AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

El derecho fundamental a la protección de datos:

Guía para el Ciudadano

El derecho fundamental a la protección de datos:

Guía para el Ciudadano

El derecho fundamental a la protección de datos:

Guía para el ciudadano

indice

¿QUÉ ES UN DATO PERSONAL?

Vivimos en la sociedad de la información y cada día se tratan millones de datos personales. Sin el uso de nuestra información personal prácticamente ninguno de los servicios de los que disponemos podría funcionar.

Hoy día, prácticamente para cualquier actividad, nos solicitan información. Facilitamos nuestros datos personales cuando abrimos una cuenta en el banco, cuando solicitamos participar en un concurso, cuando reservamos un vuelo o un hotel, cada vez que efectuamos un pago con la tarjeta de crédito o cuando navegamos por Internet.

El nombre y los apellidos, la fecha de nacimiento, la dirección postal o de correo electrónico, el número de teléfono, el DNI, la matrícula del coche y muchos otros datos que usamos a diario constituyen información valiosa que podría permitir identificar a una persona, ya sea directa o indirectamente. Gracias a esta información podemos desarrollar nuestra actividad cotidiana, inscribimos a nuestros hijos en el colegio, recibimos atención sanitaria, realizamos llamadas telefónicas o disfrutamos de nuestro ocio.

Nuestros datos pueden ser recogidos en ficheros que dependen de las administraciones públicas y de empresas y organizaciones privadas que los utilizan para desarrollar su actividad.

Debemos ser conscientes de que toda esta información revela aspectos de nuestra personalidad. Qué bienes compramos y dónde lo hacemos, nuestra historia clínica, nuestro perfil en una red social o las fotografías y videos que subimos a nuestro espacio en Internet son información que dicen todo sobre nosotros y nuestra personalidad.

Los ejemplos sobre cómo puede tratarse nuestra información en la sociedad digital y los resultados que ofrece son muy numerosos:

¡ ■ Si somos funcionarios, tenemos un blog, o hemos participado en cualquier actividad pública y ha quedado constancia bastará con poner nuestro "nombre y apellido" entre comillas en un buscador para obtener resultados a veces sorprendentes. !

¡

- En nuestro perfil en una red social contamos desde la fecha de nacimiento y el colegio en el que estudiamos hasta cuando salimos de vacaciones.
- Algo tan simple como nuestra dirección de correo electrónico del trabajo suele indicar quienes somos y en qué trabajamos y con ello una primera aproximación a nuestro perfil económico y nuestros intereses profesionales.
- Nuestro expediente académico dice todo profesionalmente sobre nosotros.
- Aparecer en un fichero sobre solvencia con un informe negativo puede afectar a nuestra capacidad de compra.
- Recibir una ayuda o subvención depende de la comprobación de decenas de datos.

!

Por tanto, nuestra información es importante, dice quienes somos, qué cosas nos gustan, cuales son nuestras capacidades y habilidades. Nuestros datos, dicen todo sobre nuestra personalidad y es esencial al usarlos, saber cómo protegerlos.

El derecho fundamental a la protección de datos es la capacidad que tiene el ciudadano para disponer y decidir sobre todas las informaciones que se refieran a él. Es un derecho reconocido en la Constitución Española y el Derecho Europeo y protegido por la Ley Orgánica de Protección de Datos (LOPD).

Pero no sólo podemos entender el derecho fundamental a la protección de datos desde un punto de vista pasivo. Cada día muchos de nosotros tratamos datos de otras personas en Internet. Hacemos comentarios, subimos y etiquetamos fotos en foros o blogs, y probablemente en la mayor parte de las ocasiones no tenemos en cuenta si aquellos a los que nos referimos están de acuerdo con ello o les puede disgustar nuestro comportamiento.

Esta Guía tiene por objeto ayudarnos a saber como debemos actuar cuando alguien ha solicitado o utilizado nuestros datos personales y a defender nuestros derechos pero también a aprender a comportarnos adecuadamente cuando usamos datos de los demás. En nuestra sociedad, adquirir una cultura sobre protección de datos es básico para la convivencia.

CUANDO ME PIDEN LOS DATOS

Todo tratamiento de datos personales comienza con su recogida. Ésta puede realizarse de muy diversas formas:

- Verbalmente. Por ejemplo en la contratación telefónica o cuando nos damos de alta en el sistema de facturación de un comercio.
- Por escrito. Cuando rellenamos impresos de admisión o de alta.
- Usando formularios online. Cuando nos damos de alta en una red social.
- Mediante la captación de nuestras imágenes por las cámaras de vigilancia de un supermercado.

En todos estos casos, quién recoge los datos, llamado responsable del fichero o tratamiento, debe cumplir con dos obligaciones básicas:

- Informarnos.
- Solicitar nuestro consentimiento.

INFORMACIÓN

La ley reconoce a toda persona el derecho a saber por qué, para qué y cómo van a ser tratados sus datos personales y a decidir acerca de su uso.

> *«Artículo 5. Derecho de información en la recogida de datos .*
> *1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:*

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
d) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
e) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
f) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.
(...)
4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a, d y e del apartado 1 del presente artículo».

Como veremos, a continuación para poder decidir si se autoriza que traten nuestros datos debemos disponer de una información previa y adecuada. Incluso cuando puedan tratar los datos personales sin nuestro consentimiento esta información es obligatoria y forma parte de nuestros derechos fundamentales. Por ello, quien recoge nuestros datos nos debe informar de modo muy claro y comprensible sobre:

- Su identidad y dirección.
- La existencia de un fichero o tratamiento en el que incluirán nuestros datos.
- La finalidad, para la qué los necesitan o requieren.
- Si los van a facilitar con posterioridad a un tercero.
- Como ejercitar los derechos de acceso y rectificación.

La información debe ser accesible y hay muchos modos de informar:

- Visualmente mediante señales o carteles. Suele ser el método que se emplea para la videovigilancia y en aquellos casos en los que no existen impresos.
- Por escrito. Si se utiliza una ficha o impreso para recoger los datos, una instancia, un formulario etc. esta información debe estar siempre presente de modo obligatorio

. ■ Verbalmente en procesos de atención o contratación telefónica.

Normalmente esta información suele identificarse con títulos del tipo "información LOPD", "protección de datos personales", o "políticas de privacidad". Es fundamental su lectura y comprensión.

Cuando los datos no se han recogido directamente de la persona interesada los responsables deben informarle en los siguientes tres meses y, cuando se trata de información publicitaria en soporte papel que usan a partir de datos de fuentes accesibles al público, como la guía telefónica, ésta información deberá incluirse en cada comunicación publicitaria.

CONSENTIMIENTO

¡ Los datos personales solamente pueden recogerse y emplearse si hemos dado nuestro consentimiento. Sólo en algunos casos muy concretos, la Ley permite que se recojan datos sin autorización del ciudadano. !

> *«Artículo 6. Consentimiento del afectado.*
> *1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.*
> *2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.*
> *3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos».*

Por tanto la regla general consiste en que nos soliciten permiso para tratar nuestros datos. Además, el consentimiento reúne ciertas características que deben respetarse:

- Es libre. Salvo que la ley lo disponga no podemos ser obligados a facilitar nuestros datos. En caso de que así fuera nos deben informar del carácter obligatorio de las preguntas que realicen y de las consecuencias que se derivan si nos negamos a facilitar datos.

- Es previo e informado. Por tanto, la información sobre el tratamiento siempre debe existir antes de que, por ejemplo en Internet, marquemos la opción de aceptación.

- Es específico. No consentimos en que traten nuestros datos para cualquier cosa que deseen. Nos tienen que señalar de modo concreto para qué se van a usar.

- Es revocable. Excepto cuando sea obligatorio facilitar los datos, si pudimos consentir libremente podremos retirar nuestro consentimiento del mismo modo.

Sin embargo, hay casos en los que nuestros datos pueden tratarse sin nuestro consentimiento. Suele suceder cuando es necesario tratarlos porque así lo establece una Ley. La propia Ley Orgánica de Protección de Datos ha previsto algunos supuestos:

- Para las funciones propias de las Administraciones Públicas en el ámbito de sus competencias. Por eso, para tratar los datos personales por los servicios sociales de un Ayuntamiento, o para la gestión de los impuestos, no hace falta nuestro consentimiento.

- Cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento. Al formalizar un contrato laboral hay ciertos datos como los de identificación o los relativos a la cuenta bancaria para el pago del salario, que obligatoriamente deben facilitarse. Esta regla se aplicaría también cuando solicitamos una beca o ayuda y, en general en todo tipo de relaciones jurídicas.

