transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos.
- Los órganos responsables del fichero.
- Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
- El nivel básico, medio o alto de seguridad que resulte exigible, de acuerdo con lo establecido en el Título VIII del RDLOPD.

Las disposiciones de supresión de los ficheros establecerán el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción (art. 20.3 LOPD).

El art. 44.3.a) de la LOPD establece que proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general publicada en el BOE o diario oficial correspondiente, constituye una infracción grave.

La falta de cumplimiento de todos los trámites citados anteriormente da lugar a que la inscripción no se actualice y el RGPD pierda su exactitud, en detrimento del derecho fundamental del ciudadano en relación con la protección de sus datos personales.

LOS FICHEROS NO AUTOMATIZADOS TAMBIÉN

La LOPD define el fichero como:

"todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso"
(artículo 3.b)

Los ficheros no automatizados también deben cumplir las obligaciones de la LOPD.

El artículo 5.1 n) del RDLOPD ha completado esta definición.

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 su datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica".

AL RECOGER Y TRATAR DATOS

INFORMAR A LOS AFECTADOS

Deben conocer para qué se utilizan sus datos.

Deben conocer que existe un fichero o un tratamiento con sus datos.

Se debe indicar el responsable del fichero y su dirección o la de su representante.

Cualquier persona tiene derecho a saber si sus datos personales van a ser incluidos en un fichero, y los tratamientos que se realizan con esos datos.

Los responsables tienen obligación de informar al ciudadano cuando recojan datos personales que le afecten. Este derecho de información es esencial porque garantiza que el consentimiento que se preste sea previo, específico e informado y es necesario para permitir el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

El art. 5 de la LOPD recoge la obligación que tienen los responsables de ficheros o tratamientos de informar a los ciudadanos de la incorporación de sus datos a un fichero, de la identidad y dirección del responsable, de la finalidad del fichero, de los destinatarios de la información, del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos, así como de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

La ley exige del deber de informar sobre algunos de estos aspectos cuando se deduzcan inequívocamente de la naturaleza de los propios datos personales y de las circunstancias en las que se produce la recogida.

Esta información debe estar incluida en los cuestionarios o impresos de recogida de los datos. En el caso de utilizar Internet como medio de recogida de los datos, también debe 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 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 lenguaje 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 personales.

En el caso de que los datos de carácter personal no hubieran sido recabados del interesado, el responsable del fichero o su representante deben informarle de esa recogida en el plazo de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad.

El incumplimiento del deber de información se encuentra tipificado como **falta leve** en el artículo 44.2.d) de la Ley Orgánica 15/1999: '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'.

PEDIR SU CONSENTIMIENTO

Sólo así se podrán tratar los datos del interesado

No será necesario el consentimiento:

- Si el tratamiento tiene por objeto la satisfacción de un interés legítimo del responsable y lo autoriza una norma con rango de Ley o una norma de derecho siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la LOPD o cuando sea necesario para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas.
- Si el tratamiento es necesario para el mantenimiento o cumplimiento de un contrato o precontrato de una relación negocial, laboral o administrativa y los datos se refieren a las partes.
- Si el tratamiento es necesario para proteger un interés vital del interesado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento y el tratamiento de los datos es necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos siempre que dicho tratamiento de datos se realice por un profesional sanitario.
- Si el tratamiento es necesario para cumplir las funciones de las Administraciones Públicas en el ámbito de sus competencias.
- Cuando una Ley habilite el tratamiento sin requerir el consentimiento inequívoco de su titular.
- Cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo del responsable del fichero o de un tercero a quien se comuniquen los datos.

El artículo 3.h) de la Ley Orgánica 15/1999 define el consentimiento como "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 que para que el consentimiento pueda ser considerado conforme a derecho deben darse los cuatro requisitos enumerados.

Así, no se infiere necesariamente su carácter expreso, salvo en los casos en que se señala en la LOPD, como en el caso del tratamiento de datos especialmente protegidos. El artículo 7.2 indica 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.

