AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Guía

DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

©AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS: 2004
D.L: M-23625-2005
NIPO: 052-04-002-2

Diseño Gráfico: ÉN

Imprime: NILO Industria Gráfica, S.A.

El derecho fundamental a la protección de datos personales deriva directamente de la Constitución y atribuye a los ciudadanos un poder de disposición sobre sus datos, de modo que, en base a su consentimiento, puedan disponer de los mismos.

La Constitución Europea reconoce en dos ocasiones el derecho fundamental a la protección de datos.

Asimismo establece que todos los países miembros de la Unión Europea deberán contar con una autoridad independiente que garantice y tutele tal derecho.

La Ley Orgánica 15/1999 regula el derecho fundamental a la protección de datos y dispone que será la Agencia Española de Protección de Datos la encargada de tutelar y garantizar el derecho.

En el empeño de facilitar un mejor respeto a la protección de datos y divulgar todo lo posible su conocimiento en el marco de una sociedad abierta y democrática, se ha elaborado esta Guía que tengo el gusto de presentar y que, con un lenguaje sencillo y directo, pretende dar un paso más en la necesaria normalización de la cultura de la protección de datos entre los ciudadanos y los responsables de los tratamientos y bases de datos.

Guía

José Luis Piñar Mañas
Director de la Agencia Española de Protección de Datos

Índice

5 CUIDA TUS DATOS PERSONALES

6 ¿QUÉ ES EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS?

7 LEGISLACIÓN SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

9 LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS PROTEGE TUS DERECHOS

11 ¿CUÁNDO PUEDEN TRATARSE DATOS PERSONALES?

12 PRINCIPIOS DE PROTECCIÓN DE DATOS

14 DATOS SENSIBLES

15 ESTOS SON TUS DERECHOS: HAZLOS VALER

17 DERECHO DE INFORMACIÓN EN LA RECOGIDA DE DATOS
- ¿TUS DATOS PERSONALES VAN A SER INCLUIDOS EN UN FICHERO?
- ¿QUÉ TRATAMIENTOS VAN A REALIZARSE CON TUS DATOS?
- SÉ CONSCIENTE DE QUE ESTÁS FACILITANDO TUS DATOS PERSONALES

18 DERECHO DE CONSULTA AL REGISTRO GENERAL DE PROTECCIÓN DE DATOS
- ¿QUIÉN ESTÁ TRATANDO TUS DATOS PERSONALES?
- DERECHO DE ACCESO
- DERECHO DE RECTIFICACIÓN
- DERECHO DE CANCELACIÓN
- DERECHO DE OPOSICIÓN

¿QUÉ PUEDES HACER EN CASO DE VIOLACIÓN DE TUS DERECHOS? 25

TUTELA DE DERECHOS 26
PROCEDIMIENTO SANCIONADOR 27

CÓDIGOS TIPO 28

ALGUNOS CASOS SIGNIFICATIVOS DE FICHEROS DE DATOS PERSONALES 29

FICHEROS DE INFORMACIÓN SOBRE SOLVENCIA PATRIMONIAL Y CRÉDITO Y SOBRE CUMPLIMIENTO O INCUMPLIMIENTO DE OBLIGACIONES DINERARIAS: FICHEROS DE MOROSOS 29
FICHEROS DE INFORMACIÓN SOBRE SOLVENCIA PATRIMONIAL Y CRÉDITO
FICHEROS SOBRE CUMPLIMIENTO O INCUMPLIMIENTO DE OBLIGACIONES DINERARIAS:FICHEROS DE MOROSOS
CARACTERÍSTICAS ESPECIALES DE ESTOS FICHEROS

FICHEROS DE MARKETING Y PUBLICIDAD 34

Guía

Los datos personales permiten identificar a una persona.

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, el número de matrícula del coche, la huella digital, el ADN, una fotografía, el número de seguridad social, ... son datos que identifican a una persona, ya sea directa o indirectamente.

Es habitual que prácticamente para cualquier actividad sea necesario que los datos personales se recojan y utilicen en la vida cotidiana.

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 ..... Son múltiples los rastros de datos que se dejan a menudo en todas estas gestiones.

Los mecanismos de recogida y tratamientos de los datos personales se encuentran en constante evolución.

Ello supone que el desarrollo y la aplicación de las nuevas tecnologías ha introducido comodidad y rapidez en el intercambio de datos, lo que ha contribuido también al incremento del número de tratamientos de datos que se realizan cotidianamente. La bondad que aportan estas técnicas es indudable respecto del progreso de las sociedades modernas y de la calidad de vida de los ciudadanos, pero se hace necesario garantizar el equilibrio entre modernización y garantía de los derechos de los ciudadanos.

> Esta ponderación entre derecho del ciudadano a preservar el control sobre sus datos personales y la aplicación de las nuevas tecnologías de la Información, es el contexto en el que el Legislador consagra el derecho fundamental a la protección de datos de carácter personal.

¿QUÉ ES EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS?

> El derecho fundamental a la protección de datos reconoce al ciudadano la **facultad de controlar** sus datos personales y la **capacidad para disponer y decidir** sobre los mismos.