- Cuando se utilizan datos que figuren en fuentes accesibles al público. Por ejemplo, cuando utilizan los datos que existen en la guía telefónica para remitirnos publicidad.

Por último, hay datos que por su relevancia para la intimidad o para garantizar la libertad y la no discriminación son merecedores de una especial protección.

> *«Artículo 7. Datos especialmente protegidos.*
> *1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.*
> *Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.*
> *2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.*
> *3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente. (...)».*

En estos casos existen reglas especiales:

- Si alguien distinto del partido político del que somos militantes, del sindicato al que estamos afiliados, de nuestra iglesia o culto, o de la asociación o fundación en la que participamos en relación con nuestras creencias, solicita datos relacionados con todas estas materias necesitará de nuestro consentimiento expreso y escrito.

- Del mismo modo, si los datos que se demandan se refieren a aspectos raciales, -como el color de la piel, raza concreta etc.-, salud, -como las enfermedades padecidas, análisis clínicos, radiografías etc.-, o vida sexual, -como hábitos sexuales, prácticas de riesgo, uso de anticonceptivos etc.-, se requiere nuestro consentimiento expreso.

En ambos casos, la existencia de una información previa que defina con precisión los aspectos esenciales del tratamiento que se va a realizar es una condición indispensable.

Existen excepciones pero deben estar fijadas por una norma con rango de Ley. La propia LOPD contempla algunos casos:

- Cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado. Es lógico que si nos atienden con motivo de una urgencia médica y nos practican pruebas de las que obtendrán información personal prevalezca nuestra salud y seguridad sobre nuestro derecho a la protección de datos personales.

  Debemos saber que los datos de salud pueden ser tratados por los profesionales de la salud, -médicos, personal de enfermería, fisioterapeutas, odontólogos etc.-, a los que acudamos o nos traten ya sea en su consulta privada o en un centro público, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

- Cuando se trate de datos recabados en el marco de una investigación policial concreta siempre que ello sea absolutamente necesario.

Por último, el consentimiento afecta también a las cesiones de datos personales. Una cesión o comunicación de datos se produce cuando el dato se facilita, aunque sólo sea para su consulta a alguien distinto del responsable, de las personas que prestan sus servicios en la entidad, o del afectado cuyos datos se traten. La regla básica consiste en que sólo con consentimiento o cuando una Ley lo permita pueden cederse datos personales.

«Artículo 11. Comunicación de datos.
1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.
2. El consentimiento exigido en el apartado anterior no será preciso:
a. Cuando la cesión está autorizada en una ley.
b. Cuando se trate de datos recogidos de fuentes accesibles al público.
c. Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
d. Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.
e. Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
f. Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica».

Para poder realizar una cesión con nuestro consentimiento nos deben informar previamente indicando la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y el tipo de actividad desarrollada por el cesionario.
Por último no debe olvidarse que:

- El consentimiento es revocable. Siempre que hayamos consentido en un tratamiento podemos revocar este consentimiento y además debe ser mediante un procedimiento gratuito, como el envío mediante un sobre prefranqueado, un teléfono gratuito o los servicios de atención al cliente.

- Cuando celebramos un contrato deberá permitir al afectado que manifieste expresamente su negativa al tratamiento o comunicación de datos para finalidades distintas del mismo. Para ello debería existir una casilla claramente visible y que no se encuentre ya marcada en el documento que se le entregue para la celebración del contrato que permita manifestar su negativa.

CÓMO DEBEN TRATARSE LOS DATOS

Las reglas que se aplican a los datos personales van más allá de la imposición de deberes para su obtención y establecen obligaciones que garantizan que el responsable de los tratamientos actuará adecuadamente. Para ello debe garantizarse la calidad de los datos, la seguridad y el secreto.

CALIDAD

Este principio legal tiene un contenido complejo que se manifiesta a través de varios subprincipios fijados por el artículo 4 de la LOPD.

En primer lugar, existe un deber de proporcionalidad.

> *«1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido».*

La proporcionalidad supone que cuando nos soliciten datos personales deberán limitarse a los estrictamente necesarios.

¡ Por ejemplo, cuando autorizamos que nos envíen publicidad no deberían pedirnos más datos que los de identificación requeridos para el envío. Si, por el contrario se trata de una publicidad personalizada en función de nuestros gustos es lógico que nos pregunten por ellos.

Cuando nuestros hijos se matriculan en un centro escolar es lógico que se soliciten datos familiares, incluso datos relacionados con la salud y alimentación del menor. Sin embargo, realizar un perfil de consumo familiar para remitir promociones podría ser excesivo. !

Siempre debemos fijarnos en que exista información suficiente respecto de qué datos se solicitan, para qué pretenden utilizarse y si no son datos excesivos.

La información sobre la finalidad define también un límite infranqueable para el responsable. No puede en ningún caso utilizar los datos para finalidad distinta de aquella sobre la que informó. Si pretende hacerlo deberá solicitar permiso

> *«2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos».*

Por ello, cuando contratamos cualquier producto o servicio, -una cuenta bancaria, consultamos a un asesor, adquirimos un paquete vacacional etc.- nuestros datos sólo pueden ser usados para proveernos del producto o servicio o para la facturación. Cualquier uso para finalidad distinta exigirá nuestro consentimiento informado o autorización por una ley.

Otro de los elementos esenciales para un adecuado tratamiento de los datos personales es la exactitud:

«3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.
4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16».

Para el funcionamiento de la sociedad de la información la exactitud de los datos personales es esencial. Cada vez más se adoptan decisiones a partir de los datos disponibles. Que se nos conceda una beca, que una notificación o requerimiento nos sea comunicada a nuestro domicilio o que una deuda telefónica sea la que corresponda depende del correcto cumplimiento de este principio. Un error, por ejemplo en datos relativos a una deuda, puede tener consecuencias gravísimas si el dato se incluye en un fichero de información sobre solvencia, más conocidos como ficheros de morosos.

Precisamente por ello, corresponde a la entidad que trata datos personales asegurarse de corregir los errores que existan en la información personal que maneja cuando tenga constancia de ellos.

En relación con los principios anteriores se establece una obligación de cancelar los datos cuando dejen de ser necesarios:

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

La regla que se aplica en este caso es muy sencilla: si ya no existe ninguna finalidad ni por tanto necesidad de tratar los datos personales, estos deben ser cancelados. No obstante, debemos ser conscientes de que la cancelación es un aspecto complejo de la gestión de datos personales que debe respetar ciertas reglas:

- Lo habitual consiste en cancelar los datos de modo automático cuando hayan dejado

de ser necesarios. Pero no siempre es así ya que en muchas ocasiones existe obligación de conservar los datos por razones legales vinculadas a la responsabilidad o al tipo del dato y la finalidad del fichero.

¡ El expediente académico en cualquier nivel educativo no debe desaparer ya que las autoridades educativas deben acreditar el grado de estudios alcanzados.

La historia clínica en una consulta privada se conserva al menos durante los cinco años posteriores a la última asistencia.

Si compramos un producto sujeto a garantía podría resultar necesario mantener nuestros datos durante el periodo de la misma. !

- El responsable debe además almacenar los datos de modo adecuado para facilitar el derecho de acceso.

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

Ello se debe, como se expone más adelante a que el derecho a conocer qué datos se encuentran en poder del responsable forma parte del derecho fundamental a la protección de datos.

- En caso de que con motivo de un tratamiento de datos personales consideremos que se ha producido cualquier infracción o hayamos sufrido un perjuicio debemos saber que los datos, aún cancelados, deben estar disponibles para la autoridad competente por periodos que dependen de cada sector. Así, el responsable debe mantenerlos bloqueados y no podrá utilizarlos, pero si los requiere una autoridad, o un tribunal, deberá ponerlos a su disposición.

Por último, el responsable debe actuar de modo leal y lícito en la recogida de datos, no puede ni debe usar engaños o infringir la le ley:

«7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos».

SEGURIDAD

El responsable que trata datos personales debe garantizar su seguridad:

> *«Artículo 9. Seguridad de los datos.*
> *1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estéen expuestos, ya provengan de la acción humana o del medio físico o natural.*
> *2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.*
> *3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley».*

Disponer de políticas de seguridad supone garantizar la integridad, disponibilidad y confidencialidad de los datos.

- La integridad nos asegura que los datos no van a sufrir modificaciones no autorizadas.