El consentimiento podrá ser tácito, en el tratamiento de datos que no sean especialmente protegidos. En este caso será preciso otorgar al afectado un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal. El responsable del tratamiento debe conocer si la comunicación ha sido objeto de devolución por cualquier causa. Si efectivamente ha sido devuelta no podrá proceder el tratamiento de los datos referidos a ese interesado. El afectado debe disponer de un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos como un envío prefranqueado al responsable del tratamiento, la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido. Una vez planteada, este tipo de solicitud de consentimiento no será posible nuevamente respecto de los mismos tratamientos y para las mismas finalidades en el plazo de un año a contar de la fecha de la solicitud.

En el caso de los menores de edad hay que distinguir entre los mayores de catorce años que pueden 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.

Una manifestación específica del consentimiento se da en el caso del envío de comunicaciones comerciales realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes regulados por la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico. Este tipo de comunicaciones sólo podrá realizarse cuando hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas (opt-in). También podrán realizarse cuando exista una relación contractual previa, siempre que se hubieran obtenido de forma lícita los datos de contacto del destinatario y se emplearan para el envío de comunicaciones comerciales referentes a productos o servicios de la propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente (opt-out). En cualquier caso el prestador debe ofrecer al destinatario la posibilidad de oponerse a su envío mediante un procedimiento sencillo y gratuito.

El tratamiento de datos sin consentimiento previo del afectado en los supuestos no exceptuados legalmente, puede ser motivo de infracción grave de acuerdo con el artículo 44.3.c) de la LOPD y la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico considera infracción leve el envío de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente cuando en dichos envíos no se cumplan los requisitos de la Ley y no constituya infracción grave.

Consentimiento del afectado en:www.agpd.es -> Canal del Responsable del fichero -> Obligaciones -> Tratamiento y Cesión -> Tratamiento

DATOS ESPECIALMENTE PROTEGIDOS

La Constitución Española establece:

“Nadie podrá ser obligado a declarar sobre su ideología, religión o creencias”

Advertir al interesado de su derecho a no prestar su consentimiento en el tratamiento de estos datos.

Se necesita consentimiento expreso y por escrito del interesado para el tratamiento de datos que revelen ideología, afiliación sindical, religión y creencias.

Se necesita consentimiento expreso o que lo disponga una ley para recabar, tratar o ceder datos relativos a origen racial, salud o vida sexual.

No se permite crear ficheros con la única finalidad de almacenar datos de carácter personal, que revelen ideología, afiliación sindical, religión, origen racial, salud o vida sexual.

Se podrán tratar, no obstante, los datos anteriores, si resulta necesario para el diagnóstico médico o la asistencia sanitaria.

La LOPD en sus artículos 7 y 8 incluye algunas reglas específicas:

- No necesitan consentimiento expreso los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.
- Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras.
- Los datos especialmente protegidos podrán ser objeto de tratamiento cuando éste resulte necesario para la prevención o para el diagnóstico médico o la gestión de un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. Igualmente cuando sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.
- Puede llegar a constituir infracción de carácter grave y muy grave, de acuerdo con lo dispuesto en los artículos 44.3.c), 44.3.g), 44.4.c) y 44.4.g), no respetar determinadas obligaciones y restricciones establecidas en el artículo 7 de la LOPD.

CALIDAD Y PROPORCIONALIDAD DE LOS DATOS

Los datos deben recogerse con fines determinados explícitos y legítimos ➡ No usarlos para otros fines.

Los datos deben ser adecuados, pertinentes y no excesivos en relación con esa finalidad ➡ No recogerlos si no son necesarios.