LEGISLACIÓN SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

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, fue aprobada la **Ley Orgánica 15/1999,** de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

Tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

La LOPD garantiza al ordenamiento jurídico español la **Directiva 95/46/CE (Directiva sobre protección de datos**).

La LOPD garantiza una serie de derechos a las personas físicas, titulares de los datos, tales como el derecho a ser informado de cuándo y porqué se tratan sus datos personales, el derecho a acceder a los datos y, en caso necesario, el derecho a la modificación o supresión de los datos o el derecho a la oposición al tratamiento de los mismos.

El derecho a la protección de datos es un derecho en constante **evolución** que se ha visto reconocido en el **Tratado Europeo por el que se establece una Constitución para Europa.**

La Constitución Europea ha recogido expresamente el derecho fundamental a la protección de datos en dos ocasiones, en la Parte I, Título VI (De la vida democrática de la Unión), el artículo I-51 (Protección de datos de carácter personal) establece en el epígrafe primero que "toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan" y en la Parte II (Carta de los Derechos Fundamentales de la Unión), Título II (Libertades), se introduce en el artículo II-68 la segunda referencia al derecho a la protección de datos, señalando de nuevo que "toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan", y añadiendo que "estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley", y que "toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación".

Asimismo, en ambos preceptos se establece que una autoridad independiente se encargará de la garantía del derecho fundamental a la protección de datos personales.

La Constitución Europea exige que en todos los Estados miembros exista una autoridad independiente que controle y garantice el Derecho Fundamental a la protección de datos.

La Agencia Española de Protección de Datos (en lo sucesivo AEPD) es el ente de derecho público que vela por el cumplimiento de la normativa sobre protección de datos personales, actuando para ello con plena independencia de las Administraciones Públicas.

En este sentido:

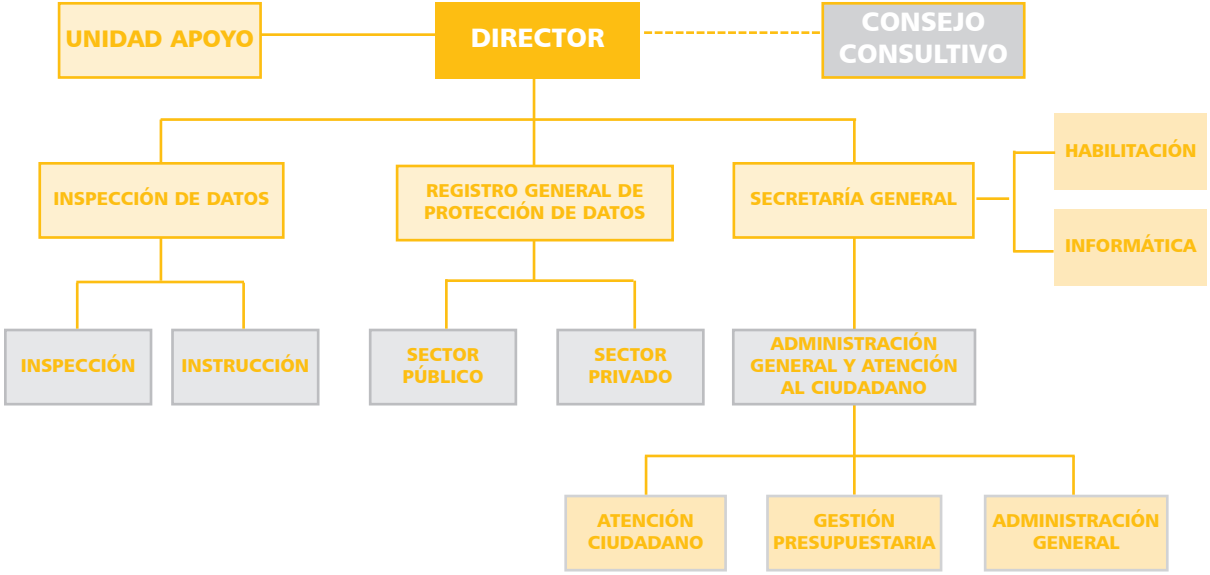
INFORMA sobre el contenido, los principios y las garantías del derecho fundamental a la protección de datos regulado en la LOPD.

AYUDA al ciudadano a ejercitar sus derechos y a los responsables y encargados de tratamientos a cumplir las obligaciones que establece la LOPD.

TUTELA al ciudadano en el ejercicio de los derechos de acceso, rectificación, cancelación y oposición cuando no han sido adecuadamente atendidos por los responsables de los ficheros.

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. Impone, en su caso, la correspondiente sanción.

La estructura orgánica de la AEPD es la siguiente:


UNIDAD APOYO
DIRECTOR
CONSEJO CONSULTIVO
INSPECCIÓN DE DATOS
REGISTRO GENERAL DE PROTECCIÓN DE DATOS
SECRETARÍA GENERAL
HABILITACIÓN
INFORMÁTICA
INSPECCIÓN
INSTRUCCIÓN
SECTOR PÚBLICO
SECTOR PRIVADO
ADMINISTRACIÓN GENERAL Y ATENCIÓN AL CIUDADANO
ATENCIÓN CIUDADANO
GESTIÓN PRESUPUESTARIA
ADMINISTRACIÓN GENERAL

¿CUÁNDO PUEDEN TRATARSE DATOS PERSONALES?