¡ Para ello los responsables asignan contraseñas individuales para identificar y autenticar a las personas autorizadas para consultar o tratar datos, establecen qué personas pueden acceder al lugar físico en el que se encuentran los expedientes, los sistemas disponen de recursos de timing out que cierran una sesión de trabajo si no se está haciendo nada, o se aseguran de que nadie pueda manipular un ordenador a través de Internet o situado tras un mostrador. !

- La disponibilidad permite que los datos estén siempre a disposición de las personas autorizadas, pudiendo ser recuperados, cuando algún evento físico o de cualquier otro tipo afecta a su funcionamiento normal.

¡ Así en caso de un accidente, incendio, inundación o caída de la tensión eléctrica, o de padecer un virus, se pueden restaurar los datos acudiendo a una copia de seguridad. !

- La confidencialidad comporta que los datos sólo sean conocidos y accesibles a los

usuarios autorizados del sistema de información. Cualquier problema de seguridad en éste ámbito puede afectar al deber de secreto.

¡ Por ello los responsables se sirven de la asignación de usuarios y contraseñas individuales, establecen políticas de destrucción de papel o soportes desechados (CD-ROM, DVD etc.), la prohibición de depositar soportes que contengan datos en los contenedores de basura, o garantizan que las pantallas situadas en un mostrador no sean consultadas a simple vista por cualquier cliente. !

SECRETO

El secreto es esencial para garantizar el derecho fundamental a la protección de datos. Sin secreto sobre los datos sobre los que se conozca no existiría este derecho.

«*Artículo 10. Deber de secreto.*
El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal estén obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo."

Este deber de secreto afecta a todas las personas que accedan a información personal contenida en un sistema sujeto al cumplimiento de lo previsto por la Ley Orgánica de Protección de Datos Personales.

¡ Esto explica, por ejemplo que en determinados servicios de atención telefónica se realicen preguntas para establecer la identidad del cliente antes de facilitar datos, que en un hospital nunca nos faciliten información sobre una persona que esté siendo atendida, o que nunca nos den acceso a datos de personas mayores de edad, aunque se trate de familiares directos, si no aportamos un escrito probando que nos han otorgado su representación. !

MIS DERECHOS

Si el derecho fundamental a la protección de datos se puede definir como un derecho a ejercer un control sobre nuestra información personal, necesitamos de herramientas concretas para poder hacer posible este control. Estos instrumentos son distintas facultades que establece la LOPD cuando regula los derechos de consulta, acceso, rectificación, cancelación y oposición.

CONSULTA

El derecho de consulta permite saber a través de un registro público quién puede haber tratado nuestros datos.

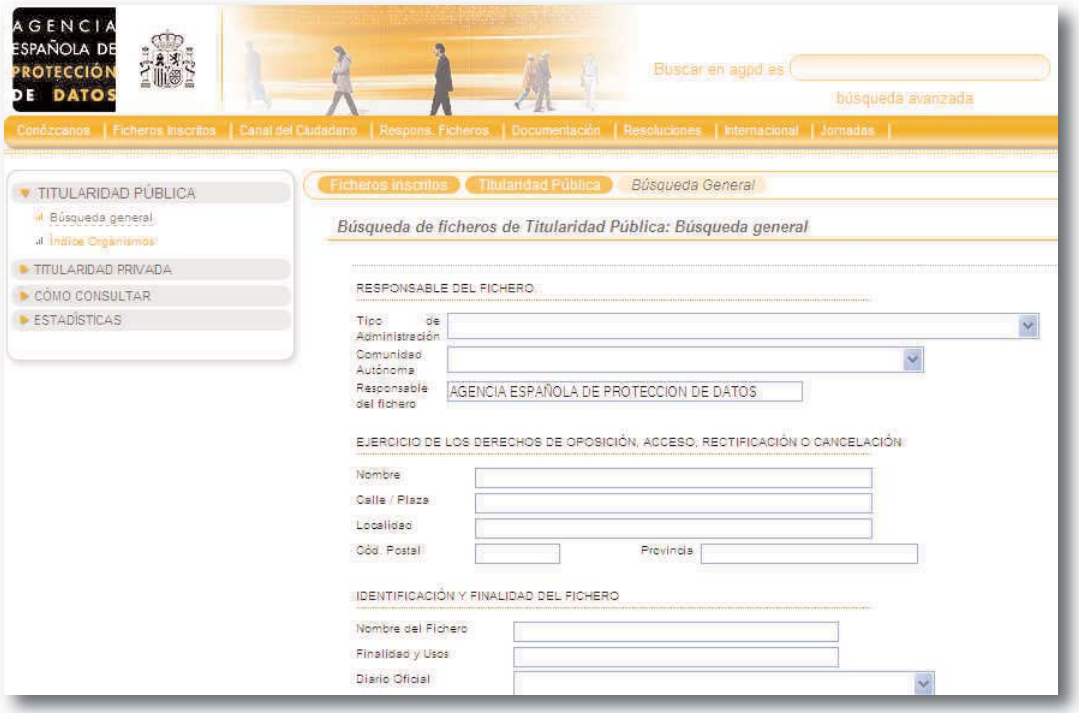
> «*Artículo 14. Derecho de consulta al Registro General de Protección de Datos.*
> *Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita».*

Todos los responsables deben inscribir sus ficheros ante el Registro General de Protección de datos al que puede accederse desde la dirección http://www.agpd.es.

De éste modo, por ejemplo, si se recibiese una carta desde la Agencia Española de Protección de Datos informando sobre un curso sin que nos conste haber permitido el uso de nuestros datos, o sin ninguna información que nos permita saber como dirigirnos al responsable del tratamiento realizaríamos los siguientes pasos:

- Conectarse al Registro General de Protección de datos y, sabiendo que la Agencia Española de Protección de Datos es una administración, escogiendo de la pestaña superior "Ficheros inscritos" la opción "titularidad pública".

- Utilizar de entre las opciones de búsqueda la que nos resulte útil. Por ejemplo incluyendo la denominación "Agencia Española de Protección de Datos" en el campo "responsable del fichero" de la búsqueda general:



■ A partir del resultado podemos escoger entre los distintos ficheros publicados aquél que se ajuste a la naturaleza del escrito que recibimos:

■ En este caso podríamos escoger el fichero "Formación, premios o eventos" y el Registro nos proporcionará una información básica o más amplia:

DERECHOS ARCO

A través de los derechos de acceso, rectificación, cancelación y oposición, también conocidos como derechos ARCO, podemos saber qué información personal se está tratando por un responsable, de quién o de dónde se obtuvIeron los datos y a quién se los ha cedido. modificar o rectificar errores, cancelar datos que no se deberían estar tratando u oponernos a tratamientos de datos personales realizados sin nuestro consentimiento.

Para ejercer estos derechos hay un conjunto de aspectos que debemos conocer:

- El ejercicio de los mismos es personalísimo, y debe, por tanto, ser ejercido directamente por los interesados ante cada uno de los responsables/titulares de los ficheros. Si tuviéramos que actuar en nombre de otra persona necesitaríamos acreditar que nos ha autorizado para representarla.

¡ Vd. puede dirigirse a cada una de las empresas u organismos públicos, de los que sabe o presume que tienen sus datos, solicitando información sobre qué datos tienen y cómo los han obtenidoy las cesiones que, a su vez, haya realizado (derecho de acceso), la rectificación de los mismos, o en su caso, la cancelación de los datos en sus ficheros (derecho de cancelación). !

- Debemos dirigirnos directamente al responsable del fichero en el que se encuentren nuestros datos personales, utilizando cualquier medio que permita acreditar el envío y la recepción de la solicitud, acompañando copia de nuestro D.N.I. o pasaporte e indicando el fichero o ficheros a consultar.

¡ Puede utilizarse por ejemplo una solicitud debidamente registrada ante una administración pública. Si el responsable ha habilitado sistemas de ejercicio de estos derechos a través de servicios de atención al cliente, formularios online etc. en los que se garantice un ejercicio personalísimo, también serán válidos. En estos casos debe guardarse la confirmación electrónica de entrega y/o lectura que es conveniente activar siempre. !

- Son derechos independientes.

¡No es necesario ejercitar primero el derecho de acceso para poder rectificar o cancelar. Si, por ejemplo sabemos que la dirección de la que dispone el responsable es errónea, podemos rectificarla directamente.!

- El ejercicio de estos derechos debe ser sencillo, gratuito, no puede suponer ingreso adicional alguno para el responsable y aunque éste disponga de un procedimiento propio para ello, no puede desatender una solicitud que debidamente presentada utilice otro medio.