Los datos deben ser exactos y responder con veracidad a la situación del titular ➡ Mantenerlos actualizados

Los datos sólo deben conservarse durante el tiempo necesario para las finalidades del tratamiento para las que han sido recogidos ➡ Cancelarlos si ya no son necesarios

El artículo 4 de la LOPD incluye todos estos principios bajo el concepto de “calidad” de los datos. Además, permite el tratamiento para fines distintos a los de recogida en el caso de uso posterior para fines históricos, estadísticos o científicos. Asimismo permite por excepción conservar datos que no sean ya necesarios de acuerdo al tratamiento para el que hubieran sido recogidos en caso de valor histórico, estadístico o científico fijado por Ley.

Constituye infracción de carácter grave, de acuerdo con lo dispuesto en el artículo 44.3.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'

ATENCIÓN DE LOS DERECHOS DE LOS CIUDADANOS

El titular de los datos que se tratan tiene derecho gratuitamente

A solicitar y obtener información de sus datos de carácter personal sometidos a tratamiento, y del origen de dichos datos así como las comunicaciones realizadas o que se prevén hacer de los mismos.

Derecho de acceso

Plazo de contestación: 1 mes desde la solicitud
Acceso: 10 días desde la notificación de estimación de la solicitud

A que se actualicen sus datos si son inexactos o incompletos.

Derecho de rectificación

Plazo: 10 días

A que se borren o se supriman sus datos si son inexactos o se han tratado ilegalmente.

Derecho de cancelación

Plazo: 10 días

A solicitar que no se traten sus datos.

Derecho de oposición

Plazo: 10 días

Existe la obligación de contestar al solicitante aunque no figuren datos suyos y se debe hacer por medios que permitan acreditar el envío y la recepción de la notificación.

- El **DERECHO DE ACCESO** podrá ejercitarse a intervalos de 12 meses sin necesidad de que el titular de los datos personales alegue justificación alguna. Podrá ejercerse en periodos inferiores cuando se invoque un interés legítimo.

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

Deberá resolverse la solicitud en un plazo de un mes desde su recepción y satisfacerse en los siguientes diez días a la notificación de la resolución.

- El **DERECHO DE RECTIFICACION** exige al titular 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. La rectificación deberá hacerse efectiva en un plazo de diez días.
- El **DERECHO DE CANCELACION** requiere indicar si revoca el consentimiento otorgado, en los casos en que la revocación proceda, o si, por el contrario, se trata de un dato erróneo o inexacto, en cuyo caso deberá acompañar la documentación justificativa. La cancelación deberá atenderse en un plazo de diez días. La cancelación dará lugar al bloqueo de los datos, cuando sea preciso conservar éstos únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

Si los datos a rectificar o cancelar hubieran sido cedidos previamente a un tercero, el responsable del fichero notificará al cesionario la rectificación o cancelación efectuada.

- La LOPD contempla excepciones a los derechos de acceso, rectificación y cancelación en el caso de los ficheros de las Fuerzas y Cuerpos de Seguridad, que podrán denegarse 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.

Otras excepciones afectan a los ficheros de la Hacienda Pública que podrán denegar el ejercicio de los derechos 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.

- Cuando se haya tratado un dato sin consentimiento del titular en los casos previstos por el artículo 6.2 LOPD, éste tiene el **DERECHO DE OPOSICIÓN**. Éste derecho supone que el titular, siempre que una ley no disponga lo contrario, 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 el caso de los datos obtenidos de fuentes accesibles al público el titular de los datos personales tendrá derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que le conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre él figuren en aquél, a su simple solicitud.

- Los derechos de acceso, oposición al tratamiento, rectificación y cancelación no son absolutos. El responsable del fichero o tratamiento podrá denegarlos cuando concurra causa legal para ello, como por ej. cuando se haya ejercitado el derecho de acceso en los últimos doce meses y no se alegue interés legítimo o cuando exista un deber legal de conservación en el caso de la cancelación. Del

mismo modo la existencia de una relación jurídica que legitime para el tratamiento podría facultar para denegar una cancelación cuando la conservación del dato resulte necesaria para el cumplimiento de las obligaciones contractuales. En caso de denegación, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las Comunidades Autónomas.