Los datos personales de un ciudadano sólo pueden tratarse, es decir, recogerse y emplearse, si:

El interesado ha dado su consentimiento.

El tratamiento es necesario para el mantenimiento o cumplimiento de un contrato o precontrato de una relación negocial, laboral o administrativa.

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.

El tratamiento es necesario para cumplir las funciones de las Administraciones Públicas en el ámbito de sus competencias.

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 quienes se comuniquen los datos.

Cuando una ley habilite el tratamiento sin requerir el consentimiento inequívoco de su titular.

PRINCIPIOS DE PROTECCIÓN DE DATOS

El tratamiento de datos de carácter personal ha de realizarse de acuerdo con los principios de información, calidad, finalidad, consentimiento y seguridad. Dichos principios se plasman en diversos preceptos de la LOPD.

Todo responsable de un fichero o tratamiento de datos personales está obligado a cumplir los citados principios recogidos en la LOPD.

> El responsable de un fichero o tratamiento es la entidad, la 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 de sus clientes, de sus proveedores, de sus empleados; un médico será responsable del tratamiento de los datos personales que conforman las historias clínicas de sus pacientes; 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; ...

Los principios de la LOPD pretenden proteger los datos personales de los interesados:

Los datos deben tratarse de manera leal y lícita.

Los datos deben recogerse con fines determinados, explícitos y legítimos. Los datos deben ser adecuados, pertinentes y no excesivos en relación con el ámbito y los fines para los que se han recogido.

Los datos deben ser exactos y mantenerse actualizados de manera que respondan con veracidad a la situación actual de su titular.

Los responsables deben atender a los interesados que soliciten el acceso a sus datos personales.

Los datos personales sólo deben conservarse durante el tiempo necesario para las finalidades del tratamiento para el que han sido recogidos. Deben ser cancelados cuando hayan dejado de ser necesarios o pertinentes para el fin con que se obtuvieron.

Todo responsable o encargado de un tratamiento tiene que adoptar todas las medidas necesarias para garantizar la seguridad de los datos personales e impedir cualquier alteración, pérdida, tratamiento o acceso no autorizado.

El responsable tiene que notificar al Registro General de Protección de Datos la creación, modificación o supresión de cualquier fichero o tratamiento de datos personales.

14 DATOS SENSIBLES

Se consideran datos sensibles aquellos datos referidos a ideología, creencias, religión, afiliación sindical, salud, origen racial o vida sexual de las personas.

Como norma general los datos de ideología, creencias, religión o afiliación sindical no pueden ser tratados ni almacenados en ficheros. Sólo pueden ser objeto de tratamiento con el consentimiento expreso y por escrito del afectado.

Los datos relativos al origen racial, a la salud y a la vida sexual sólo podrán ser recogidos, tratados y cedidos, si alguna Ley así lo dispone por razones de interés general, o en caso de que el afectado haya consentido expresamente.

Los datos sensibles pueden ser objeto de tratamiento, si resulta necesario para la prevención o para el diagnóstico médicos, para la prestación de asistencia sanitaria o de un tratamiento médicos o para la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario.

También pueden ser tratados estos datos 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 prestar su consentimiento.

Los profesionales sanitarios correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que acuden a los centros sanitarios públicos o privados, de acuerdo con la legislación sanitaria, y guardando el deber de secreto, obligación que subsistirá aún después de finalizar su relación asistencial.

Toda persona tiene derecho a saber porqué y cómo son tratados sus datos personales y decidir acerca del tratamiento

El derecho a la protección de datos puede considerarse una condición preventiva para la garantía de otras libertades y derechos fundamentales.

La LOPD reconoce específicamente a los ciudadanos los siguientes derechos en materia de protección de datos:

DERECHO DE **INFORMACIÓN EN LA RECOGIDA DE DATOS**

DERECHO DE **CONSULTA AL REGISTRO GENERAL DE PROTECCIÓN DE DATOS**

DERECHO DE ACCESO

DERECHO DE **RECTIFICACIÓN**

DERECHO DE CANCELACIÓN

DERECHO DE **OPOSICIÓN**

ESTOS SON TUS DERECHOS

El ciudadano tiene **derecho a ser informado**, en el momento que facilita sus datos personales.

El **derecho de consulta** permite al ciudadano, dirigiéndose al Registro General de Protección de Datos de la AEPD, conocer de la existencia de un fichero o tratamiento de datos.

El ciudadano puede ejercitar los **derechos de acceso, rectificación, cancelación y oposición** ante el responsable de un fichero o de un tratamiento con el fin de conocer sus datos personales, para solicitar que sean modificados o cancelados, o bien para oponerse a su tratamiento

> Tales derechos pueden ejercerse respecto de cualquier fichero o tratamiento de datos personales, ya sean automatizados o no automatizados

Los derechos de acceso, rectificación, cancelación y oposición tienen carácter personalísimo, es decir, sólo pueden ejercerse por el titular de los mismos o por su representante legal. No obstante, podrá encomendarse su ejercicio a un representante, siempre que el mismo pueda acreditar suficientemente tal condición.