¡Esto significa que el responsable no puede establecer como modo de ejercicio de estos derechos un línea telefónica de tarificación adicional, o exigir el envío de un certificado o burofax.!

- El contenido de las solicitudes viene establecido por el artículo 25 del Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos:

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

  - Petición en que se concreta la solicitud.

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

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

- El responsable debe atender la petición, incluso cuando no existan datos personales del solicitante, y garantizar que su organización sea capaz de informar sobre cómo ejercer los derechos.

Puede obtenerse información y modelos para el ejercicio de los derechos en el Canal del Ciudadano de la Agencia Española de Protección de Datos.

Una vez planteado el ejercicio de uno de los derechos ARCO hay que saber que cada uno reúne características diferentes.

DERECHO DE ACCESO

Este derecho se caracteriza por:

- Nos permite conocer obtener gratuitamente información sobre nuestros datos de carácter personal sometidos a tratamiento.

- El contenido del acceso 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. El afectado podrá obtener del responsable información relativa a datos concretos, a datos incluidos en un determinado fichero o a la totalidad de sus datos sometidos a tratamiento.

- Sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que se acredite un interés legítimo al efecto

- La petición debe ser atendida en el plazo máximo de un mes a contar desde la recepción de la solicitud, momento a partir del cual el acceso deberá hacerse efectivo en un máximo de 10 días hábiles.

- El artículo 15.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, reconoce el derecho del afectado a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos así como las comunicaciones realizadas o que se prevén hacer de los mismos.

- El afectado podrá optar por recibir la información a través de uno o varios de los siguientes sistemas de consulta del fichero:

- Visualización en pantalla.

- Escrito, copia o fotocopia remitida por correo, certificado o no.

- Telecopia.

- Correo electrónico u otros sistemas de comunicaciones electrónicas.

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

DERECHO DE RECTIFICACIÓN

Este derecho se caracteriza por:

- Permite corregir errores, modificar los datos que resulten ser inexactos o incompletos y garantizar la certeza de la información objeto de tratamiento.

- La solicitud de rectificación deberá indicar a qué datos se refiere y la corrección que haya de realizarse y deberá ir acompañada de la documentación justificativa de lo solicitado.

- El responsable del fichero resolverá sobre la solicitud de rectificación o cancelación en el plazo máximo de diez días hábiles a contar desde la recepción de la solicitud.

- Si los datos rectificados hubieran sido cedidos previamente, el responsable del fichero deberá comunicar la rectificación efectuada al cesionario, en idéntico plazo, para que éste, también en el plazo de diez días contados desde la recepción de dicha comunicación, proceda, asimismo, a rectificar los datos.

DERECHO DE CANCELACIÓN

Este derecho se caracteriza por:

- Permite que se supriman los datos que resulten ser inadecuados o excesivos. La cancelación implica el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones Públicas, Jueces y Tribunales. Transcurrido el plazo legal de prescripción de las responsabilidades legales derivadas del tratamiento, deberá procederse a la supresión de los datos.

- En la solicitud de cancelación, el interesado deberá indicar a qué datos se refiere, aportando al efecto la documentación que lo justifique, en su caso.

- El responsable del fichero resolverá sobre la solicitud de cancelación en el plazo máximo de diez días hábiles a contar desde la recepción de la solicitud.

- Si los datos cancelados hubieran sido cedidos previamente, el responsable del fichero deberá comunicar la cancelación efectuada al cesionario, en idéntico plazo, para que éste, también en el plazo de diez días contados desde la recepción de dicha comunicación, proceda, asimismo, a cancelar los datos.

DERECHO DE OPOSICIÓN

El derecho de oposición puede ejercitarse en tres supuestos distintos:

- Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario.

¡ Aunque puede tratarse de supuestos muy excepcionales, podría darse en el caso de personas que hayan sido víctimas de violencia de género. Se expondrían a riesgos para su seguridad si sus datos se publicasen , por ejemplo, en la web de la empresa en la que trabaje. !

En este caso:

- En la solicitud deberán hacerse constar los motivos fundados y legítimos, relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho.

■ Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, cualquiera que sea la empresa responsable de su creación. Este supuesto es distinto del envío de publicidad por medios electrónicos que se examina mas adelante.

¡ Habitualmente recibimos publicidad personalizada mediante buzoneo ya sea porque han obtenido nuestros datos de una fuente accesible al público, ya sea porque consentimos en el marco de una relación. !

La oposición se rige aquí por principios específicos:

- No es necesario aportar motivo alguno:

¡ Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud. !

- Si la campaña publicitaria se realizase por ejemplo, utilizando ficheros de una empresa contratada, debe trasladar la petición al anunciante en un máximo de 10 días.

¡ Si el derecho de oposición se ejercitase ante una entidad que hubiera encomendado a un tercero la realización de una campaña publicitaria, aquélla estará obligada, en el plazo de diez días, desde la recepción de la comunicación de la solicitud de ejercicio de derechos del afectado, a comunicar la solicitud al responsable del fichero a fin de que el mismo atienda el derecho del afectado en el plazo de diez días desde la recepción de la comunicación, dando cuenta de ello al afectado. !

■ Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal.

¡ Se trata de supuestos, por ahora poco habituales en los un programa informático propone una decisión que nos afecta, utilizando para ello algún tipo de análisis sobre datos personales. Un ejemplo podría ser el desarrollo de tests psicotécnicos en procesos de selección de personal. !

En estos casos hay que tener en cuenta que:

- La regla general es que cabe oponerse libremente.

1. Los interesados tienen derecho a no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta.

- Sin embargo este tratamiento sería posible en la celebración o ejecución de un contrato a petición del interesado, siempre que se respeten las siguientes condiciones:

Que la persona afectada pueda alegar lo que estimara pertinente, a fin de defender su derecho o interés.

Que el responsable informe previamente al afectado, de forma clara y precisa, de que se adoptarán decisiones basadas en un tratamiento automatizado de datos personales y que cancelará los datos en caso de que no llegue a celebrarse finalmente el contrato.

También será posible cuando esté autorizada por una norma con rango de Ley que establezca medidas que garanticen el interés legítimo del interesado.

En todos los casos examinados el derecho de oposición deberá ser atendido en un máximo de 10 días hábiles.

NO HAN RESPETADO MIS DERECHOS ¿QUÉ PUEDO HACER?

Tanto en el caso de que no se atienda, como en el que se deniegue el ejercicio de un derecho de acceso, rectificación, cancelación u oposición, el afectado puede dirigirse a la Agencia Española de Protección de Datos o a las Agencias autonómicas existentes en las Comunidades Autónomas de Madrid, Cataluña y País Vasco cuando se trate de ficheros de administraciones públicas bajo su competencia, -como la autonómica, la municpal o las universidades públicas-, solicitando la tutela de sus derechos:

> *« Artículo 18. Tutela de los derechos.*
> *1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia Española de Protección de Datos, en la forma que reglamentariamente se determine.*
> *2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia Española de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación.»*

Otra opción, de la que disponemos es la de presentar una denuncia ante una infracción a la Ley Orgánica Protección de Datos. Estas denuncias pueden referirse a cualquier vulneración de la normativa de protección de datos, así como la relativa al envío de mensajes publicitarios por medios electrónicos.. La Agencia Española de Protección de Datos, tiene la función de velar por el cumplimiento de la legislación y controlar su aplicación, y para ello dispone de las potestades de inspeccionar y sancionar las infracciones que constate.

¡ En su actividad de inspección o sanción la Agencia Española de Protección de Datos ha detectado incumplimientos relacionados con la falta de registro de ficheros, la ausencia de cláusulas o carteles informativos, infracciones a la seguridad como el abandono de documentos con datos en la basura, tratamiento de datos personales de menores sin consentimiento, altas indebidas en registros de morosidad o el llamado SPAM, entre otros supuestos. !

La Agencia Española de Protección de Datos dispone de información y modelos de reclamaciones en el Canal del Ciudadano.

¿PUEDO TRATAR LOS DATOS DE OTRAS PERSONAS?¿QUÉ DEBO HACER?

La llamada Web 2.0 y las redes sociales han supuesto un cambio profundo en nuestro modo de comportarnos en Internet. Por medio de nuestros blog, en espacios en los que compartimos fotografías y video, y en las redes sociales solemos tratar información de familiares y amigos, e incluso de personas con las que no tenemos una relación directa.