- De acuerdo con lo previsto en el artículo 44.3.e) de la propia Ley Orgánica, constituye **infracción grave**, el impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada. También puede considerarse, a tenor del art. 44.4.h) de la misma Ley, como **infracción muy grave** la circunstancia de no atender u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.

Deber de información en www.agpd.es -> Canal del responsable -> Obligaciones -> Atención de los derechos de los ciudadanos

AL RECIBIR UN SERVICIO EN EL QUE SE ACCEDE A LOS DATOS

La realización de ese tratamiento por terceros, a los que denominaremos encargados del tratamiento, deberá estar regulada por un **contrato** escrito o cualquier otra forma que permita acreditar su celebración y contenido que expresamente indique las obligaciones del encargado del tratamiento.

Los datos sólo se tratarán conforme a las instrucciones del responsable del fichero.
Los datos no se utilizarán con fin distinto al establecido en el contrato.
Los datos no se comunicarán, ni para conservación, a otras personas.
Las medidas de seguridad a implementar.
La destrucción o devolución de los datos una vez cumplido el contrato.

El artículo 12 de la LOPD regula el acceso a los datos por cuenta de terceros.

El responsable del fichero o tratamiento debe ser diligente en la elección del encargado asegurándose de que cumplirá adecuadamente las condiciones del encargo respetando escrupulosamente todas las previsiones en materia de protección de datos. El contenido del contrato no deberá limitarse a una simple reproducción de lo dispuesto por el artículo 12 LOPD y deberá establecer de modo específico las obligaciones del encargado.

Si fuese necesaria una subcontratación deben cumplirse los siguientes requisitos establecidos en el RDLOPD:

- Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar. Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.
- Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.
- Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato previsto por el artículo 12 LOPD.

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

AL COMUNICAR DATOS A TERCEROS

Es necesario (arts. 11 y 21 LOPD), el consentimiento previo del interesado.

No será necesario el consentimiento del interesado para la cesión

que tenga por objeto la satisfacción de un interés legítimo del cesionario y lo autorice una norma con rango de Ley o una norma de derecho siempre que no prevalezca el interés a los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la LOPD o cuando la cesión de los datos sea necesaria para cumplir un deber que imponga una de dichas normas.

Que esté autorizada por Ley.

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

En caso de que exista una relación jurídica que implique la cesión y ésta se limite a la finalidad 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.

En caso de urgencia relativa a la salud o para la realización de estudios epidemiológicos en los casos legalmente previstos.

Además de en los casos anteriores para las cesiones de datos entre Administraciones Públicas no será necesario el consentimiento

cuando se realicen entre Administraciones Públicas con fines históricos, estadísticos o científicos

Si se trata de datos recogidos de fuentes accesibles al público excepto si se destinan a ficheros privados

Para el ejercicio de las mismas competencias o de competencias que versen sobre las mismas materias

Si se trata de los datos de carácter personal que una Administración Pública obtenga o elabore con destino a otra.

El responsable del fichero o tratamiento deberá informar al titular en el momento en que se 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 este modo, cuando la cesión venga impuesta por Ley, cuando se trate de un cesión sin consentimiento basada en la existencia 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.

A tenor del artículo 44.4 b) de la Ley Orgánica se considera infracción muy grave la cesión de datos de carácter personal sin consentimiento del interesado, fuera de los casos en que estén permitidas.

Comunicación de datos en www.agpd.es -> Canal del responsable -> Obligaciones -> Tratamiento y cesión -> Cesión

EN TRANSFERENCIAS INTERNACIONALES

Se considera una transferencia internacional cualquier tratamiento que suponga una transmisión de datos fuera del Espacio Económico Europeo, tanto si se realiza una cesión de datos, como si tuviera por objeto la prestación de un servicio al responsable.

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

¿Qué países son considerados con un nivel de protección adecuado?