> Todos estos derechos tienen **carácter gratuito**

Estos derechos deben ser respetados por los responsables de los tratamientos de datos personales.

> Si un ciudadano ejercita estos derechos y no recibe, a su juicio, la contestación adecuada puede dirigirse a la Agencia Española de Protección de Datos para solicitar la tutela de estos derechos, para lo cual se instruirá el correspondiente procedimiento.

En la página web de la Agencia **www.agpd.es** se encuentran disponibles los modelos de solicitudes para ejercitar estos derechos, así como para interponer en su caso las relamaciones oportunas ante la propia Agencia.

DERECHO DE INFORMACIÓN EN LA RECOGIDA DE DATOS.
¿Tus datos personales van a ser incluidos en un fichero?
¿Qué tratamientos van a realizarse con tus datos personales?
SÉ CONSCIENTE DE QUE ESTÁS FACILITANDO TUS DATOS PERSONALES.

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.

El ciudadano debe ser informado de la recogida de sus datos y de su utilización. Este derecho de información es esencial porque condiciona el ejercicio de otros derechos tales como el derecho 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, así como de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

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.

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

Esta obligación general del responsable debe ser facilitada con carácter general, salvo que la información se deduzca inequívocamente de la naturaleza de los propios datos personales y de las circunstancias en las que se produce la recogida.

En la medida de lo posible esta información debe estar incluida en los cuestionarios o impresos de recogida de los datos.

> 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.

Si está previsto que los datos sean transmitidos a otras personas, la información debe realizarse a lo más tardar en el momento en que se produzca la primera comunicación de los datos.

DERECHO DE CONSULTA AL REGISTRO GENERAL DE PROTECCIÓN DE DATOS. ¿Quién está tratando tus datos personales?

El art. 14 de la LOPD, permite a cualquier ciudadano dirigirse al Registro General de Protección de Datos (en lo sucesivo RGPD) con el fin de obtener información sobre la existencia de tratamientos de datos de carácter personal, de sus finalidades y de la identidad del responsable del mismo. La consulta al RGPD es pública y gratuita, y su objeto es hacer posible a todo ciudadano el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

> La AEPD no dispone de los datos personales de los ciudadanos incluidos en los ficheros declarados, pero sí puede, previa solicitud de la persona afectada o bien de su representante, facilitar la dirección de la oficina o dependencia del responsable del fichero o tratamiento ante la que se pueden ejercer los derechos de acceso, rectificación, cancelación u oposición, siendo el citado responsable quien debe atender la petición efectuada por la persona titular de los datos.

La consulta al RGPD puede realizarse por escrito o a través de la página web de la Agencia **www.agpd.es**, en la que mensualmente se actualiza la información sobre los ficheros y tratamientos inscritos.

DERECHO DE ACCESO

Toda persona tiene derecho a dirigirse al responsable o encargado de un fichero o tratamiento para conocer la totalidad de los datos personales que le afecten y así mismo, recibir una copia inteligible de los mismos, y cualquier información sobre su origen.

Ejerciendo el derecho de acceso, la persona puede informase de las finalidades del tratamiento, del tipo de datos registrados, de su origen, de los destinatarios de los datos y de las posibles transferencias de datos a otros países.

> El ejercicio del derecho de acceso permite controlar la exactitud de los datos, y en caso de ser necesario, hacerlos rectificar o cancelar.

En virtud del derecho de acceso, regulado en el art. 15 de la LOPD, el ciudadano puede solicitar y obtener gratuitamente información sobre sus datos de carácter personal sometidos a tratamiento, así como la información disponible sobre el origen de dichos datos y de las comunicaciones realizadas o que se prevean realizar.

> Esta información puede obtenerse bien mediante la mera consulta de los datos por medio de su visualización en pantalla, o bien a través de escrito, copia, telecopia o fotocopia, certificada o no, realizada en forma inteligible, sin utilizar claves o códigos que requieran para su comprensión el uso de dispositivos mecánicos específicos.

El derecho de acceso respecto de los tratamiento realizados por una determinada entidad, persona u órgano administrativo, sólo podrá ejercitarse a intervalos no inferiores a doce meses, salvo que el ciudadano acredite un interés legítimo que posibilite su ejercicio con anterioridad al cumplimiento de dicho período.

Para ejercer este derecho el ciudadano tiene que dirigirse al responsable del fichero o tratamiento, aportando fotocopia del DNI o documento que acredite la identidad y sea admitido en Derecho, o en caso de representación, documento acreditativo de la misma, e indicando el domicilio a efectos de notificaciones, la fecha y firma del solicitante. Los ciudadanos deben utilizar cualquier medio que permita acreditar el envío y la recepción de la solicitud.

