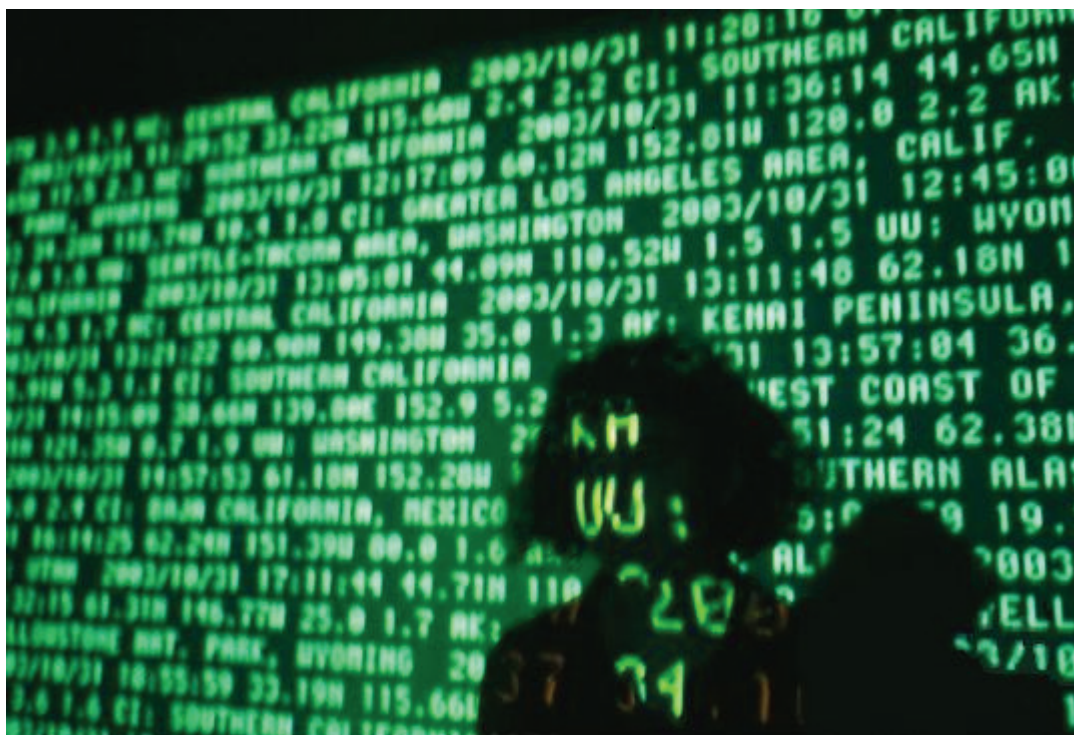




Instituto Nacional
de Tecnologías
de la Comunicación

Guías Legales

PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL



OBSERVATORIO DE LA SEGURIDAD DE LA INFORMACIÓN

Área Jurídica de la Seguridad y las TIC

¿Qué son los datos de carácter personal y quién debe cumplir la normativa?

Según lo dispuesto en el art. 3 a) de la Ley Orgánica 15/1999 de Protección de Datos, es considerado **Dato de carácter personal** “cualquier información concerniente a personas físicas identificadas o identificables”, otorgando protección tanto a los datos de personas claramente identificadas, como a los de aquellas que a pesar de no estarlo, podrían llegar a identificarse a partir de los datos con los que se cuenta.

A modo ejemplificativo, serán considerados datos de carácter personal el nombre, los apellidos, la dirección postal e incluso la dirección de correo electrónico, así como el número de teléfono fijo, móvil, la matrícula de un vehículo, la dirección IP con la que se navega por Internet, el ADN, cualquier tipo de imagen de una persona física..., **en definitiva, cualquier dato de carácter personal que identifique o pueda identificar a una persona.**



Todas las cuestiones relativas a la Protección de Datos de Carácter Personal se encuentran reguladas en la **Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD)** y el **Reglamento de Medidas de Seguridad RD 994/1999 (RMS)**, así como en las Instrucciones de la Agencia Española de Protección de Datos y demás resoluciones publicadas por ésta.

La normativa mencionada es aplicable exclusivamente a los datos de carácter personal de personas físicas y de obligado cumplimiento para toda empresa o Administración Pública, que trate datos de carácter personal.

¿Por qué es tan importante su protección?

La protección de los datos de carácter personal es un **derecho fundamental** que encuentra su origen normativo en los artículos **10 y 18.4 de la Constitución Española** que otorgan a las personas físicas el **derecho a la intimidad**, y establecen 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.”