Se consideran países que proporcionan un nivel de protección adecuado, los estados miembros de la Unión Europea, Islandia, Liechtenstein, Noruega o un Estado respecto del cual la Comisión de las Comunidades Europeas haya declarado que garantiza un nivel de protección adecuado, estando incluidos, hasta la fecha, entre estos últimos, Suiza, Argentina, las entidades estadounidenses adheridas a los "principios de 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.

¿Cuándo se debe solicitar la autorización del Director de la AEPD para realizar una transferencia internacional de datos?

Se debe obtener la autorización previa del Director de la AEPD cuando se tenga previsto realizar transferencias internacionales de datos a países que no proporcionan un nivel de protección adecuado y la transferencia no se ampare en alguno de los supuestos previstos en el art. 34 de la LOPD. Esta autorización sólo podrá ser otorgada si se obtienen garantías adecuadas, como los contratos basados en las cláusulas tipo aprobadas por la Comisión Europea, o las Reglas Corporativas Vinculantes intra grupos empresariales (en inglés Binding Corporate Rules).

¿CÓMO?

Mediante solicitud del exportador de datos que pretenda llevar a cabo la transferencia, consignando la finalidad, los colectivos de interesados, los datos objeto de transferencia y la documentación que incorpore las garantías exigibles para la obtención de la autorización, en la que conste una descripción de las medidas de seguridad concretas que van a ser adoptadas, tanto por el exportador como por el importador de los datos.

EXCEPCIONES A LA AUTORIZACION

No es preciso solicitar la autorización cuando la transferencia internacional de datos se encuentra amparada en alguna de las excepciones previstas en el art. 34 de la LOPD. Ej. Consentimiento del afectado a la transferencia, la transferencia es necesaria para establecer la relación contractual entre el afectado y el responsable del fichero, la transferencia se refiere a una transferencia dineraria, ...

No obstante

Se debe notificar a la AEPD
Se debe informar al interesado

De acuerdo con lo dispuesto en el artículo 44.4.e) de la Ley Orgánica 15/1999, 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, constituye una falta muy grave.

Transferencias internacionales en www.agpd.es -> Canal del responsable ->
Obligaciones -> Transferencias internacionales
Y en -> Jornadas de la Agencia -> Las Transferencias Internacionales

MEDIDAS DE SEGURIDAD

Se deben adoptar las medidas de índole técnica que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

El artículo 9 de la LOPD condiciona estas medidas al estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

- La aplicación de las medidas de seguridad se ordena a garantizar la confidencialidad, integridad, y disponibilidad de los datos. La seguridad constituye un instrumento esencial para garantizar el derecho fundamental a la protección de datos.
- Las medidas de seguridad se aplican tanto a los ficheros como a los tratamientos.
- Las medidas de seguridad deben aplicarse tanto por el responsable del fichero, como por el encargado del tratamiento.
- Deben aplicarse medidas de seguridad a ficheros y tratamientos en soportes no automatizados.

De conformidad con lo dispuesto en el artículo 44.3.h) de la Ley Orgánica 15/1999, constituye infracción grave, '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.'

NIVELES DE SEGURIDAD

El reglamento de desarrollo de la LOPD fija tres niveles de seguridad atendiendo a la naturaleza de la información.

Los niveles de seguridad son acumulativos de modo que un fichero de nivel alto deberá aplicar también las medidas previstas en los niveles básico y medio.

NIVEL ALTO: Ficheros o tratamientos

que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

Que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.

Que contengan datos derivados de actos de violencia de género.

NIVEL MEDIO: Ficheros o tratamientos

relativos a la comisión de infracciones administrativas o penales.

Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre.

Aquellos de los que sean responsables las Administraciones Tributarias y se relacionen con el ejercicio de sus potestades tributarias.

Aquellos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.

Aquellos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias, y aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

Aquellos de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los de localización. Estos ficheros aplicarán además lo previsto en el artículo 103 RDLOPD respecto del registro de accesos.