Como regla general no adquirimos ninguna obligación en materia de protección de datos cuando:

- Estamos ejerciendo legítimamente nuestro derecho de información o la libertad de expresión.

¡ Debemos tener en cuenta que por el mero hecho de informar sobre algo no estamos exentos de responsabilidad. Debe informarse sobre hechos o personas con relevancia pública, debemos haber tratado de verificar la certeza de la información, y ésta debe ser de interés público. Del mismo modo, para opinar debemos ser respetuosos con la dignidad de las personas objeto de nuestra crítica. !

- El entorno en el que publicamos datos, -como cuando escribimos sobre alguien identificándolo, o subimos o etiquetamos una fotografía-, es cerrado. Esto es, nuestro perfil no está abierto a todos los usuarios de la red social, o a los amigos de los amigos.

¡ Así, si etiquetamos en Internet una fotografía que pueda ver cualquiera sin permiso del afectado, podríamos incurrir en responsabilidad en materia de protección de datos personales. !

Sin embargo, incluso aunque no se aplicase la Ley Orgánica de Protección de Datos personales a nuestro comportamiento en Internet, no dejan de existir riesgos que deben ser tenidos en cuenta:

- Podemos ser responsables por daños causados a la imagen, reputación o intimidad de

otras personas.

- Los datos personales que se publican en Internet disponibles para cualquiera pueden escapar a nuestro control y ser muy difíciles de eliminar con posterioridad.

- Podemos poner en situación de riesgo a otras personas, especialmente cuando se trate de imágenes de menores o personas con discapacidad.

- Internet es un medio con características muy específicas: lo que en el mundo físico puede no ser más que una broma de mal gusto en Internet puede causar graves perjuicios.

Si se está interesado en este aspecto de la protección de datos personales es muy recomendable consultar las publicaciones de la Agencia Española de Protección de Datos. Recomendaciones a usuarios de Internet o la guía Derechos de niños y niñas, deberes de padres y madres, destinada a los menores.

¿QUÉ COSAS DEBO SABER SOBRE ALGUNOS TRATAMIENTOS DE DATOS?

Junto a las reglas generales sobre protección de datos es importante conocer aspectos específicos que se dan en algunos tratamientos que puedan resultar sensibles:

NIÑOS

La protección de los datos personales de los menores adquiere una especial relevancia en la sociedad de la información. Los menores son sujetos cuyos datos poseen gran relevancia en sectores como la escuela o el consumo de productos de ocio. Además, el acceso generalizado a Internet prácticamente desde los diez años define una generación de niños que navegan, juegan online, publican fotos, usan chats privados o se inscriben en redes sociales.

Por último, los propios padres suponen un factor positivo en la educación de los menores en este ámbito pero a veces generan prácticas de riesgo. Por ejemplo, al publicar información sobre nuestros hijos en un blog o en una red social podemos estar afectando a sus derechos o exponiéndoles a riesgos innecesarios.

Esta realidad incide particularmente sobre el derecho fundamental a la protección de datos de los menores ya que:

- Los niños no tienen, salvo que reciban una formación adecuada, capacidad de entender y discernir sobre su derecho fundamental.

- Su información personal es valiosa para muchos sectores de actividad.

- El menor puede ser utilizado de modo instrumental para obtener información sobre su entorno familiar.

- El propio menor, cuando carece de formación adecuada, incurre en prácticas de riesgo para su privacidad y seguridad o la de terceros. Ello se debe a que gran parte de las conductas de riesgo en I nternet parten de una captación inicial de datos personales como una fotografía o una dirección de correo asociada a una mensajería privada.

Por ello, distintas normas se han ocupado de proteger los derechos a la intimidad, el honor o la propia imagen del menor como la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar, y a la propia imagen o la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.

En protección de datos se aplica el artículo 13 del Reglamento de Desarrollo de la Ley Orgánica.

«Artículo 13. Consentimiento para el tratamiento de datos de menores de edad.

1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.

2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.
3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.
4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales».

Para tratar datos de menores deben respetarse ciertas reglas:

- Sólo pueden consentir por si mismos los mayores de catorce años.

¡ Por ejemplo para registrarse en una red social que admita menores de esta edad no necesitarán autorización de los padres, o para realizar actos de consumo para los que puedan consentir como alquilar videojuegos aptos para su edad. !

- Se necesita autorización de padre, madre o tutor legal cuando:
  - Se recojan y traten datos de menores de catorce años.

¡ Así, cuando un menor realiza una actividad extraescolar prestada por un tercero, como cursos voluntarios no ofrecidos por el colegio o excursiones con alojamiento, se necesitará el consentimiento paterno o materno, o cuando proceda de un representante legal. !

  - Los mayores de catorce años cuando la Ley la exija.

¡ Hay actividades que un menor no puede realizar sin autorización de sus padres como adquirir y/o conducir un ciclomotor, explotar comercialmente su imagen personal, contratar una cuenta bancaria o disponer de una tarjeta de débito. Cualquier tratamiento de datos personales en este tipo de casos requiere también del consentimiento paterno o materno, o cuando proceda de un representante legal. !

- Se prohíbe utilizar al menor para recabar datos que permitan obtener información

sobre los demás miembros del grupo familiar, o sobre las características del mismo sin el consentimiento de los titulares de tales datos.

¡ Ya no es admisible, por ejemplo, exigir en el registro de un menor en una página de Internet obligarle a facilitar datos personales de sus padres como el nivel de renta, el tipo vivienda, el coche que utilizan etc. !

- Podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización para el tratamiento de los datos de los menores.

¡ Esta posibilidad se establece para que el responsable pueda dirigirse a los padres y obtener la autorización correspondiente. !

- Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible.

¡ Las políticas de privacidad habituales con tecnicismos legales de difícil comprensión o expresiones formales que no se corresponden con la edad del niño no son admisibles. Deberá recurrirse aun lenguaje didáctico y coloquial. !

- El responsable del fichero o tratamiento debe disponer de procedimientos para verificar la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales.

¡ No basta, especialmente en Internet, con lo que el menor declare. Algunas entidades solicitan que se rellenen formularios de declaración de la edad y/o autorización parental y que se remitan por fax o se digitalicen y envíen por correo electrónico acompañados de documentación acreditativa también digitalizada. !

La Agencia Española de Protección de Datos pone a disposición de los ciudadanos una página dedicada a la protección de datos de los menores con información adicional, guías y recursos.

INTERNET

En los últimos años Internet ha cambiado profundamente. Antes nos limitábamos a navegar buscando información y en algunos casos nos registrábamos para realizar compras u obtener distintos servicios.

La Internet de hoy, el llamado Web 2.0 y en particular las redes sociales, suponen un cambio profundo.

- Para ser eficaz en una red social el individuo se identifica. La identidad posee por ello un valor extraordinario.
  - La información, el mensaje, la publicidad son personalizadas.

¡ El anuncio que vemos en pantalla está pensado para nuestro sexo, perfil de edad, nivel de estudios y/o grupos a los que nos hemos adherido en la red de la que se trate. !

  - Se utilizan estrategias de viralidad para diseminar la información.

¡ Así se notifica a "nuestros amigos" todo lo que hacemos y nos gusta lo cual facilita las estrategias publicitarias, o se acude a los propios usuarios para que difundan publicidad a sus "amigos" a cambio de premios. !

- Los espacios de comunidad en Internet se presentan y se perciben como ámbitos equivalentes a los del mundo físico en los las reglas de juego del entorno no las define el usuario. Cuando se registra se somete a unas reglas contractuales fijadas por el proveedor de servicios aunque se presentan al usuario con una apariencia de gratuidad. Sin embargo existe una transacción: facilitamos nuestros datos personales.

¡ Cuando nos registramos en una red social no solemos verificar la información legal, no sabemos qué se puede hacer con nuestros datos, o como está configurado el entorno, quién puede consultar nuestra información y para que finalidad. !

- El usuario debe conocer las reglas del juego para mantener algún control sobre su información personal y la de terceros y los proveedores de servicios de redes sociales están obligados a respetar ciertos principios en esta materia. Por ello deberían:

  - Informar a los usuarios de su identidad y proporcionarles información clara y completa sobre las finalidades y las distintas maneras en que van a tratar los datos personales.

  - Establecer procedimientos que sean respetuosos con la intimidad. Para ello las políticas de privacidad deben ser claras y ofrecer el perfil del usuario preferentemente cerrado o en todo caso, que permita al usuario una fácil configuración.