> El responsable del fichero o tratamiento tiene que resolver la solicitud de acceso en el plazo máximo de un mes a contar desde la fecha en que haya recibido la solicitud. En caso de estimar la solicitud, el acceso debe hacerse efectivo en el plazo de los diez días siguientes a la notificación.

La obligación de contestar a dicha solicitud ha de producirse con independencia de que figuren o no datos personales del ciudadano en sus ficheros. La contestación al derecho de acceso ha de practicarse utilizando cualquier medio que permita acreditar el envío y la recepción de la misma.

Puede denegarse el derecho de acceso si:

> puede suponer un peligro 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.
>
> o en el caso de ficheros de la Hacienda Pública, si este derecho obstaculiza 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.

DERECHO DE RECTIFICACIÓN

El artículo 16 de la LOPD, reconoce al ciudadano el derecho a dirigirse al responsable de un fichero o tratamiento para que rectifique sus datos personales.

> Si un ciudadano contrasta que sus datos personales son inexactos tiene derecho a solicitar su rectificación ante el responsable.

La solicitud de rectificación debe indicar el dato que se estima erróneo y la corrección que debe realizarse y debe ir acompañada de la documentación justificativa de la rectificación solicitada.

> Este derecho puede ejercitarse cuando el tratamiento contenga datos inexactos o incompletos.

El responsable del fichero o tratamiento tiene el deber de atender el derecho de rectificación **en el plazo de diez días naturales**.

Deberá contestar de forma motivada a la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado en sus ficheros, debiendo utilizar cualquier medio que permita acreditar el envío y la recepción de su respuesta.

> Si los datos rectificados hubieran sido cedidos previamente a un tercero, el responsable del fichero tiene la obligación de notificar al cesionario la rectificación practicada.

DERECHO DE CANCELACIÓN

Este derecho, regulado en el art. 16 de la LOPD, ofrece al ciudadano la posibilidad de dirigirse al responsable para solicitar la cancelación de sus datos personales.

> Si un ciudadano verifica que sus datos personales son inexactos o se han tratado ilegalmente, tiene derecho a solicitar su supresión.

Este derecho puede ejercerse cuando el tratamiento no se ajuste a lo dispuesto en la LOPD y, en particular, cuando los datos resulten inexactos o incompletos.

En la solicitud de cancelación, el interesado debe indicar la existencia del dato erróneo o inexacto, en cuyo caso deberá acompañar la documentación justificativa.

> La cancelación dará lugar al bloqueo de los datos cuando sea preciso conservar éstos únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, de cara a posibles responsabilidades.

El bloqueo tendrá una duración equivalente al plazo de prescripción de dichas responsabilidades, debiéndose proceder a la total supresión de los datos una vez cumplido el mismo.

El responsable del fichero o tratamiento tiene la obligación de hacer efectivo el derecho de cancelación en el plazo de diez días naturales.

Deberá contestar de forma motivada a la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado en sus ficheros, debiendo utilizar cualquier medio que permita acreditar el envío y la recepción de su respuesta.

> Si los datos cancelados hubieran sido cedidos previamente a un tercero, el responsable del fichero deberá notificar al cesionario la cancelación efectuada.

El responsable del fichero o tratamiento podrá denegar la cancelación, tanto en el caso de ficheros privados como públicos, cuando exista un deber legal de conservación de los datos, durante el plazo establecido en cada caso por la legislación aplicable. Asimismo, podrá denegar la cancelación cuando la conservación del dato sea necesaria para el cumplimiento de las obligaciones contractuales que le vinculen con el interesado y justifiquen el tratamiento de los datos y, en todo caso, cuando su cancelación pudiese causar perjuicio al propio ciudadano titular de los mismos o a terceros.

DERECHO DE OPOSICIÓN

Toda persona tiene la posibilidad de oponerse, por un motivo legitimo y fundado, referido a una situación personal concreta, a figurar en un fichero o al tratamiento de sus datos personales, siempre que una ley no disponga lo contrario. En principio, el ciudadano tiene la facultad de disponer y decidir sobre los usos de los datos personales que le conciernen, y por lo tanto, puede oponerse a aparecer en un determinado fichero o a que sus datos sean comunicados a terceros.

> El ciudadano puede oponerse mediante su simple solicitud, a que sus datos sean tratados con fines de publicidad y de prospección comercial

Este derecho de oposición se encuentra regulado en los arts. 6.4, 17 y 30.4 de la LOPD. Se ejercita mediante una solicitud por escrito dirigida al responsable del fichero o tratamiento, en la que se hagan constar los motivos fundados y legítimos relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho.

El responsable del fichero o tratamiento tiene un plazo máximo de un mes a contar desde la recepción de la petición, para resolver la solicitud de oposición. Si transcurrido este plazo no se ha recibido de forma expresa una respuesta a la petición de acceso, ésta puede entenderse desestimada a los efectos de presentar una reclamación de tutela de derechos ante la AEPD.

> En el caso de que sea procedente acceder a la oposición, el responsable del fichero ha de excluir del tratamiento los datos del ciudadano solicitante.