Observando el día a día de cualquier persona, **constantemente estamos facilitando datos de carácter personal a empresas privadas y administraciones públicas**, ya sea para abrir una cuenta bancaria, para obtener una tarjeta de descuento en nuestro restaurante habitual o para solicitar una licencia de obras a nuestro Ayuntamiento. Esto implica en la mayoría de los casos que perdamos el rastro de nuestros datos y de las finalidades para las que originariamente fueron facilitados, implicando la pérdida de control sobre los mismos.

La protección de datos es un derecho fundamental

La constante evolución de las nuevas tecnologías, conlleva inevitablemente que toda la información se encuentre digitalizada, por lo que su tráfico, incluso a nivel global resulta mucho más sencillo. Los gobiernos nacionales y en especial la Unión Europea, han iniciado acciones conjuntas de cara a evitar, o en su caso frenar, el intercambio descontrolado y no autorizado de base de datos digitalizadas que contengan datos de carácter personal.

Principios básicos de la Normativa

La normativa de protección parte de una serie de principios básicos dispuestos en los artículos 4, 5 y 6 de la LOPD que pueden resumirse en la obligación por parte de los Responsables de Fichero a que todas sus bases de datos deben cumplir con el **principio de calidad** de los datos, con el **deber de información** a los afectados¹, así como respecto a la **regulación**, legítima y no, **del tratamiento**² que se lleve a cabo de dichos datos personales.

Es esencial que te informen antes de recabar los datos

El Principio de Calidad de los datos, tiene como finalidad primordial evitar que se proceda a recopilar datos de forma masiva, sin ser

¹ Afectado o interesado: “persona física titular de los datos que sean objeto del tratamiento.”(Art.3 e) LOPD)

² Tratamiento de datos: “operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias”. (Art. 3 c) LOPD)

estrictamente necesario para la finalidad originaria y que se aparte de la misma, destinándose a otras finalidades. Del mismo modo, es estrictamente obligatorio cancelar (borrar) dicha base de datos, una vez haya desaparecido la finalidad para la cual fueron recabados y para la que el afectado prestó el consentimiento³ inicialmente.

A modo de ejemplo, dicho principio impediría a un empresario utilizar la base de datos de sus empleados para realizar una campaña comercial de un nuevo producto, o que un médico utilizara su base de datos de pacientes para realizar una prospección comercial de un producto farmacéutico concreto. Todo ello viene justificado por el hecho de que inicialmente la base de datos no fue creada con dicha finalidad, ni el consentimiento inicial se prestó para ello.

Por otro lado, el principio de deber de información en la recogida de los datos, obliga al Responsable del Fichero⁴, de forma previa a la recogida de los datos, a informar al titular respecto a:

La **existencia de un fichero**⁵ en el que se tratan datos de carácter personal, de la **finalidad** de la recogida de éstos y de los **destinatarios** de la información.

El **carácter obligatorio o facultativo** de las respuestas a los apartados del formulario.

Las **consecuencias** de la obtención de los datos o de la negativa a suministrarlos.

La **posibilidad de ejercer los derechos** de acceso, rectificación, cancelación y oposición.



Los **datos de la entidad** que recaba los datos o, en su caso, de su representante.

En tal caso, es necesario que todos estemos atentos y la entidad que trata los datos personales incluya en la parte inferior o en cualquier otro lugar fácilmente visible una

³ Consentimiento del interesado: *“toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.”* (Art. 3 h LOPD)

⁴ Responsable del fichero o tratamiento: *“persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.”* (Art. 3 d LOPD)

⁵ Fichero: *“todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.”*

pequeña cláusula con la información indicada⁶. En caso contrario, estará incumpliendo con lo dispuesto en el artículo 5 de la LOPD.

No obstante, existen excepciones a dicho requisito. Son:

Cuando expresamente una ley así lo prevea.

Cuando el tratamiento tenga fines históricos, estadísticos o científicos.

Cuando proporcionar la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia Española de Protección de Datos o del Organismo Autónomo equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

Cuando los datos procedan de fuentes accesibles al público⁷ y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del **origen** de los datos y de la **identidad del Responsable** del Tratamiento así como de los **derechos** que le asisten.

Por último, el tercer principio básico, es el relativo al **Tratamiento de los datos** que regula la obligación, de manera previa al tratamiento, del deber de prestar por parte del afectado el consentimiento inequívoco, cuestión analizada a fondo en el siguiente epígrafe.

⁶ Ejemplo de aviso LOPD “En cumplimiento de lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal le informamos que sus datos personales quedarán incorporados y serán tratados en los ficheros automatizados de NOMBRE_EMPRESA, con el fin de indicar la finalidad concreta. Le informamos de la posibilidad de que ejerza los derechos de acceso, rectificación, cancelación y oposición de sus datos de carácter personal solicitándolo por escrito y junto a una copia de su DNI dirigida al Responsable del Fichero.”