Aquellos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

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

En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual será suficiente la implantación de las medidas de seguridad de nivel básico cuando:

Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.

Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesorio se contengan aquellos datos sin guardar relación con su finalidad.

Se trate de ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

En la web de la Agencia se puede encontrar un cuadro resumen completo de las medidas reglamentarias y una guía al documento de seguridad.

Cuadro resumen medidas de seguridad y Guía al documento de seguridad en:
www.agpd.es -> Canal del responsable -> Guía documento de seguridad

DIVULGAR Y CONTROLAR

Definir las funciones y obligaciones de las personas con acceso a los datos de carácter personal y a los sistemas de información

Asegurarse de que todos conozcan las normas de seguridad que les afectan y las consecuencias de incumplirlas

El RDLOPD en sus artículos 8 y 9 hace alusión a la necesidad de que el responsable del fichero se implique en la definición, difusión y control de las normas de seguridad entre el personal encargado de llevarlas a cabo o simplemente de respetarlas.

DEBER DE GUARDAR SECRETO

Obligación de guardar secreto profesional sobre los datos de carácter personal a los que se tenga acceso

Para todos los que intervengan en cualquier fase del tratamiento

El **artículo 10** de la Ley Orgánica 15/1999, exige a quienes intervengan en cualquier fase del tratamiento de los datos a guardar secreto profesional sobre los datos, subsistiendo la obligación aún después de finalizar su relación con el responsable del fichero.

El incumplimiento del deber de secreto puede ser constitutivo de una infracción leve, en los términos del artículo 44.2.e), o de infracción grave de acuerdo con lo previsto en el artículo 44.3.g) en virtud del cual, '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.'

La vulneración del deber de guardar secreto sobre los datos de carácter personal especialmente protegidos a que hacen referencia los apartados 2 y 3 del artículo 7, así como de aquellos que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas, puede ser constitutivo de una infracción muy grave en los términos del artículo 44.4.g) de la Ley Orgánica 15/1999.

SANCIONES

¡Incumplir la Ley se sanciona!

De 601,01 a 60.101,21 euros
para infracciones leves

De 60.101,21 a 300.506,05 euros
para infracciones graves

De 300.506,05 a 601.012,10 euros
para infracciones muy graves

El artículo 45 de la LOPD establece las sanciones. Sobre las mismas, especifica que la cuantía se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora. Existe un régimen específico en el caso de los ficheros de titularidad pública.

En ningún caso podrá imponerse una sanción más grave que la fijada en la Ley para la clase de infracción en la que se integre la que se pretenda sancionar.

DEBER DE COLABORAR CON LA AGENCIA

Ejerce la potestad sancionadora y la potestad inspectora

Puede requerir la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de la LOPD.

Puede ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajusten a las disposiciones de la LOPD.

Puede requerir cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

Puede 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.

De acuerdo con lo dispuesto en el artículo 44.2.b) de la Ley Orgánica 15/1999 constituye infracción leve, '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.' Por otro lado, el artículo 44.3.i) y j) de la misma Ley Orgánica establece, serán infracciones graves, "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, así como practicar la obstrucción al ejercicio de la función inspectora."



NOTTIFICACIONES
ELEMATICAS A
LA **A**EPD

COMO NOTIFICAR

MEDIANTE EL SISTEMA NOTA:

Utilizando el formulario electrónico PDF:

Los formularios se componen del impreso de solicitud de inscripción y del contenido de la notificación del fichero.

NOTA permite el uso de notificaciones tipo precumplimentadas o de notificaciones generales para presentarlas en la AEPD:

Ejemplo de notificaciones tipo:

Ficheros de Comunidad de Propietarios, Nóminas - Recursos Humanos, Clientes y/o proveedores, Gestión escolar, Pacientes o Libro Recetario de oficinas de farmacia para ficheros de titularidad privada.