En relación a los tratamientos de datos con fines de publicidad y de prospección comercial, los ciudadanos pueden ejercer el derecho de oposición y, a su simple solicitud, el responsable ha de dar de baja sus datos personales en el tratamiento, cancelando de este modo las informaciones que figuraban en el mismo.

> El derecho de oposición puede ejercitarse:
>
> cuando no es obligatoria la recogida de los datos
>
> renunciando a otorgar el consentimiento para el tratamiento de datos especialmente protegidos de ideología, religión o creencias
>
> solicitando la eliminación de datos contenidos en ficheros comerciales
>
> señalando, en su caso, con una x la casilla destinada a indicar que no está de acuerdo con la cesión o comercialización de sus datos

Puede ejercerse en el momento de la recogida de la información o posteriormente, dirigiéndose al responsable del fichero.

> El derecho de oposición no puede ejercerse ante muchos ficheros de titularidad pública, como por ejemplo, los de Hacienda Pública, los ficheros policiales, Seguridad Social, ...

¿QUÉ PUEDES HACER EN CASO DE VIOLACIÓN DE TUS DERECHOS?

En caso de sospechar que han sido violados tus derechos en materia de protección de datos, en primer lugar debes intentar determinar la identidad del responsable del tratamiento. Para ello puedes ejercer tu derecho de consulta al Registro General de Protección de Datos, así como los derechos de acceso, rectificación, cancelación y/u oposición, según sea el caso.

Si no obtienes un resultado satisfactorio con este procedimiento puedes acudir a la Agencia Española de Protección de Datos.

> Las actuaciones contrarias al derecho fundamental a la protección de datos de carácter personal pueden ser denunciadas por los ciudadanos ante la AEPD y, en su caso, posteriormente ante la jurisdicción contencioso-administrativa.

Además, si de dichas actuaciones se derivase un perjuicio para los interesados, los mismos podrán reclamar la correspondiente indemnización, bien ante la jurisdicción civil, bien ante el Órgano administrativo responsable, a través, en este caso, del procedimiento establecido al efecto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

> Al ponerte en contacto con la AEPD deberás describir el problema con los suficientes pormenores, para ello puedes utilizar los formularios disponibles en la página web de la AEPD www.agpd.es.

TUTELA DE DERECHOS

El derecho a la tutela de derechos de los ciudadanos por parte de la AEPD está reconocido en el art. 18 de la LOPD.

> El procedimiento de tutela tiene por finalidad garantizar el ejercicio efectivo por parte del ciudadano de los derechos de acceso, rectificación, cancelación y oposición.

El ciudadano al que le haya sido denegado el ejercicio de los derechos de acceso, rectificación, cancelación y oposición puede ponerlo en conocimiento de la AEPD, para que ésta constate la procedencia o improcedencia de la denegación.

Para solicitar la tutela de derechos, el ciudadano tiene que presentar en la AEPD un escrito, en el que se expresen con claridad sus datos, el contenido de la reclamación y los preceptos de la LOPD que considere vulnerados.

La Agencia, a continuación, da traslado de la reclamación al responsable del fichero o tratamiento instándole para que, en el plazo de quince días, formule las alegaciones que estime pertinentes.

> La AEPD tramitará el correspondiente procedimiento administrativo y resolverá el mismo en el plazo máximo de seis meses, dando traslado de su resolución a las partes.

Los procedimientos de tutela de derechos no tienen carácter sancionador, limitándose a estimar o desestimar las reclamaciones planteadas por los ciudadanos ante la Agencia. Sin embargo, en algunas ocasiones, los hechos constatados en los citados procedimientos pueden dar lugar a la iniciación de procedimientos sancionadores.

> Las resoluciones del Director de la Agencia Española de Protección de Datos son firmes en vía administrativa por lo que contra las mismas sólo se podrá interponer recurso potestativo de reposición, o bien recurso contencioso-administrativo ante la Audiencia Nacional.

PROCEDIMIENTO SANCIONADOR

Los arts. 43 a 49 de la LOPD regulan el procedimiento sancionador que podrá tramitar la AEPD. Este procedimiento se inicia contra los responsables de ficheros cuando existan pruebas razonables de que se ha producido alguna infracción de los principios y garantías contenidos en la LOPD.

El procedimiento sancionador se inicia siempre de oficio mediante acuerdo del Director de la Agencia cuando existan pruebas razonables de que se ha producido alguna infracción de los principios y garantías contenidos en la LOPD.

El régimen sancionador establecido en los arts. 43 y siguientes de la LOPD, articula las infracciones en tres tipos: leves, graves y muy graves.

Normalmente el acuerdo de iniciación se origina como consecuencia de una denuncia realizada por un ciudadano o de un tercero. En otras ocasiones se debe al conocimiento por parte de la AEPD de un hecho presuntamente ilícito, por ejemplo, a través de alguna noticia aparecida en los medios de comunicación social.

> La AEPD investiga la denuncia y puede suspender temporalmente el tratamiento. En caso de concluir que se ha violado la LOPD la Agencia puede ordenar la supresión o destrucción de los datos o prohibir el tratamiento.