⁷ 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.*” Art.3 j LOPD

¿Qué implica el consentimiento respecto al tratamiento de los datos?

Uno de los ejes fundamentales en la protección de datos es el **consentimiento de los afectados**. Dicho consentimiento debe ser prestado **siempre antes de facilitar nuestros datos** al Responsable del Fichero para que proceda a su tratamiento, garantizando así que el titular conoce la finalidad, sus derechos, así como los datos del Responsable del Fichero.

La regla general establecida por la ley es la de solicitar a los titulares de los datos el “**consentimiento, libre, específico, informado e inequívoco**”. Más concretamente, cada uno de estos requisitos implica:⁸

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

Específico, es decir referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del Responsable del Tratamiento, tal y como establece el artículo 4.2 de la Ley Orgánica 15/1999.

Informado, es decir, que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que se lleva a cabo.

Precisamente por ello el artículo 5.1 de la Ley Orgánica impone el deber de informar a los interesados de una serie de extremos que en el mismo se contienen.

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

Por tanto, nunca nos podrán solicitar el consentimiento para tratar nuestros datos personales, de forma que no conozcamos con qué **finalidad** son tratados, cuál es la **forma de ejercicio de nuestros derechos, quién es el Responsable** del Fichero o

Salvo
disposición en
contrario, el
consentimiento
siempre
deberá ser
inequívoco

⁸ Información obtenida de “*Caracteres del consentimiento definido por la LOPD (nivel 4)*”

que no se derive claramente de nuestros actos que deseábamos prestar el consentimiento.

Otra de las características principales del consentimiento y que según lo dispuesto en el art. 6 de la LOPD debe cumplirse "salvo disposición en contrario" es el hecho de que **la aceptación por parte del afectado debe ser inequívoca, expresa o tácita,**



pero siempre una aceptación inequívoca. No obstante para que ese consentimiento tácito pueda ser considerado inequívoco será preciso otorgar al afectado un plazo prudencial para que pueda claramente tener conocimiento de que su omisión de oponerse al tratamiento implica un consentimiento al mismo.⁹

Es esencial conocer que tipo de datos se están solicitando, ya que dependiendo de esto **la forma de prestar el consentimiento puede variar.** A continuación se indican una serie de datos personales respecto a los que el consentimiento debe cumplir una serie de características especiales:

Consentimiento expreso y por escrito: En caso de que los datos solicitados sean relativos a la ideología, afiliación sindical, religión y creencias.¹⁰

Consentimiento expreso: Los datos de carácter personal relativos al origen racial, a la salud y a la vida sexual exclusivamente podrán ser tratados, cedidos y recabados cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

No obstante, existen **excepciones relativas a la prestación del consentimiento.** Exclusivamente podrán recabarse datos personales sin mediar consentimiento en caso de que:

Sean datos recabados por las Administraciones Públicas para el ejercicio de sus funciones y dentro 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.

⁹ Información obtenida de "Caracteres del consentimiento definido por la LOPD (nivel 4)"

¹⁰ Se exceptúan los ficheros mantenidos por 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.

Cuando el tratamiento de los datos **tenga por finalidad proteger un interés vital del interesado** (tales como la vida o la integridad física).

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 tercero a quien se comuniquen los datos.

¿Qué derechos tengo sobre mis datos de carácter personal?

Como hemos indicado anteriormente, toda persona física dispone de una serie de derechos respecto a sus datos de carácter personal. Son cuatro los derechos que prevé la normativa vigente:

Derecho de Acceso: Habilita al titular a solicitar información respecto a qué datos personales tiene el Responsable del Fichero y cómo han sido obtenidos.

Derecho de Rectificación: Derecho a solicitar al Responsable del Fichero que varíe alguno de nuestros datos personales de que disponga.

Derecho de Cancelación: Derecho a solicitar que todos aquellos datos de que disponga el Responsable del fichero sean cancelados, o en su caso bloqueados.

El derecho de cancelación tiene particularidades por el hecho de que **la cancelación no es directa e inmediata**, sino que la solicitud dará lugar en una primera **fase al “bloqueo” de los datos**, conservándose únicamente a disposición de las

Administraciones Públicas o Jueces y Tribunales, para poder disponer de éstos en caso de responsabilidades nacidas de ellos, y en todo caso durante el plazo de prescripción de dichas acciones. Cumplido el plazo deberá procederse a la supresión de los datos.