  - Informar y advertir a sus usuarios frente a los riesgos de atentado a la intimidad cuando transfieren datos a los Servicios de Red Social SRS.

  - Recomendar a sus usuarios no poner en línea imágenes o información relativa a otras personas sin el consentimiento de éstas.

  - En la página inicial debería figurar un enlace hacia una oficina de reclamaciones, tanto para miembros como para no miembros, que cubra cuestiones de protección de datos.

  - Deberían establecer plazos máximos de conservación de los datos de los usuarios inactivos y suprimir las cuentas abandonadas.

  - Por lo que se refiere a los menores deberían adoptar medidas adecuadas con el fin de limitar los riesgos.

Junto a las redes sociales el impacto más apreciable en los derechos de los ciudadanos se produce con motivo de la publicación de datos personales en sitios web, blogs o foros que son indexados por los buscadores. Esta indexación multiplica los efectos dañinos cuando la publicación no debería haberse producido, cuando resulta inexacta o desproporcionada ya que:

■ Hace visible de modo muy rápido toda esta información dándole una relevancia que por si mismo no alcanzaría el sitio web.

¡ Un foro de debate minoritario, un boletín municipal, un blog poco consultado son indexados con la misma eficacia que la página más vista. Por ello, personas cuya visibilidad en internet es limitada se encuentran con que toda se información puede concentrarse en un par de páginas con registros de búsqueda. Basta con poner su nombre entre comillas y esperar unas décimas de segundo. !

■ Permite integrar de modo conjunto información dispersa facilitando la elaboración de perfiles de una misma persona.

¡ Así, encontraremos información sobre si se tiene cuenta en una red social abierta a las búsquedas, publicaciones en diarios oficiales u opiniones manifestadas en foros abiertos. De este modo con muy poco esfuerzo podríamos conocer profesión, actividades preferidas o hobbies, e incluso la ideología de una persona, con muy poco esfuerzo. !

■ Aunque desaparezca el sitio web donde se encontraba la información o cuando ésta se elimina, si la información no se borra del archivo histórico o memoria caché del buscador permanecerá disponible durante un periodo tras su supresión en el origen.

El derecho a la protección de datos ofrece herramientas que pueden utilizarse para defender nuestros derechos en Internet. Para ello es conveniente seguir con ciertas reglas de actuación:

■ Debemos dirigirnos al web, blog, foro o cualquier otro espacio de internet en el que se encuentra la información y ejercer nuestros derechos de cancelación u oposición. Habitualmente los responsables de estos espacios disponen de páginas de denuncia sobre contenidos no deseados que suelen ser el cauce adecuado para ejercer estos derechos.

■ Además deberíamos verificar la desaparición de esta información en los principales buscadores, asegurarnos de que no se encuentra indexada y, en su caso, ejercer nuestros derechos ante estos.

PUBLICIDAD

La realización de campañas publicitarias personalizadas requieren del tratamiento de datos personales. Cuanto mas específico sea el destinatario de la publicidad más intensa será la necesidad de tratar datos para lograr transmitir un mensaje.

La Ley 34/1988, de 11 de noviembre, general de publicidad, define esta actividad como:

> *«toda forma de comunicación realizada por una persona física o jurídica, pública o privada, en el ejercicio de una actividad comercial, artesanal o profesional, con el fin de promover de forma directa o indirecta la contratación de muebles o inmuebles, servicios, derechos y obligaciones»*

Por otra parte, junto a esta publicidad en sentido tradicional la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico regula el desarrollo comunicaciones comerciales realizadas por vía electrónica, -correo electrónico o SMS entre otros-, definiendo una comunicación comercial como:

> *«toda forma de comunicación dirigida a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional».*

Para realizar estas actividades debemos distinguir la publicidad más tradicional de la realizada por medios electrónicos ya que las reglas reglas que se aplican son diferentes.

PUBLICIDAD A TRAVÉS DE MEDIOS NO ELECTRÓNICOS

Para la realización de campañas comerciales los datos personales pueden obtenerse de diversas formas.

- Mediante el uso de datos obtenidos de fuentes accesibles al público:

i Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente,

el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación..

Ésta es la publicidad para la que por ejemplo se utilizan los datos contenidos en guías o listines telefónicos. En éste ámbito debemos saber que:

- Se requiere consentimiento expreso, previo e informado del abonado:

  - Para ser incluido por primera vez en la guía telefónica.

  - Para que aparezcan en la guía datos adicionales a los que la normativa identifica como mínimos: nombre, dirección, -excepto el piso y letra o identificador de la puerta, y operador de acceso que proporciona el servicio de telefonía.

- Asimismo, el abonado tiene derecho a que los datos que aparecen en la guía no puedan ser utilizados con fines de publicidad o prospección comercial, debiendo constar así de manera clara en la guía mediante el signo U.

- El receptor de la publicidad obtenida de fuentes accesibles al público debe ser informado en cada comunicación sobre el origen de los datos y la identidad del responsable del tratamiento, los derechos que le asisten y ante quién podrá ejercitarlos. Además, hay que informar de que sus datos provienen de una fuente accesible al público y la entidad de la que hubieran sido obtenidos.

- Como se indicó anteriormente podemos oponernos a la envío de esta publicidad.

- Obteniendo el consentimiento del destinatario de la publicidad.

En este caso quien nos remite publicidad debe haber obtenido previamente nuestro consentimiento. Para ello deberíamos haber sido informados con claridad y precisión sobre el hecho de que nuestros datos personales serán utilizados para remitirnos información

comercial, así como de los sectores específicos y concretos de actividad de los que podremos recibir publicidad. Este consentimiento puede obtenerse de los siguientes modos:

- EXPRESAMENTE

  Se produce cuando tras haber sido informados sobre todos los detalles del tratamiento de nuestros datos se nos requiere para que manifestemos de modo activo nuestra voluntad de recibir este tipo de comunicaciones.

  Este consentimiento se presta para finalidades determinadas, explícitas y legítimas relacionadas con publicidad o prospección comercial y deberá existir información previa sobre los sectores específicos y concretos de actividad de los que podrá recibir información o publicidad. Cuando con motivo de un contrato, adicionalmente se prevea el envío de información deberá existir una casilla visible y no premarcada o un procedimiento equivalente que permita negarse.

No debemos olvidar que siempre tendremos el derecho a revocar el consentimiento.

- TÁCITAMENTE

  Se trata de aquellos supuestos en los que no es necesaria una respuesta afirmativa para consentir. Basta con que no manifestemos nada para que tras un periodo de tiempo se entienda que hemos consentido.

  Son mensajes del tipo: «Desde la entidad A deseamos utilizar sus datos personales para remitirle nuestras ofertas promocionales. Si Vd. no nos indica lo contrario en un plazo de 30 días entenderemos que nos autoriza a ello».

  Lo regula el artículo 14 del Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos.

«2. El responsable podrá dirigirse al afectado, informándole en los términos previstos en los artículos 5 de la Ley Orgánica 15/1999, de 13 de diciembre y 12.2 de este reglamento y deberá concederle 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. En particular, cuando se trate de responsables que presten al afectado un servicio que genere información periódica o reiterada, o facturación periódica, la comunicación podrá llevarse a cabo de forma conjunta a esta información o a la facturación del servicio prestado, siempre que se realice de forma claramente visible».

Cuando recibamos un mensaje en el que una entidad con la que tengamos algún tipo de relación nos solicita el consentimiento tácito debemos tener en cuenta que:

- Disponemos de un plazo de 30 días desde la recepción para manifestar nuestra negativa.

- La entidad debe asegurarse de que el envío informativo se ha entregado. Si nunca lo recibimos no puede presumir que hemos consentido.

- La negativa a recibir publicidad impide a la entidad remitirnos una nueva petición para el mismo tratamiento y finalidad hasta pasado al menos un año.

- El medio para negarse debe ser sencillo, gratuito y no implicar un ingreso adicional para la entidad.

- No debemos olvidar que cualquiera que sea la forma en la que se haya obtenido nuestro consentimiento tendremos derecho a revocarlo

FICHEROS DE EXCLUSIÓN

El Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos ha previsto la posibilidad de que solicitemos ser incluidos en ficheros de exclusión, también conocidos como listas Robinsón.

« Artículo 49. Ficheros comunes de exclusión del envío de comunicaciones comerciales.

1. Será posible la creación de ficheros comunes, de carácter general o sectorial, en los que sean objeto de tratamiento los datos de carácter personal que resulten necesarios para evitar el envío de comunicaciones comerciales a los interesados que manifiesten su negativa u oposición a recibir publicidad.