CÓDIGOS TIPO

Los responsables de ficheros o tratamientos de datos de carácter personal están obligados a cumplir los principios y las garantías que establece la LOPD. El cumplimiento de estas obligaciones muchas veces redunda en un aumento de calidad en la prestación de sus servicios y ello, en una mejor consideración por parte de las personas con las que mantiene una relación contractual, negocial, laboral, ...

> Un código tipo es un documento de buenas prácticas en la aplicación de los principios y garantías de protección de datos de carácter personal que ha sido adoptado mediante un acuerdo sectorial, un convenio administrativo o una decisión de empresa, por una organización de responsables de ficheros o tratamientos de datos de titularidad pública o privada.

El art. 32 de la LOPD establece que los códigos tipo deberán ser inscritos en el Registro General de Protección de Datos de la AEPD.

El hecho de que un sector de actividad haya elaborado un código tipo y éste haya sido inscrito en el RGPD puede aportar una garantía adicional a la voluntad y el compromiso de la entidad que exhibe dicho Código de conducta, además de una transparencia en el desarrollo de sus tratamientos de datos.

El cumplimiento de la LOPD es obligatorio para todos los responsables de ficheros o tratamientos de datos de carácter personal.

> Un código tipo no garantiza de manera absoluta el cumplimiento de la normativa de protección de datos de carácter personal.

El art. 29 de la LOPD regula los ficheros o tratamientos de datos de carácter personal derivados de la prestación de servicios de información sobre solvencia patrimonial y crédito. A tal efecto, distingue entre los ficheros o tratamientos de prestación de información sobre la solvencia patrimonial y el crédito y los ficheros sobre cumplimiento o incumplimiento de obligaciones dinerarias (generalmente denominados "ficheros de morosos").

FICHEROS DE INFORMACIÓN SOBRE SOLVENCIA PATRIMONIAL Y CRÉDITO Y SOBRE CUMPLIMIENTO O INCUMPLIMIENTO DE OBLIGACIONES DINERARIAS: FICHEROS DE MOROSOS

FICHEROS DE INFORMACIÓN SOBRE SOLVENCIA PATRIMONIAL Y CRÉDITO

Estos ficheros aparecen regulados en el artículo 29.1 de la LOPD y su régimen es similar al de los restantes ficheros sometidos a la misma. No obstante, se establecen determinadas especialidades en cuanto a la recogida de los datos.

> Los responsables de este tipo de ficheros se encuentran habilitados por la LOPD para realizar tratamientos sobre datos de carácter personal obtenidos bien de los registros y fuentes accesibles al público establecidos al efecto, o bien de informaciones facilitadas por el interesado o con su consentimiento.

A tal fin el art. 3,j) de la LOPD indica que tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos en la normativa específica, las listas de personas pertenecientes a grupos profesionales (únicamente los datos relativos a nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia a grupo), los diarios y boletines oficiales y los medios de comunicación social. Además, en estos casos, será necesario que la consulta de estas fuentes pueda ser realizada por cualquier persona no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación.

En todo caso, este tipo de ficheros deberán observar las siguientes reglas en el momento de realizar la recogida de los datos:

No deberán incorporarse datos personales que supongan una información sesgada respecto de aquella que ha aparecido publicada.

Los datos han de referirse a una información exacta.

No deberán incorporar aquellas informaciones que por su naturaleza y circunstancias no permitan una identiicación completa del interesado

> Además, el ciudadano tiene derecho a solicitar al responsable del tratamiento que le comunique los datos, así como las evaluaciones y apreciaciones que se hayan comunicado durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado dichos datos.

FICHEROS SOBRE CUMPLIMIENTO O INCUMPLIMIENTO DE OBLIGACIONES DINERARIAS: FICHERO DE MOROSOS

> El artículo 29.2 de la LOPD permite tratar datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por los acreedores o por quien actúe por su cuenta o interés.

Este caso da lugar a los ficheros o tratamientos comunes de solvencia patrimonial y crédito, conocidos popularmente como "ficheros de morosos".

Como en el caso de los ficheros de información sobre la solvencia patrimonial y el crédito, el ciudadano tiene derecho a solicitar al responsable que le comunique los datos, así como las evaluaciones y apreciaciones que se hayan comunicado durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado dichos datos.

> La inclusión de los datos de carácter personal en los ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias, sólo podrá efectuarse cuando exista una deuda cierta, vencida y exigible, que haya resultado impagada, y después de que se haya requerido al ciudadano afectado el pago de la deuda por el acreedor.

No podrán ser incluidos en ficheros de esta naturaleza los datos personales de un ciudadano cuando exista un principio de prueba documental que contradiga la existencia de la propia deuda. Del mismo modo, tal circunstancia determinará la cancelación cautelar del dato personal desfavorable en los supuestos en que ya se hubiera efectuado la inclusión en el fichero.

Los responsables de estos ficheros sólo podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los ciudadanos y que no se refieran, cuando sean adversos, a más de seis años, y siempre que respondan con veracidad y exactitud a la situación actual de éstos.

> En el caso de que el ciudadano incluido en este tipo de fichero haya procedido al pago de la deuda deberá procederse a la cancelación del dato referido al mismo.