Por ello, como titulares de los datos, y especialmente respecto a determinados datos de carácter personal (salud, etc.) **no podemos esperar que nuestros datos sean directamente cancelados**, sino que quedarán en poder del Responsable del Fichero, aunque con su acceso bloqueado, en tanto exista alguna posibilidad de requerirse



judicialmente o por parte de la Administración Pública durante el plazo que marque la Ley.

Derecho de Oposición: Derecho a solicitar que nuestros datos personales no sean tratados con una finalidad concreta, sin que ello suponga la eliminación de la base de datos.

El **ejercicio de cualquiera de estos derechos es personalísimo**, y debe, ser ejercido directamente por el afectado (titular de los datos de carácter personal) ante el Responsable del Fichero.

¿Cómo puedo ejercitar mis derechos?

El ejercicio de los derechos **no requiere de ningún formalismo concreto**, sino que basta con remitir, por cualquier medio, la solicitud de ejercicio del mismo.¹¹

El único requisito adicional que puede exigirse es que la solicitud vaya acompañada de una copia del DNI del titular de los datos, de forma que el Responsable del Fichero pueda corroborar la identidad del solicitante, cumpliendo así con el principio de calidad de datos.

El ejercicio de derechos encuentra como particularidad los plazos de que dispone el Responsable de Tratamiento para atender las solicitudes:

Derecho de Acceso: El Responsable del Fichero dispone de **30 días**, desde la recepción de la solicitud, para atenderla. No obstante, el ejercicio del derecho de acceso ha sido limitado a **una vez cada 12 meses**, salvo interés legítimo, evitando así el abuso por parte de los usuarios.

El ejercicio de los derechos debe ser siempre, sencillo y gratuito

Derecho de Rectificación: El Responsable del Fichero dispone de un plazo de **10 días** para contestar la solicitud de ejercicio.

Derecho de Cancelación: El Responsable del Fichero dispone de un plazo de **10 días** para contestar a la solicitud de ejercicio.

¹¹ Se recomienda que el ejercicio de los derechos sea llevado a cabo mediante un medio que permita la demostración posterior.

Derecho de Oposición: En lo relativo a los plazos de ejercicio del derecho de oposición, aún no se encuentra regulado reglamentariamente, tal y como indica la LOPD. No obstante, el ejercicio del derecho de oposición deberá llevarse a cabo conforme al mismo procedimiento indicado al inicio del apartado.

Si el Responsable del Fichero no cumpliera con los plazos, puede denunciar a la Agencia Española de Protección de Datos (www.agpd.es), incluyendo toda la documentación relativa a la solicitud realizada al Responsable del Fichero.

Otros derechos de Interés

Además de los derechos anteriormente indicados, existen otro tipo de derechos que causan dudas muy frecuentes entre los usuarios. A continuación se indican los casos más comunes

Borrado de los listines telefónicos.

Es frecuente que algunas personas, decidan que su número de teléfono fijo no aparezca en los listines telefónicos de las compañías de telecomunicaciones, considerados a los efectos de la normativa de protección de datos, Fuentes Accesibles al Público.

En estos casos, la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal habilita a los titulares de la línea telefónica a solicitar que sus datos personales (nombre, apellidos, dirección postal y teléfono) no aparezcan reflejados en el listín, evitando así que sus datos puedan ser recabados sin consentimiento previo.



Para ejercer este derecho, previsto en la ley, basta con que lo solicitemos por escrito junto a una fotocopia de nuestro DNI (siguiendo el procedimiento general) solicitando que se proceda a la exclusión total o parcial.

En caso de que se solicite el ejercicio de dicho derecho, la empresa editora del listín deberá cumplirlo en la **siguiente edición (formato papel)** y en **10 días**, en el caso de las **ediciones electrónicas**.

Derecho a no recibir comunicaciones comerciales.

Es frecuente que recibamos publicidad y comunicaciones de carácter comercial en nuestros buzones físicos y en nuestras cuentas de correo electrónico, lo que supone

una gran molestia y un gasto económico importante en relación al ancho de banda empleado a la hora de descargarlos y el tiempo para eliminarlos.

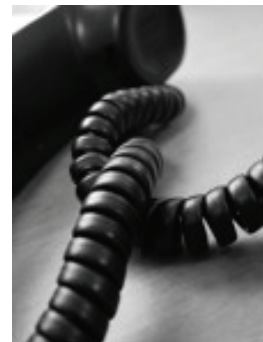
Atendiendo a la normativa aplicable, (Art. 30 de la LOPD y Art. 19 y ss de la LSSI-CE) hay que tener en cuenta que sólo debemos recibir información comercial siempre que hayamos prestado nuestro consentimiento a recibir comunicaciones comerciales, o en su caso nuestros datos hayan sido recabados de fuentes accesibles al público.