A tal efecto, los citados ficheros podrán contener los mínimos datos imprescindibles para identificar al afectado.

2. Cuando el afectado manifieste ante un concreto responsable su negativa u oposición a que sus datos sean tratados con fines de publicidad o prospección comercial, aquél deberá ser informado de la existencia de los ficheros comunes de exclusión generales o sectoriales, así como de la identidad de su responsable, su domicilio y la finalidad del tratamiento.
El afectado podrá solicitar su exclusión respecto de un fichero o tratamiento concreto o su inclusión en ficheros comunes de excluidos de carácter general o sectorial.
3. La entidad responsable del fichero común podrá tratar los datos de los interesados que hubieran manifestado su negativa u oposición al tratamiento de sus datos con fines de publicidad o prospección comercial, cumpliendo las restantes obligaciones establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento.
4. Quienes pretendan efectuar un tratamiento relacionado con actividades de publicidad o prospección comercial deberán previamente consultar los ficheros comunes que pudieran afectar a su actuación, a fin de evitar que sean objeto de tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa a ese tratamiento».

La inclusión en una lista de este tipo supone:

- Oponernos a recibir publicidad de una determinada entidad o de un sector de actividad. O a través de distintos canales publicitarios (correo postal, teléfono, correo electrónico, mensajes, SMS).

- Obliga a consultar estos ficheros a cualquier entidad que pretenda realizar una campaña publicitaria antes de realizar el envío.

- Ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

Desde el punto de vista del ejercicio de derechos rigen en este ámbito las mismas reglas que se expusieron más arriba con una particularidad. Si la entidad que realiza la campaña es distinta de la que anuncia sus productos y ejercemos nuestros derechos ante la primera, aquélla estará obligada, en el plazo de diez días, desde la recepción de la comunicación de la solicitud de ejercicio de derechos del afectado, a comunicar la solicitud al responsable del fichero a fin de que el mismo otorgue al afectado su derecho en el plazo de diez días desde la recepción de la comunicación.

PUBLICIDAD A TRAVÉS DE MEDIOS ELECTRÓNICOS

Esta es la publicidad que recibimos mediante el envío de correos electrónicos o mensajes

cortos del tipo SMS o mensajes de fax. Se trata de un tipo de publicidad regulada de modo específico por la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, más conocida como LSSI y por la Ley 32/2003 de noviembre, General de Telecomunicaciones.

¡ Habitualmente este tipo de mensajes encajan con lo que comúnmente se denomina SPAM, aunque debemos reservar este concepto para el correo comercial no solicitado. !

Es fundamental tener en cuenta que una dirección de correo electrónico o un número telefónico cuando pertenecen a una persona identificable o identificada son un datos de carácter personal. En este ámbito conviene tener en cuenta que:

- Si no se tiene relación previa con quien remite la comunicación comercial éste necesita obtener un consentimiento expreso para poder realizar el envío.

- No será necesario este consentimiento cuando exista una relación contractual previa en la que se hayan obtenido lícitamente los datos de contacto y la publicidad se refiera a productos o servicios de la propia empresa y a productos similares a los contratados.

¡ Así, sería posible que nuestro banco nos remita por este método información sobre productos financieros pero no podría hacer una campaña de publicidad para promocionar la venta de vinos. !

Además debe facilitarnos desde el primer mensaje el derecho a oponernos a recibir este tipo de mensajes a través de un procedimiento sencillo y gratuito.

¡ Un ejemplo de este cumplimiento de este tipo de obligación es la inclusión al final de los SMS publicitarios del lema no mas Publi+un número gratuito al que remitir un mensaje para oponerse. !

- La regla del consentimiento se aplica a personas físicas y jurídicas.

- No es admisible el uso de campañas del tipo "envía a un amigo" a cambio de una contraprestación para evadir las reglas del consentimiento.

¡ Cuando un amigo nos recomienda un producto o servicio debe hacerlo en el marco de una relación privada. Si una entidad utiliza a sus clientes para que realicen en su nombre una campaña comercial, por ejemplo ofreciendo ventajas a los que realicen un número mínimo de envíos estaría incumpliendo la normativa. !

- El envío de estas comunicaciones debe respetar ciertas reglas:

  - Deberán ser claramente identificables, identificar al responsable del envío e incluir al comienzo del mensaje la palabra publicidad o la abreviatura publi.

  - Disponer de procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el consentimiento que hubieran prestado y facilitar información accesible por medios electrónicos sobre dichos procedimientos.

  - Cumplir con los deberes de información y demás obligaciones que la LOPD contempla para el tratamiento de datos personales.

INFORMACIÓN SOBRE SOLVENCIA

Para facilitar una mejor valoración de los riesgos sobre la solvencia de las personas cuando contratan bienes o servicios, el legislador permite que los acreedores puedan incluir información de los deudores en los llamados ficheros de morosos sin su consentimiento. De este modo cuando una persona solicita una hipoteca, o compra un bien a plazos se suele verificar su capacidad de cumplir con sus obligaciones dinerarias consultando con la información disponible en estos ficheros. En caso de que la información que se obtenga resulte desfavorable puede negarse la concesión de un crédito o no contratarse con quién solicita un servicio o pretende comprar mediante sistemas de pago aplazado, o exigirle garantías adicionales.

Que la información sobre solvencia contenida en estos ficheros resulte veraz, adecuada y proporcional es fundamental tanto para garantizar un funcionamiento adecuado de nuestra economía como para garantizar los derechos de todos los consumidores. Por ello la Ley

es particularmente exigente en esta materia fijando requisitos muy estrictos para tratar este tipo de información.

> *«Artículo 29. Prestación de servicios de información sobre solvencia patrimonial y crédito.*
> *1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento.*
> *2. Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley.*
> *3. En los supuestos a que se refieren los dos apartados anteriores, cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos.*
> *4. Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos».*

.

Estos datos suelen obtenerse a través de distintos procedimientos:

- Ficheros con datos obtenidos de registros y fuentes accesibles al público, habitualmente a partir de resoluciones judiciales publicadas en diarios y boletines oficiales.

  Las principales fuentes de obtención de estos datos son diarios y boletines oficiales en los que se publican edictos de órganos judiciales o de otras administraciones públicas relacionadas con el cobro de sanciones económicas, embargos o subastas, entre otras informaciones.

- Informaciones facilitadas o consentidas por el interesado. Estos ficheros son los denominados de información positiva puesto que permiten conocer informaciones de los que podemos llamar buenos pagadores que, con su consentimiento, posibilitan que se utilice dicha información.

Entre los datos que suelen incluirse pueden citarse informaciones sobre los créditos contraídos y otros datos bancarios o similares.

Es preciso insistir en que la posibilidad de incluir datos se basa en el consentimiento del interesado por lo que éste puede revocarlo en cualquier momento, así como ejercer los derechos de acceso, rectificación, cancelación u oposición.

- Tratamiento de datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés.

Por otra parte, se fijan requisitos para poder tratar este tipo de datos:

- Debe existir una deuda previa, vencida, exigible e impagada.

¡ El acreedor que comunica esta información a un fichero de solvencia debe demostrar que existía una deuda anterior al momento de la comunicación y que el plazo para pagarla ha vencido sin que el deudor haya abonado la cantidad correspondiente. Si no se dan todas estas circunstancias no puede anotarse la morosidad en ningún fichero de información sobre solvencia. !

- Antes de la inclusión en el fichero debe realizarse un requerimiento previo de pago advirtiendo que si no se paga se procederá a la inclusión en estos ficheros. Esta información debe facilitarse también al celebrar cualquier contrato para la adquisición de productos, la contratación del servicio o la contracción de una deuda hipotecaria o un préstamo personal, cuyo incumplimiento pueda dar lugar a la inclusión en un fichero de morosos.

- Cuando el responsable del fichero de información sobre solvencia reciba la comunicación del acreedor e incluya la información en el fichero, debe dirigirse al deudor y notificarle la inclusión de los datos. En la notificación le informará sobre sus derechos de acceso, rectificación, cancelación y oposición. Para ello dispone de un plazo máximo de treinta días.

¡ La notificación obligatoria por el gestor del fichero sobre solvencia garantiza que podamos conocer quien nos ha incluido y porqué así como corregir errores o solicitar la cancelación de

los datos si no procede si inclusión. Es obligación del acreedor probar la existencia de la deuda y conservar la documentación que lo acredite.

- Quién notifica la inclusión de la deuda debe acreditar que efectivamente se ha realizado el envío. Cumplirá con su obligación cuando el destinatario rechace el envío y/o o cuando la dirija a la dirección que figure en el contrato.

¡ Es muy importante que mantengamos nuestra dirección actualizada en el caso que hayamos contraído obligaciones susceptibles de ser notificadas en caso de incumplimiento pues si se nos notifica al domicilio del contrato y no es el correcto, no sabremos que estamos en un fichero de morosos. !

- La información sobre solvencia puede ser consultada en tres casos, cuando el afectado:

  - Mantenga algún tipo de relación contractual que aún no se encuentre vencida.
  - Pretenda celebrar un contrato que implique el pago aplazado del precio.
  - Pretenda contratar la prestación de un servicio de facturación periódica.

- En el caso de la solvencia patrimonial suelen intervenir cuatro tipos de sujetos: 1) el deudor; 2) el acreedor que notifica la deuda; 3) el fichero común que sirve información sobre solvencia patrimonial; y 4) las entidades que consultan esta información. Por ello se ha diseñado un sistema que permita acceder siempre a su información con independencia de con quién mantenga su relación.

  - Si se dirige a una entidad que consultó la información ésta le indicará todos los datos relativos al mismo a los que ella pueda acceder y los la identidad y dirección del titular del fichero consultado para que pueda dirigirse ante él.

  - Si se dirige al titular del fichero común, esto es a quién informa sobre su solvencia, éste deberá comunicarle los datos que figuran en el fichero y las evaluaciones y apreciaciones que sobre el afectado se hayan comunicado en los últimos seis meses junto con el nombre y dirección de los destinatarios de las mismas.

Si en este caso se trata de rectificar o cancelar un dato, el titular del fichero común debe trasladar dicha solicitud a la entidad que haya facilitado los datos, para que ésta la resuelva. En el caso de que el responsable del fichero común no haya recibido contestación por parte de la entidad en el plazo de siete días, procederá a la rectificación o cancelación cautelar de los mismos.

Si la rectificación o cancelación se solicita a una entidad que ha consultado el fichero ella no podrá tramitarla pero deberá informar en el plazo de diez días facilitándole la identidad de quien gestiona el fichero común, para que pueda ejercer sus derechos ante él.

- Si se presenta una solicitud de rectificación o cancelación a quien haya facilitado los datos al fichero común procederá a la rectificación o cancelación de los mismos en sus ficheros y a notificarlo al titular del fichero común en el plazo de diez días, dando asimismo respuesta al interesado siguiendo el procedimiento general antes examinado.

Si no estima la reclamación deberá contestarle en todo caso. De no contestarle o denegar su solicitud puede solicitar gratuitamente la tutela de su derecho por la AEPD.

- Es fundamental garantizar la calidad, certeza y actualización de los datos sobre solvencia. Por ello:

- Los datos deberán ser cancelados cuando se hubieran cumplido seis años contados a partir del vencimiento de la obligación incumplida o del plazo concreto si aquélla fuera de vencimiento periódico. (por ejemplo las cuotas sucesivas de una hipoteca).

- Sólo podrán ser objeto de tratamiento los datos que respondan con veracidad a la situación de la deuda en cada momento concreto.

- El pago de la deuda determinará la cancelación de todo dato relativo a la misma, sin que pueda mantenerse información de que fué deudor en el pasado aunque ya pagó.

Finalmente, debe tenerse en cuenta que, en muchas ocasiones, los acreedores contratan el cobro de las deudas con terceras empresas especializadas. Si recibe una comunicación por parte de una de estas empresas de recobro, debe analizarse con detalle quien es el verdadero acreedor, pudiendo actuar conforme se ha indicado anteriormente.

Tanto si el que reclama el pago es el acreedor, como si lo hace una tercera empresa contratada, para obtener el cobro no pueden facilitar información a terceros distintos del deudor. Si facilitan información sobre morosidad a los vecinos, familiares, al lugar de trabajo o a cualquier tercero incumplen una obligación de secreto que puede ser sancionada.

RECUERDA QUE ...

- Cuando un responsable de un fichero o tratamiento, una empresa, una administración, una página web, solicita y recoge tus datos debe informarte adecuadamente. No olvides nunca leer esta información y muy especialmente las políticas de privacidad en Internet.

- Tienes la capacidad de consentir respecto del tratamiento de tus datos. Cuando dicho tratamiento sea obligatorio debes recibir información que precise ese carácter.

- Los responsables de ficheros y tratamientos deben tratar adecuadamente los datos personales garantizando entre otros principios que los datos se encuentren actualizados, que se utilicen sólo para las finalidades para los que fueron recogidos, así como la seguridad y el secreto.

- Puedes saber qué organizaciones han inscrito sus ficheros y los datos básicos sobre los mismos ante el Registro General de Protección de Datos.

- Para controlar los tratamientos sobre tu información puedes ejercer los derechos de acceso, rectificación, cancelación y oposición al tratamiento. Si estos derechos no son respetados puedes solicitar la tutela de la Agencia Española de Protección de Datos.

- La primera garantía para la protección de tu derecho fundamental a la protección de datos depende de tu propia conducta. Si facilitas datos personales sin leer previamente la información sobre privacidad, si no aprendes a configurar tu perfil en una red social, si expones información personal en Internet, te expones a riesgos.

- Debes respetar el derecho fundamental a la protección de datos de los demás y no publicar o tratar su información personal sin su consentimiento.

- Los niños son especialmente vulnerables respecto del tratamiento de sus datos. Es necesario formarles adecuadamente para que aprendan a proteger su privacidad y nunca debe confiarse en quienes no cumplan de modo riguroso con las normas específicas aplicables a los menores.

- En las redes sociales nuestra privacidad se encuentra particularmente expuesta debemos comprobar las condiciones de uso de cada red, aprender a configurar nuestro perfil y a actuar respetando los derechos de los demás.

- La información sobre solvencia es fundamental para el funcionamiento de la economía y para garantizar nuestra capacidad para contratar bienes y servicios. Por ello, debemos ser muy diligentes y asegurarnos al contratar que se garantizan nuestros derechos.

RECURSOS Y PUBLICACIONES DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Te recomendamos visitar en nuestra página web http://www.agpd.es/ las siguientes secciones:

CANAL DEL CIUDADANO

Aquí se encuentra una completa información sobre los derechos de acceso, rectificación, cancelación y oposición con formularios y documentación que ayuda. Además, desde ella puede accederse a servicios de atención al ciudadano, consultas y sugerencias.

SECCIÓN DESTINADA A LOS MENORES

La Agencia Española de Protección de Datos, en su compromiso con la protección de los datos personales de los menores, ha creado esta sección web en la que se ofrecen recursos y materiales informativos destinados tanto a niños como a padres, tutores y miembros de la comunidad académica interesados en profundizar en el derecho fundamental a la protección de datos de una forma sencilla y educativa.

Para ello se han recopilado materiales divulgativos propios y enlaces a webs en las que se puede encontrar más información y otros recursos de interés.

CONSULTA DE FICHEROS INSCRITOS

El objetivo de esta sección es difundir y dar publicidad a la existencia de ficheros con datos de carácter personal inscritos en el RGPD. La información se actualiza diariamente, por lo que los ficheros aparecerán al día siguiente de su inscripción en el Registro General de Protección de Datos.

El derecho de consulta al Registro, regulado en el artículo 14 de la LOPD habilita a cualquier persona para conocer, de forma pública y gratuita, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del fichero.

GUÍA SOBRE EL DERECHO A LA PROTECCIÓN DE DATOS DE LOS NIÑOS Y NIÑAS Y LOS DEBERES DE PADRES Y MADRES.

Esta publicación contiene información sobre aspectos básicos que deben ser conocidos por los menores para proteger su información personal. Resulta particularmente útil para que los niños aprendan a comportarse en Internet. Por otra parte contiene un decálogo de consejos útiles para padres y madres.

RECOMENDACIONES A USUARIOS DE INTERNET.

Aquí pueden encontrarse un conjunto de recomendaciones que nos ayudan a saber como controlar nuestra información en internet y cómo tratar la información perteneciente a otras personas.

ESTUDIO SOBRE LA PRIVACIDAD DE LOS DATOS PERSONALES Y LA SEGURIDAD DE LA INFORMACIÓN EN LAS REDES SOCIALES ONLINE.

Se trata de un completo estudio que permite conocer a fondo el funcionamiento de las redes sociales y sus implicaciones en el derecho a la protección de datos.

www.agpd.es