Agenda, Nóminas, Alumnos, Padrón, Registro, Control de acceso, Profesores, Gestión económica, Historia clínica y Recursos Humanos en el caso de ficheros de titularidad pública.

Formas de presentación:

De forma telemática, a través de Internet, permite la utilización de firma electrónica.

Mediante formato papel, que incluye un código óptico de lectura para agilizar su inscripción.

Mediante interfaz XML:

Para aquellos responsables o desarrolladores que quieran realizar las inscripciones con sus propias aplicaciones informáticas, a través de Internet con y sin certificado de firma reconocido.

¿Dónde presentar la hoja de solicitud de inscripción?:

La presentación de solicitudes en el Registro Electrónico de la AEPD podrá realizarse durante las 24 horas de todos los días del año.

En caso de no presentar la hoja de solicitud en el Registro Electrónico, ésta podrá ser enviada a la dirección de la AEPD c/ Jorge Juan, 6 28001- Madrid. También es posible su entrega en los Registros y oficinas a los que se refiere el artículo 38.4 de la Ley 30/1992.

Los formularios pueden obtenerse de forma gratuita en la página Web de la AEPD: www.agpd.es

Sistema NOTA:
en www.agpd.es -> Inscripción de ficheros -> NOTA

PASOS PARA LA CUMPLIMENTACIÓN DEL FORMULARIO

Descargar de la web www.agpd.es

Responder a las preguntas iniciales del asistente dependiendo del tipo de solicitud y forma de presentación elegido.

Cumplimentar los apartados de la notificación.

Cumplimentar la Hoja de solicitud.

Generar/Enviar la notificación:

En el caso de presentación a través de Internet con certificado de firma electrónica, deberá antes Finalizar y Firmar la notificación con su certificado de firma electrónica reconocido.

Recibir el acuse de recibo de la AEPD del envío realizado.

La no recepción del mensaje de confirmación, o en su caso, la recepción de un mensaje de indicación de error implica que no se ha producido la recepción del mismo, debiendo realizarse la presentación en otro momento o utilizando otros medios.

Enviar la Hoja de solicitud firmada a la AEPD. En el caso de presentación a través de Internet con certificado de firma electrónica no será necesario remitir la Hoja de solicitud.

¿Cuándo se inscribe el fichero en el RGPD?

El RGPD inscribe el fichero si la notificación se ajusta a los requisitos exigibles. En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.

Una vez inscrito el fichero en el RGPD, la AEPD notificará la resolución de inscripción del Director de la Agencia Española de Protección de Datos en la que se comunicará el código de inscripción asignado, a la dirección que a esos efectos se ha hecho constar en el apartado correspondiente de la Hoja de solicitud.

Igualmente, cuando los interesados así lo manifiesten expresamente en el formulario de notificación, podrán recibir por medios telemáticos la notificación de la resolución de inscripción de ficheros en el RGPD, para lo que deberán disponer de una dirección electrónica a efectos de notificaciones del Servicio de Notificaciones Telemáticas Seguras. La suscripción a este servicio es voluntaria y tiene carácter gratuito (www.notificaciones.administracion.es).

Otros servicios disponibles para el responsable de ficheros

En el Canal del responsable de la página web de la Agencia, se puede consultar el contenido completo de la inscripción mediante certificado de firma electrónica de la persona que ha presentado en su día la notificación. En caso de no disponer de un certificado de firma, puede realizar la consulta identificándose mediante el DNI y el código de inscripción.

Además, se podrá realizar el seguimiento del estado de tramitación de las notificaciones remitidas a la AEPD a través de Internet mediante el sistema NOTA.

La inscripción de un fichero en el RGPD, únicamente acredita que se ha cumplido con la obligación de notificación dispuesta en la Ley Orgánica 15/1999, sin que de esta inscripción se pueda desprender el cumplimiento por parte del responsable del fichero del resto de las obligaciones previstas en la Ley y demás disposiciones reglamentarias.

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE **DATOS**





www.agpd.es