En caso de que la comunicación comercial hubiera sido realizada obteniendo los datos desde fuentes accesible al público, dicha comunicación deberá contener los **datos identificativos del Responsable**, de **qué fuente accesible al público han sido obtenidos** los datos, así como los **derechos** de acceso, rectificación, cancelación y oposición que ostenta respecto a los mismos.

En relación a servicios de Telecomunicaciones.

En este caso, el derecho nace de la normativa de Telecomunicaciones. Concretamente la Ley 32/2003, General de Telecomunicaciones, en su artículo 33 establece que **todo abonado** a un operador de servicios de comunicación electrónica (teléfono, Internet, etc.) **tiene derecho a que sus datos de tráfico sean cancelados siempre y cuando no sean necesarios para transmitir la comunicación ordenada por el usuario.**

Por otro lado, **nuestros datos de tráfico o personales, no pueden ser utilizados para ofrecernos servicios adicionales o con fines comerciales** por parte de los operadores de telecomunicaciones, salvo que hayamos prestado consentimiento expreso para ello.



¿Qué es lo más importante que debo saber sobre la protección de datos?

Siempre debemos **ser informados de forma previa** respecto a cuál es la finalidad para la que se recaban nuestros datos de carácter personal, quién será el Responsable del Tratamiento y cuáles son los derechos de que disponemos.

Para el **tratamiento de datos de nivel alto** (salud, origen racial, sindicales, etc.) se nos debe solicitar el **consentimiento expreso o en su caso expreso y por escrito**, según proceda.

Los ficheros en el que albergan nuestros datos de carácter personal **se deben encontrar completamente actualizados**, cumpliendo así con el principio de calidad y es necesario que una vez terminada la finalidad concreta para la que se recabaron, sean destruidos de forma segura.

Para ejercer los derechos, basta con que rellenemos el modelo disponible en el sitio Web de la AEPD (www.agpd.es) acompañado **de una copia de nuestro DNI**,. En todo caso deberá **ser gratuito y sencillo**, entendiéndose como tal, que el envío de un FAX no incumple con el requisito de gratuidad.

En caso del ejercicio de los derechos (acceso, oposición, cancelación y rectificación) es necesario **que el Responsable del Fichero cumpla con los plazos establecidos**. En caso contrario remitiremos denuncia a la Agencia Española de Protección de Datos mediante el formulario disponible en la Agencia Española de Protección de Datos.

Para ampliar la información relativa a la normativa, competencias, derechos y posibles acciones para la defensa de los mismos, le recomendamos que se ponga en contacto con la **Agencia Española de Protección de Datos** en la siguiente dirección:

C/ Jorge Juan, 6

28001-Madrid

Telf.: 901 100 099 / www.agpd.es

Casos prácticos...

A continuación se describe una serie de casos desde un punto de vista completamente práctico. La intención última es acercar al lector situaciones cotidianas previstas por la normativa de protección de datos de carácter personal.

Caso 1:

Beatriz casi diariamente al recoger su correspondencia en el buzón se encuentra, por un lado, gran cantidad de publicidad, y por otro, correspondencia directamente dirigida a su nombre con información publicitaria relativa a diversos productos y servicios de empresas que desconoce.

Beatriz no entiende porqué le remiten esta información y se pregunta **¿cómo puede evitarlo? y ¿hasta qué punto esa actuación es legal?**

El caso de Beatriz es un ejemplo más de la situación que viven muchos ciudadanos diariamente, sintiéndose desbordados por la cantidad de información publicitaria que reciben por parte de las empresas, en especial, durante las épocas de campañas publicitarias destinadas a captar un mayor número de clientes posibles.

Para responder a la duda de si la actuación llevada a cabo por estas empresas es legal o no, se debe distinguir, en primer lugar, entre el supuesto de publicidad genérica (buzoneo) y la publicidad dirigida directamente a nombre de Beatriz.

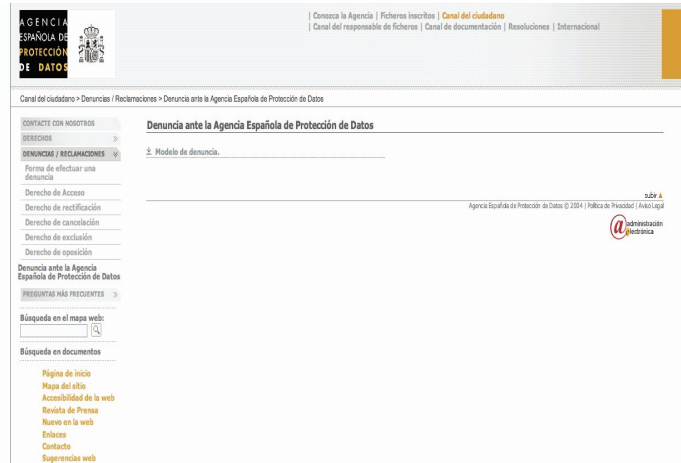


El primer caso, el conocido como “buzoneo”, es perfectamente legal desde el punto de vista de la protección de datos, ya que las empresas no tratan datos de carácter personal para llevarlo a cabo, sino que simplemente se limitan a depositar publicidad en los buzones.

En el segundo caso, la cuestión es diferente. La empresa que dirige la publicidad a Beatriz dispone de un fichero en el que se contienen los datos personales de todas las personas que van a recibir la publicidad, por lo que debe analizarse si dicho fichero y las comunicaciones comerciales cumplen con los requisitos establecidos en la normativa vigente, especialmente respecto a lo dispuesto en los arts. 5, 6 y 30 de la LOPD.

La empresa puede disponer de los datos de Beatriz por varios motivos:

En primer lugar, porque Beatriz se los haya facilitado en algún momento anterior mediante un formulario web, formulario en papel, entrevista; u otra vía de similar naturaleza. En todo caso, esta recogida de datos deberá haberse realizado cumpliendo con la obligación de informar al afectado respecto a: los datos del Responsable del Fichero, la finalidad para la que serán destinados esos datos y los derechos de que dispone el afectado, entre otros. De no haberse atendido esta obligación, Beatriz podrá formular la denuncia o reclamación pertinente. Para ello puede visitar la página www.agpd.es y descargar el formulario de denuncia que figura disponible en la sección “Denuncias/Reclamaciones” y seguir las recomendaciones allí indicadas.



Es necesario comprobar si el consentimiento prestado por Beatriz era inequívoco, o si de sus actos no puede derivarse que el consentimiento fue prestado para realizar comunicaciones comerciales. En tal caso, cabe destacar que el consentimiento inequívoco no implica que deba ser expreso, o por escrito, sino que resulta suficiente que de los hechos se derive inequívocamente que Beatriz presta su consentimiento. En caso de que no haya sido así, Beatriz podrá seguir los pasos anteriormente indicados para iniciar la denuncia ante la AEPD.

En segundo lugar, existe la posibilidad de que los datos de Beatriz hayan sido obtenidos, según lo dispuesto en el art. 30.2 LOPD, a partir de “Fuentes Accesibles al Público”.

En este caso, la empresa se encuentra legalmente habilitada para realizar la comunicación comercial sin consentimiento de Beatriz. No obstante, aún ésta tendrá la posibilidad de comprobar que realmente se cumple plenamente con la legislación.

En este sentido, se recomienda que Beatriz compruebe la comunicación comercial para detectar si en ella figuran los datos del responsable del envío, los derechos que le asisten, y la fuente accesible al público de la que fueron recabados. Si alguno de estos datos no figurase, Beatriz podrá denunciar ante la AEPD.

Finalmente, y aunque la empresa emisora haya cumplido con todos los requisitos legales en vigor, Beatriz siempre tendrá la posibilidad de ejercer sus derechos de acceso, rectificación, cancelación y oposición frente al Responsable del Fichero. Así mismo, es recomendable que remita por escrito su deseo inequívoco de que el Responsable del Fichero cancele sus datos, siendo desde dicho momento gravemente penado el hecho de que la misma empresa le remita nuevamente información comercial.

Por último conviene recordar que Beatriz puede acudir a la página www.agpd.es para descargar los formularios de ejercicio de derechos disponibles en la sección de “Denuncias / Reclamaciones”.

Caso 2:

Un profesional independiente (abogado, procurador, etc.) que trabaje por cuenta propia, está obligado a cumplir la legislación de protección de datos. En ese caso, ¿qué procedimiento debería seguir para cumplir con los requisitos mínimos?.



Efectivamente debe cumplir la normativa de protección de datos, ya que trata datos de carácter personal de sus clientes.

En cuanto a la obligatoriedad del nivel de requisitos que debe cumplir, al menos atenderá la obligación de información a sus clientes cada vez que recabe datos de éstos, mediante la utilización de la cláusula tipo anteriormente indicada en la que se informe de los datos del Responsable del Fichero, de la finalidad para la que son recabados los datos, e informar a éstos a su vez de los derechos que les corresponden, y en cualquier caso, solicitar el consentimiento inequívoco para el tratamiento de los datos, cumpliendo de esta forma con los arts. 5 y 6 de la LOPD.

De igual modo, y como entidad privada que trata datos de carácter personal con una finalidad concreta, el Responsable de Fichero deberá someterse a una auditoría de protección de datos que garantice el cumplimiento de todas las obligaciones dispuestas en la LOPD y en el Reglamento de Medidas de Seguridad (RMS), en especial, en lo que respecta a disponer del Documento de Medidas de Seguridad y las relaciones contractuales con los posibles Encargados de Tratamiento que pudieran tratar datos de carácter personal, así como proceder a la notificación de todos los ficheros con datos de carácter personal a la AEPD, mediante el programa NOTA de la

AEPD al que podrá acceder a través de la página web de la propia Agencia, en la sección del Responsable del Fichero.

Caso 3:

Marta, con cierta frecuencia, recibe correos electrónicos “de tipo cadena” en los que aparecen numerosas direcciones de correo electrónico dentro del propio mensaje, que pertenecen a todas las personas a las que fueron enviados previamente.

Marta se cuestiona, por un lado, si es legal que aparezca a la vista de todos los receptores esas direcciones de correo y, por otro lado, qué podría hacer para no incurrir en ninguna ilegalidad.

Recientemente, la Agencia Española de Protección de Datos ha condenado a una persona que envió un correo electrónico “de tipo cadena” sin utilizar la opción de “Con copia oculta”, de forma que quedaron visibles todas las direcciones de correo electrónico de las personas que lo habían recibido inicialmente.

El primer aspecto que debemos tener en cuenta es el Informe de 1999 de la AEPD, el cual deja claro que dentro de la definición de dato de carácter personal también se encuentran las direcciones de correo electrónico, ahora bien, siempre que identifiquen o hagan identificable a su titular.



La AEPD entiende de forma directa que las direcciones de correo que tengan el formato “[nombre@proveedor.com](#)” o que muestren cualquier otro dato identificativo del titular antes de la @, son direcciones de correo electrónico dignas de protección desde el punto de vista de la protección de datos.

La AEPD llega más lejos al establecer que incluso las direcciones que aparentemente no tengan ningún elemento identificativo del titular podrían llegar a ser también un dato de carácter personal. Estos supuestos son aquellos en los cuales la dirección de correo electrónico aparezca necesariamente referenciada a un dominio concreto, de tal forma que será posible proceder a la identificación del titular mediante la consulta del servidor en el que se gestione dicho dominio, sin que ello pueda considerarse que

lleve aparejado un esfuerzo desproporcionado por parte de quien procede a la identificación.¹²

Por todo lo anterior, siempre que se vaya a realizar un reenvío de algún correo electrónico en cadena es recomendable borrar todas las direcciones de correo de los remitentes e incluirlas en el apartado “CCo” lo que implica que dicho correo será enviado a todas las direcciones ahí incluidas pero sin resultar visibles por parte de terceros, garantizando de esta forma, la privacidad y la protección de los datos (e-mail) de los remitentes.

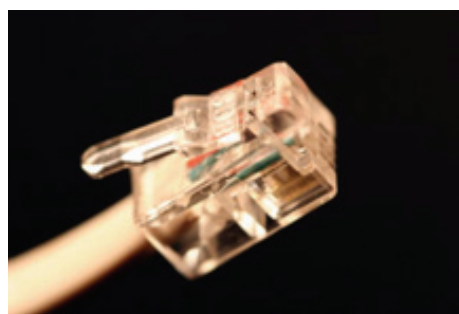
Curiosidades...

Se expone a continuación el análisis de una serie de resoluciones e informes de la Agencia Española de Protección de Datos (AEPD) que han analizado y despejado cuestiones dudosas.

El análisis de casos concretos ayuda con frecuencia a esclarecer aspectos prácticos que desde el punto de vista de la normativa de protección de datos pueden no resultar totalmente claros tras un primer análisis de la normativa.

La dirección IP: ¿Se considera datos de Carácter Personal?

Las direcciones **IP** o **Internet Protocol** es el conjunto de números que identifican de manera lógica y jerárquica un equipo en Internet; ya sea un ordenador o cualquier otro dispositivo capaz de conectarse a Internet.



La dirección IP con la que un equipo navega por Internet, es única en el momento de la navegación y ningún otro equipo puede estar navegando con la misma dirección, es por esto que cabría identificarla como **la “matrícula” del equipo en Internet.**¹³

¹² Texto extraído del Informe de la AEPD relativo a si las direcciones de correo electrónico son datos de carácter personal.

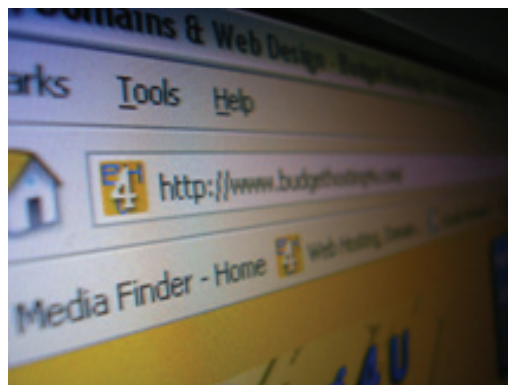
¹³ Hay que tener en cuenta que las direcciones IP pueden ser dinámicas o estáticas dependiendo si el usuario accede siempre con la misma dirección, o si lo hace cada vez que se conecta con una diferente. No obstante, e independientemente de que lo haga con una modalidad o con otra, queda registrado en el archivo histórico del proveedor.

Si se parte del concepto de dato de carácter personal dispuesto en el artículo 3 a) de la LOPD se observa que el **dato de carácter personal es todo aquel dato que identifique o haga identificable a una persona física.**

La dirección IP por sí sola no hace identificable directamente a una persona física, sino que hace identificable a un equipo, y en su caso, a una conexión a Internet contratada a nombre de una persona en concreto, al menos inicialmente.

Todos los proveedores de acceso a Internet disponen de un fichero histórico¹⁴ en el que queda guardada la dirección IP asignada a cada uno de sus abonados en el momento concreto en el que se conectan, de igual manera los datos de tráfico, fecha, hora y otros de semejante naturaleza; de cara a poder facturar posteriormente los servicios.

Con todo ello, la Agencia Española de Protección de Datos, entendió en el Informe 327/2003 que siempre que medie la asistencia de terceras partes responsables de la asignación, se puede identificar a un usuario de Internet, esto es, obtener su identidad civil (nombre dirección, número de teléfono, etc) por medios razonables, de modo que **no cabe duda de que se puede hablar de datos de carácter personal en el sentido de la letra a) del artículo 3 de la Ley 15/1999.**



Internet: ¿Es una fuente accesible al público?

Existe una gran confusión en el sector empresarial y a nivel particular respecto a la definición de “Fuentes Accesibles al público” (concepto ya indicado en la nota al pie nº7 de la presente guía), y respecto a si Internet supone una fuente accesible al público o no.

¹⁴ Cabe destacar lo dispuesto en la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de Marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público a redes públicas de comunicaciones, y por la que se modifica la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de Julio, en la que se establece la obligación de todos los prestadores de servicios de comunicaciones electrónicas disponibles al público o que exploten redes públicas de comunicaciones, según lo dispuesto en la Ley 32/2003, General de Telecomunicaciones.

Son muchas las sanciones que ha impuesto la AEPD a empresas y particulares por entender que Internet era una fuente accesible al público y que por tanto podía tratar dichos datos sin autorización por parte de su titular.

La AEPD, se ha pronunciado estableciendo que “la inclusión voluntaria de dicha dirección de correo electrónico por aquél [...] no legitima la utilización de la misma por terceros para fines distintos de los expresamente señalados por el denunciante en cualquiera de las páginas en las que éste hubiera reflejado su dirección de correo electrónico, pues sólo el denunciante, como titular de sus datos personales, más concretamente, en este caso, de su dirección de correo electrónico, está legitimado, en los términos y con las excepciones establecidas en la LOPD, para decidir sobre el destino y uso de sus datos personales.”¹⁵

A partir de lo señalado, no es posible obtener direcciones de correo electrónico, o cualquier otro dato de carácter personal de Internet y tratarlo como si proviniera de una fuente accesible al público, sin consentimiento del titular.

El consentimiento del titular debe ser siempre previo y destinado a una finalidad concreta, no bastando, por ejemplo, que se preste el consentimiento en un sitio Web dedicado a mantener un directorio profesional concreto y finalmente pueda ser utilizado para cualquier otra finalidad como el envío de comunicaciones comerciales, etc.

Como la propia AEPD establece, “...la publicación en Internet de una dirección de correo electrónico por su titular no la convierte en un dato que pueda ser utilizado sin límite alguno por parte del responsable del fichero en el que se encuentren incluida.”

Si desea más información respecto a resoluciones de la AEPD, le recomendamos que visite www.agpd.es, en el apartado Procedimientos Sancionadores.

¹⁵ Texto de la propia resolución sancionadora de la AEPD.