Para ello, el acreedor tendrá que comunicar al responsable del fichero común de información de solvencia patrimonial y crédito, en el plazo de una semana, la inexactitud o inexistencia de la deuda. Por lo tanto, si la deuda ya se ha pagado, el acreedor tiene la obligación de informar al responsable del fichero común para que proceda a la rectificación del dato del ciudadano que no responde a su situación actual.

CARACTERÍSTICAS DE ESTOS FICHEROS

COMUNICACIÓN DE INCLUSIÓN

> En todo caso, el responsable de un fichero o tratamiento común de morosidad tiene la obligación de notificar al ciudadano que ha procedido a incluirlo en el mismo haciendo referencia de los datos incluidos, así como al derecho que le asiste para recabar información de la totalidad de ellos en los términos establecidos en la LOPD.

Dicha notificación deberá efectuarse por el responsable en el plazo máximo de treinta días a contar desde el registro del dato, e informará al afectado de su derecho a recabar información sobre los datos recogidos en el mismo.

La inscripción en el fichero o tratamiento común de la obligación incumplida se efectuará, bien en un solo asiento, si fuese de vencimiento único, bien en tantos asientos como vencimientos periódicos incumplidos existan, señalando, en este caso, la fecha concreta de cada uno de ellos.

Se efectuará una notificación por cada deuda concreta y determinada, con independencia de que ésta se tenga con el mismo o con distintos acreedores.

El responsable del fichero común deberá adoptar las medidas organizativas y técnicas necesarias que permitan acreditar la realización material del envío de la comunicación y la fecha de entrega o intento de entrega de la notificación.

> La notificación se dirigirá a la última dirección conocida del afectado, a través de un medio fiable e independiente del responsable del fichero o tratamiento común.

DERECHO DE ACCESO

En relación con este derecho, los responsables de los ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito están obligados a satisfacer el derecho de acceso, cualquiera que sea el origen de los datos incluidos en los mismos.

> Además, cuando el ciudadano lo solicite, el responsable del fichero común deberá informar sobre las evaluaciones y apreciaciones que se hayan comunicado en los últimos seis meses, así como el nombre y dirección de la persona o entidad a quien se hayan revelado los datos.

Las personas o entidades a las que se presta el servicio solamente están obligadas, ante el ejercicio del derecho de acceso, rectificación y cancelación de un ciudadano, a comunicar los datos relativos al mismo a los que tengan acceso, y la identidad del responsable del fichero común para que pueda completar el ejercicio de sus derechos.

DERECHOS DE RECTIFICACIÓN Y CANCELACIÓN

> En los ficheros comunes de prestación de servicios de información sobre solvencia patrimonial y crédito, cuando el afectado lo solicite, el responsable del fichero deberá cumplir la obligación de atender los derechos de rectificación y cancelación.

En relación al ejercicio de estos derechos se pueden plantear los siguientes supuestos:

Si la solicitud del ejercicio de los derechos de rectificación o cancelación de datos se dirige al responsable del fichero común, éste trasladará dicha solicitud al acreedor que haya facilitado los datos relativos a la deuda, para que éste resuelva. En el caso de que el responsable del fichero común no haya recibido contestación por parte del acreedor en el plazo de diez días, procederá cautelarmente a la rectificación o cancelación de los mismos.

Si la solicitud del ejercicio de los derechos de rectificación o cancelación de datos se dirige a otra entidad participante en el sistema y hace referencia a datos que dicha entidad haya facilitado al fichero común, por ser la misma la acreedora del interesado, dicha entidad procederá a la rectificación o cancelación de los datos en sus ficheros y a notificarlo al responsable del fichero común en el plazo de diez días.

Si la solicitud hace referencia a datos que la entidad acreedora no hubiera facilitado al fichero común, dicha entidad informará al afectado sobre este hecho, proporcionándole, además, la identidad del responsable del fichero común para que pueda completar el ejercicio de sus derechos.

FICHEROS DE MARKETING Y PUBLICIDAD

> Las entidades que se dedican a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial ... pueden utilizar los nombres y direcciones, así como otros datos personales que figuren en fuentes accesibles al público.

Los repertorios telefónicos y las listas de personas pertenecientes a un Colegio profesional, que contengan los datos de nombre, título, profesión, actividad, grado académico, y la dirección son fuentes de acceso público. También lo son los diarios y boletines oficiales y los medios de comunicación.

Cuando una entidad toma datos personales de una fuente accesible al público para realizar un tratamiento de publicidad o marketing debe informar al interesado del origen de los datos y de la identidad del responsable del tratamiento, diarios y boletines oficiales y medios de comunicación.

Los interesados pueden ejercer el derecho de acceso para conocer sus datos personales y el origen de los mismos.

Toda persona tiene derecho a oponerse al tratamiento de sus datos personales con esta finalidad.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

La información de esta guía puede ser ampliada en

www.agpd.es

Servicio de Atención al Ciudadano

Sagasta nº 22. 28004 Madrid
correo - e: ciudadano@agpd.es
tl: 901 100 099 fax: 91 445 56 99

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS