Guía de Protección de Datos para Empresas

Índice

Sumario

Sumario

Sumario

Sumario

Sumario

Sumario

Sumario

¿EN QUÉ CONSISTE EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE LOS DATOS PERSONALES?

En nuestro ordenamiento jurídico, en la línea de lo establecido en la normativa comunitaria e internacional, se recoge y tutela el derecho a la protección de los datos personales. El que los datos personales deban ser protegidos significa que debe garantizarse en todo momento el poder de decisión y disposición sobre ellos a aquella persona que le son propios, al ser elementos que pertenecen a su vida privada. El derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos.

El artículo 18.4 de la Constitución española dispone que la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. Con ello incorpora una garantía de otros derechos, fundamentalmente el honor y la intimidad y es en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento de datos. El derecho de la libertad informática o autodeterminación informática permite el acceso, rectificación y cancelación de la información almacenada, disponiendo de los datos personales, de manera que la persona tiene derecho a controlar la veracidad y exactitud de sus datos, impidiendo la difusión de aquellos que sean sensibles o reservados y confirmando que se utilizan para los fines predeterminados. Así, al hablar de la protección de datos personales, hay que ser conscientes de que como derecho tiene dos proyecciones: una proyección del derecho como facultades del titular y otra proyección como límite a las actuaciones o ingerencias de terceros.

¿DÓNDE SE CONTIENE EL RÉGIMEN JURÍDICO GENERAL EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES?

Al mandato constitucional se da cumplimiento con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. El desarrollo de la Ley se encuentra, con carácter general, en el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos (modificado por Real Decreto 156/1996, de 2 de febrero), el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992 y el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal. Además, la remisión a la protección de datos personales está recogida en las disposiciones que, en los últimos tiempos, han venido a regular aspectos de la sociedad de la información: Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico y Ley 59/2003, de 19 de diciembre, de firma electrónica.

¿QUÉ VENTAJAS APORTA EL CUMPLIMIENTO DE LA NORMATIVA EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES?

Las empresas que deben manejar cotidianamente datos de sus clientes, trabajadores, proveedores y suministradores pueden tener la sensación de que la aplicación de la Ley en materia de protección de datos personales no supone sino una carga y gasto añadidos para cumplir una obligación legal que aparentemente no les aporta nada. Sin embargo, el tratamiento de datos no debe ser considerado únicamente una rutinaria operación para el desarrollo de la actividad económica o empresarial, sino que también es un importante activo económico. Debe desterrarse la idea de que la legislación existente no contempla más que medidas de vigilancia, inspección, fiscalización, control y sanción. En realidad, la legislación sobre protección de datos personales favorece a todos, ciudadanos y empresas,

ya que puede convertirse en un excelente argumento para mejorar la imagen, competitividad y rentabilidad de los negocios.

Una de las primeras ventajas de adecuación a las exigencias de la Ley radica en proporcionar más confianza a los clientes, factor que muchas veces es subestimado. El gran valor de contar con unos ficheros o bases de datos bien regularizados se observa al poder optimizar la gestión de clientes y proveedores. En este sentido, la cantidad de información a almacenar en una empresa crece anualmente a pasos agigantados y el aprovechamiento de esa información no siempre resulta optimizado. Además, al obligar la Ley Orgánica a ocuparse del almacenamiento, disponibilidad y destrucción de esos datos debería realizarse un planteamiento empresarial estratégico para poder sacar el máximo partido de las infraestructuras y sistemas de almacenamiento de datos, ya que a menudo se reúnen datos innecesarios u obsoletos y el volumen de información a gestionar puede hacer ineficiente el sistema. Otra de las ventajas radica en que mediante la realización de auditorias se puede racionalizar, aparte del grado de protección, la gestión del ciclo de vida de la importancia o valor de los datos. Determinados datos que en un primer momento puedan resultar cruciales para el negocio, pueden dejar de serlo a medida que transcurre el tiempo. Esta regularización en la gestión de los datos puede ser la oportunidad para diseñar un plan estratégico para sacar el mayor rendimiento a los datos y cumpliendo los objetivos de la Ley se acaban optimizando recursos y ahorrando costes.

En fin, tampoco se puede dejar de mencionar el ahorro del elevado riesgo a la hora de evitar las imposiciones de las multas correspondientes por la infracción de la normativa. La protección de datos de carácter personal constituye una obligación para las empresas y los profesionales, si no quieren quedar expuestos a duras sanciones por la Agencia Española de Protección de Datos. Así, se establecen una serie de obligaciones en aras a la protección de los datos personales contenidos en ficheros automatizados que poseen empresas y administraciones públicas, y que son tratadas por éstas con diferentes finalidades (gestión de personal, proveedores, clientes, campañas de publicidad, etc.).

¿CUÁLES SON LAS PRINCIPALES OBLIGACIONES DE LAS EMPRESAS EN MATERIA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL?

a) Obligación de notificación e inscripción de los ficheros y obtención del consentimiento

b) Informar previamente a las personas de las cuales se vaya a obtener cualquier tipo de datos personales y obtención del consentimiento

c) Obligaciones en relación con la cesión de datos y la prestación de servicios al responsable del tratamiento

d) Obligación de guardar secreto

e) Obligación de garantizar la seguridad de los datos de carácter personal

f) Obligaciones en relación con el ejercicio de los derechos de los ciudadanos (acceso, rectificación, cancelación y oposición)

g) Deber de colaboración con la Agencia Española de Protección de Datos

2. El concepto de datos de carácter personal

¿CÓMO SE DEFINEN LOS DATOS DE CARÁCTER PERSONAL?

La Ley Orgánica de Protección de Datos define los datos de carácter personal como cualquier información concerniente a personas físicas identificadas o identificables. En definitiva, toda información sobre una persona física identificada o identificable constituye dato personal

¿A QUÉ PERSONAS SE REFIEREN LAS INFORMACIONES PROTEGIDAS COMO DATOS DE CARÁCTER PERSONAL?

A personas físicas identificadas o identificables. La Agencia Española de Protección de Datos ha indicado que la protección conferida por la Ley Orgánica de protección de datos no es aplicable a las personas jurídicas, que no gozarán de ninguna de las garantías establecidas, y por extensión, lo mismo ocurrirá con los profesionales que organizan su actividad bajo la forma de empresa (ostentando, en consecuencia la condición de comerciante a la que se refiere el Código de Comercio) y con los empresarios individuales que ejercen una actividad comercial y respecto de las cuales sea posible diferenciar su actividad mercantil de su propia actividad privada, estando en el primer caso excluidos también del ámbito de aplicación de la Ley. En definitiva, pues, tanto las personas jurídicas como los profesionales y los comerciantes individuales (estos dos últimos sólo en los estrictos términos señalados, esto es, cuando sus datos hayan sido tratados sólo en su consideración de empresarios), quedan fuera del manto protector de la Ley Orgánica. Por el contrario, tanto los profesionales como los comerciantes individuales quedarían bajo el ámbito de aplicación de la Ley Orgánica y, por tanto, amparados por ella cuando los primeros no tuvieran organizada su actividad profesional bajo la forma de empresa, no ostentando, en consecuencia, la condición de comerciante y los segundos cuando no fuera posible diferenciar su actividad mercantil de la propia actividad privada. En estos dos casos deberán aplicarse siempre las garantías de la Ley Orgánica dada la naturaleza fundamental del derecho a proteger. Ello exigirá siempre ir analizando caso por caso para hallar en cada supuesto

concreto el limite fronterizo donde resulte afectado el derecho fundamental a la protección de datos de los interesados personas físicas, o, por el contrario, aquél no resulte amenazado por incidir tan solo en la esfera de la actividad comercial o empresarial, teniendo en todo caso presente que, en caso de duda, la solución deberá siempre adoptarse a favor de la protección de los derechos individuales.

¿QUÉ INFORMACIONES SE INCLUYEN EN EL CONCEPTO DE DATO PERSONAL?

Cualquier información. El objeto de tutela del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, sino los datos de carácter personal. El que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo. Existen datos públicos (nombre, apellidos, estado civil, teléfono, D.N.I, número de hijos, trabajo, ...) y datos privados (ideología, creencias, salud, datos biométricos...). Pues bien, la protección también alcanza a aquellos datos personales públicos que, por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos.

Por tanto, se refiere a cualquier aspecto parcial que afecte a nuestra persona que pueda ser objeto de registro en algún soporte físico, que lo haga susceptible de tratamiento y toda modalidad de uso posterior de estos datos por los sectores públicos y privados. Datos que aisladamente pueden no significar nada pero que asociándolos o tratándolos informativamente pueden revelar un perfil más completo del individuo.

2. El concepto de datos de carácter personal

Además, los conceptos legales se caracterizan por su total amplitud para dar cabida a aquellos aspectos que van surgiendo a consecuencia de la evolución de la informática y las nuevas tecnologías: toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable. En consecuencia, la regla es que cualquier detalle o circunstancia que permita ser asociado a una persona determinada se considerará dato de carácter personal. Estos datos podrían incluir, en sentido estricto, desde el año de nacimiento hasta el último día en que alguien se conectó a Internet.

¿LA DIRECCIÓN DE CORREO ELECTRÓNICO SE CONSIDERA DATO PERSONAL?

La Agencia de Protección de Datos ha sostenido desde 1999 la consideración de la dirección de correo electrónico como un dato de carácter personal alegando que, en todo caso, las direcciones de correo electrónico se forman por un conjunto de signos o palabras libremente elegidos, generalmente por su titular, con la única limitación de que dicha dirección no coincida con la correspondiente a otra persona, pudiendo con los datos obtenidos a través de una cuenta de correo elaborar un perfil detallado del usuario, quedando vulnerada con ello su intimidad, su vida privada.

¿LA DIRECCIÓN IP SE CONSIDERA DATO PERSONAL?

Cada ordenador se identifica con una dirección IP numérica única que consta de cuatro series de números enteros entre 0 y 255. Las direcciones IP se clasifican en dos clases: pueden ser direcciones dinámicas o fijas. La Agencia de Protección de Datos considera dato personal a la dirección IP, principalmente aduciendo que los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP, ya que, por ejemplo, un proveedor de acceso a Internet que tiene

un contrato con un abonado a Internet, normalmente mantiene un fichero histórico con la dirección IP (fija o dinámica) asignada, el número de identificación del suscriptor, la fecha, la hora y la duración de la asignación de dirección. Es más, si el usuario de Internet está utilizando una red pública de telecomunicaciones, como un teléfono móvil o fijo, la compañía telefónica registrará el número marcado, junto con la fecha, la hora y la duración, para la posterior facturación. Obviamente, el cruce de tales datos con la IP es lo que convierte a esta última en dato de carácter personal. En consecuencia, con la asistencia de los responsables de la asignación se puede identificar a un usuario de internet, es decir, obtener su identidad, por medios razonables, y, por tanto, puede hablarse de datos de carácter personal en el sentido de la Ley Orgánica.

¿LOS NÚMEROS DE TELEFONÍA FIJA Y MÓVIL SE CONSIDERAN DATOS PERSONALES?

Los números de telefonía móvil constituyen otra posible específica categoría de datos de carácter personal, ya que también se pueden enviar comunicaciones comerciales a través de este medio electrónico. Con relación a la telefonía móvil hay que puntualizar que existen dos modalidades: la modalidad prepago y la modalidad de contrato. Mientas en la modalidad de telefonía móvil de contrato no cabe duda de que a través del número asignado por la compañía de telefonía es posible conocer los datos personales referentes al titular del mismo, ya que dichos datos necesariamente han de ser facilitados en el momento de contratar el servicio, en el caso de la modalidad prepago, en principio, no es imprescindible facilitar los datos personales del consumidor que adquiere la tarjeta prepago con el número de teléfono y, en consecuencia, en este segundo caso el operador de telecomunicaciones no tendrá conocimiento de quien es el titular de ese número de móvil en particular.

En este segundo supuesto, aunque, en principio, la persona titular de la tarjeta prepago no está identificada por la operadora del servicio de telefonía, se debe recordar que la Ley orgánica de protección de datos no exige que para que un dato sea considerado personal se refiera a una persona física identificada, sino que es suficiente que

2. El concepto de datos de carácter personal

sea identificable. Aunque la Agencia de Protección de Datos todavía no se ha manifestado respecto a la consideración de los números de telefonía móvil como datos de carácter personal, consideramos que se puede extrapolar a este supuesto el argumento esgrimido por la Agencia en relación a la consideración como dato personal de las direcciones de correo electrónico en las que no constaban los datos identificativos de la persona, sino únicamente un conjunto de siglas pero necesariamente vinculadas a una dirección IP, ya que se puede averiguar el titular de una tarjeta prepago mediante la realización de una consulta al operador de telecomunicaciones que gestione dicho número de teléfono móvil, y sin que ello pueda considerarse que lleve aparejado un esfuerzo desproporcionado por parte de quien procede a la identificación, debido a que los operadores de telefonía móvil suelen ofrecer ventajas a sus usuarios de tarjetas prepago por registrarse en su página web, o les ofrecen la posibilidad de participar en concursos o promociones, y, obviamente, ese registro supondrá la recogida de datos personales.

Por tanto, los números de telefonía móvil pueden ser considerados como datos de carácter personal, ya que la telefonía móvil, al igual que la dirección de correo electrónico, es un medio de comunicación a través del cual se puede acceder a la privacidad de una persona y, en consecuencia, el titular de un número de teléfono móvil tiene derecho a controlar el uso que se haga de dicho dato.

¿QUÉ DATOS DE CARÁCTER PERSONAL QUEDAN EXCLUIDOS DEL RÉGIMEN DE PROTECCIÓN DE LA LEY ORGÁNICA DE PROTECCION DE DATOS?

En principio, la Ley Orgánica de protección de datos se refiere a todos ellos como objeto de protección, puesto que todos ellos pertenecen a la persona y deben quedar dentro de su ámbito de control. Únicamente, se excluye de forma expresa el régimen de protección de los datos de carácter personal establecido en la Ley:

a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas.

c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.

¿QUÉ DATOS DE CARÁCTER PERSONAL QUEDAN SUJETOS A UN RÉGIMEN LEGAL ESPECÍFICO?

Se regirá por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por la Ley Orgánica de protección de datos, el tratamiento de los siguientes datos personales:

a) Los ficheros regulados por la legislación de régimen electoral.

b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.

c) Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas.

d) Los derivados del Registro Civil y del Registro Central de penados y rebeldes.

2. El concepto de datos de carácter personal

e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

¿EXISTEN DIFERENCIAS LEGALES ENTRE DATOS PERSONALES?

Aunque la Ley se refiere con carácter general a todos los datos como objeto de protección, existen diversos grados de protección en la legislación dependiendo del tipo de datos manejados. En virtud de la clase de datos de que se trate se van a exigir requisitos más o menos rigurosos para permitir su tratamiento de forma legítima y se prevén también distintos niveles de seguridad para su protección. Se exigen los niveles más básicos de seguridad para los datos públicos o accesibles al público mientras que se reservan los niveles de protección más altos para aquellos datos privados que también se denominan como de especial protección o datos sensibles.

¿QUÉ DATOS SE CONSIDERAN PÚBLICOS O ACCESIBLES AL PÚBLICO?

Se consideran datos accesibles al público aquellos que se encuentran a disposición del público en general, no impedida por cualquier norma limitativa, y están recogidos en medios tales como censos, anuarios, bases de datos públicas, repertorios de jurisprudencia, archivos de prensa, repertorios telefónicos o análogos, así como los datos publicados en forma de listas de personas pertenecientes a grupos profesionales que contengan únicamente los nombres, títulos, profesión, actividad, grados académicos, dirección e indicación de su pertenencia al grupo. No obstante, cuando se habla de datos públicos para contraponerlos a los privados también se hace referencia a aquellos datos que no están publicados específicamente en ninguna fuente de acceso público pero que son conocidos por un gran número de personas y que se consideran notorios. Es decir, el carácter notorio o público de un dato no le situaría fuera de la protección de la Ley Orgánica de Protección de Datos.

¿QUÉ DATOS SE CONSIDERAN PRIVADOS O ESPECIALMENTE PROTEGIDOS?

Este tipo de datos son conocidos por un reducido grupo de personas y el titular de estos datos no está obligado a facilitarlos a terceras personas, salvo en supuestos excepcionales. Este tipo de datos contemplados especialmente en la Ley son los referidos al **origen racial, salud, vida sexual, la ideología, afiliación sindical, religión y creencias.** La muestra más clara de su especial protección puede verse en la prohibición de ficheros cuya exclusiva finalidad sea la de almacenar datos que revelen alguna de estas características o circunstancias del afectado. Cuando el fichero no tenga exclusivamente esta finalidad se permitirá su creación y gestión cuando se guarden determinados requisitos.

Para permitir el tratamiento de datos que se refieran al origen racial, salud y vida sexual se exige que exista una Ley que así lo disponga en interés general o que se consiga el consentimiento expreso del titular o afectado. En cambio, para permitir el tratamiento de datos que se refieran a la ideología, afiliación sindical, religión y creencias se añade al requisito del consentimiento expreso del titular o afectado el que sea prestado por escrito. Exceptuándose de este requisito los ficheros de partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas, asociaciones y fundaciones u 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. La creación de ficheros

¿QUÉ SE REQUIERE PARA CREAR UN FICHERO DE DATOS DE CARÁCTER PERSONAL?

Un fichero es todo conjunto organizado de datos de carácter personal, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso. El concepto de fichero no se determina en función de su titularidad pero ésta implica la aplicación de un régimen jurídico distinto, dependiendo de si estamos ante ficheros pertenecientes a la Administración o a un particular. El carácter público o privado de un fichero se debe a la naturaleza administrativa del órgano, dependencia, entidad u organismo responsable.

Así los ficheros de titularidad pública han de ajustarse a lo dispuesto en el Capítulo I del Título IV de la Ley Orgánica de Protección de Datos que exige la publicación en el Boletín Oficial del Estado o diario oficial correspondiente de una disposición general, para proceder a su creación, modificación o cancelación. Estando además sometidos a un régimen sancionador especial.

Los ficheros de titularidad privada se rigen por lo dispuesto en el Capítulo II del Título IV, que exige proceder a la notificación de su creación, modificación o cancelación ante la Agencia Española de Protección de Datos.

¿CUÁNDO DEBEN ADAPTARSE A LA NORMATIVA EN MATERIA DE PROTECCIÓN DE DATOS LOS FICHEROS AUTOMATIZADOS?

Los ficheros y tratamientos automatizados, inscritos o no en el Registro General de Protección de Datos, deben adecuarse a la Ley Orgánica dentro del plazo de 3 años, a contar desde su entrada en vigor. En dicho plazo, los ficheros de titularidad privada deberán ser comunicados a la Agencia Española de Protección de Datos y las Administraciones Públicas, responsables de ficheros de titularidad pública, deberán aprobar la pertinente disposición de regulación del fichero o adaptar la existente.

Este tipo de ficheros sometidos a cualquier clase de sistema informático si hubiese sido creado antes de 1999 se debería haber adaptado ya a lo dispuesto en la Ley orgánica de protección de datos puesto que el plazo para hacerlo se cumplió el 14 de enero de 2003. En consecuencia, es ya exigible a todos los ficheros automatizados o informatizados las medidas de seguridad establecidas en la Ley orgánica de protección de datos.

¿CUÁNDO DEBEN ADAPTARSE A LA NORMATIVA EN MATERIA DE PROTECCIÓN DE DATOS LOS FICHEROS EN SOPORTE PAPEL?

En el supuesto de ficheros y tratamientos no automatizados, su adecuación a la Ley Orgánica deberá cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados. Por tanto a los ficheros en soporte papel, tarjetas de clientes y proveedores, curricula, contratos laborales o nóminas, a partir del 24 de octubre de 2007, les serán de aplicación todas las medidas que exige la ley, exceptuando las formales.

En este caso, aunque se trate de ficheros menos sofisticados, de uso manual y sin que existan programas o sistemas informáticos que permitan ordenar, archivar, buscar o cruzar datos de forma automatizada, deben ser también objeto de control según lo dispuesto en la Ley Orgánica de Protección de Datos.

Teniendo en cuenta que la inscripción de los ficheros de datos de carácter personal en soporte papel, todavía no es obligatoria, cuando una empresa inicia su actividad, lo primero que ha de hacer es identificar con exactitud los ficheros automatizados que van a ser necesarios para el logro de su actividad u objeto legítimos, determinar el nivel de seguridad que les corresponde y notificar su creación ante la Agencia Española de Protección de Datos.

3. La creación de ficheros

¿CÓMO SE IDENTIFICAN LOS FICHEROS DE LA EMPRESA?

Normalmente, toda empresa cuenta con tres ficheros de datos de carácter personal:

1º) Fichero de Trabajadores o Nóminas que suele recoger datos identificativos (nombre y apellidos, dirección, teléfono, fecha de nacimiento, D.N.I, número de la Seguridad Social...), datos profesionales (formación y titulación académica, experiencia profesional, puestos desempeñados, rendimiento obtenido...) y datos económicos (salario, número de cuenta,...). En casos muy excepcionales puede recoger datos de salud (altas y bajas médicas, minusvalías, resultados de reconocimientos médicos...) y datos de afiliación sindical.

   Estos ficheros, si contienen todos los datos que se han enumerado, han de reunir las medidas de seguridad de nivel básico, medio y alto. No obstante, la Agencia Española de Protección de Datos permite que se proceda a la creación de distintos ficheros dentro de la misma empresa y con referencia a los mismos trabajadores afectados pudiendo diferenciar, entre ellos, los que contienen unos y otros datos, distinguiéndose también los distintos niveles de seguridad exigibles a cada uno. Por ejemplo, se crean dos ficheros distintos, uno conteniendo los datos identificativos básicos y otro en los que se refieran o puedan reflejar de algún modo datos de salud o afiliación sindical. Resultando únicamente exigible la implantación de las medidas de nivel alto a los relacionados con la salud o con la afiliación sindical. De esta forma quizá resulte más cómodo o sencillo implantar las medidas de seguridad de nivel alto a ficheros más reducidos y controlables.

2º) Fichero de Clientes que recogen datos identificativos (nombre y apellidos, dirección, teléfono, fecha de nacimiento, D.N.I...) y si son otras empresas personas jurídicas también datos profesionales de sus representantes. Con frecuencia también se recogen datos económicos (facturación, importe de gastos, forma de pago, números de cuenta...), y suelen recoger, además, datos relacionados con sus preferencias, gustos o aficiones. Si recogen todos los datos mencionados las medidas de seguridad que se adoptan en estos casos son las de nivel básico

y medio. Hay que tener presente que por contener un conjunto de datos suficientes como para permitir obtener perfiles o realizar evaluaciones de personalidad del consumidor, han de adoptarse, aparte de las medidas de seguridad de nivel básico, las de nivel medio y en concreto la auditoría bianual.

3º) Fichero de Proveedores que recogen los nombres, apellidos y cargo de representantes legales o personas de contacto en empresas. Las medidas de seguridad normalmente adoptadas para este tipo de datos son las de nivel básico.

¿CÓMO SE REGULA LA CREACIÓN DE FICHEROS DE DATOS DE CARÁCTER PERSONAL POR LA PERSONA DEL AFECTADO O INTERESADO ?

La Ley sirve de amparo a los datos de las personas físicas o naturales identificadas o identificables y excluye de su ámbito los datos de las personas jurídicas de cualquier forma y naturaleza (sociedad, asociación, fundación o corporación).

Es evidente que los datos de los trabajadores tratados por la empresa (nombre, apellidos, dirección, teléfono, fecha de nacimiento, edad, sexo, DNI, titulación académica, formación, categoría profesional, datos económicos, salario, cuenta bancaria, afiliación sindical, etc.) entran dentro del ámbito de aplicación de la Ley puesto que se refieren a personas físicas perfectamente identificadas.

Mayores problemas plantean los datos de los clientes, proveedores y suministradores cuando son personas jurídicas. Es evidente que las personas jurídicas actúan en el tráfico económico con perfecta autonomía con respecto a las personas físicas que las componen o las dirigen. Sin embargo, también es cierto que las personas jurídicas requieren para el desarrollo y desenvolvimiento de su actividad la intervención de sus representantes legales o apoderados

que son personas físicas. La Agencia de Protección de Datos, considera que, con carácter general, los datos de los profesionales y comerciantes individuales tratados en su condición de empresarios, representantes o apoderados de una persona jurídica, quedan excluidos del ámbito de aplicación de la Ley orgánica de protección de datos. En cuanto a los datos de clientes o proveedores que son personas físicas y que actúan como tales en su actividad mercantil, esta es la cuestión más controvertida y exigirá siempre ir analizando caso por caso para hallar en cada supuesto concreto el límite fronterizo donde resulte afectado el derecho fundamental a la protección de datos de los interesados personas físicas, o, por el contrario, aquél no resulte amenazado por incidir tan sólo en la esfera de la actividad comercial o empresarial, teniendo en todo caso presente que, en caso de duda, la solución deberá siempre adoptarse a favor de la protección de los derechos individuales.

Al estar ante derechos fundamentales la regla debe ser interpretada en sentido restrictivo y estarían sujetos a la Ley Orgánica de Protección de Datos los datos de los profesionales o comerciantes que no tengan organizada su actividad bajo la forma de empresa y los datos de empresarios y comerciantes individuales tratados únicamente en la esfera de su vida personal y no profesional. También estarían sujetos a la protección de la Ley en aquellos casos en los que no sea posible diferenciar su actividad mercantil de su propia actividad privada.

¿CÓMO SE REGULA LA CREACIÓN DE FICHEROS DE DATOS DE CARÁCTER PERSONAL POR LAS CARACTERÍSTICAS DEL FICHERO?

También se establece en la Ley que están afectados por su regulación tanto los datos registrados en soportes automatizados como los almacenados manualmente o en soporte papel, siempre que estén incorporados a ficheros y sean susceptibles de tratamiento automatizado o no.

¿CÓMO SE REGULA LA CREACIÓN DE FICHEROS DE DATOS DE CARÁCTER PERSONAL POR EL TERRITORIO DONDE SE REALIZA EL TRATAMIENTO?

Respecto al ámbito territorial o aplicación de la Ley orgánica de protección de datos por el lugar de tratamiento de los datos se extiende su regulación a aquellas empresas que:

a) Realicen el tratamiento en territorio español en el marco de las actividades económicas o comerciales del responsable del tratamiento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea aplicable la legislación española en aplicación de las normas internacionales.

c) Cuando el responsable del tratamiento recurra, para realizar el mismo, a medios situados en el territorio español.

¿QUÉ FICHEROS QUEDAN EXCLUIDOS DE LA APLICACIÓN DE LA LEY?

Existen determinados ficheros excluidos expresamente de la aplicación de la Ley:

a) La Ley no será de aplicación a los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas, al margen de cualquier actividad profesional (agendas personales, correspondencia particular...)

b) La Ley no será de aplicación a los ficheros sometidos a la normativa sobre protección de materias clasificadas. Se consideran materias clasificadas los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueden dañar o poner en riesgo la seguridad y defensa del Estado.

c) La Ley no será de aplicación a los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.

¿QUÉ FICHEROS TIENEN UNA REGULACIÓN ADICIONAL A LA PREVISTA EN LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS?

Existen una serie de ficheros que además de regirse por lo dispuesto sobre ellos en la Ley orgánica de protección de datos cuentan con leyes especiales que se ocupan de regular mediante disposiciones específicas los siguientes tratamientos de datos personales:

a) Los ficheros regulados por la legislación de régimen electoral.

b) Los ficheros que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.

c) Los ficheros que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas.

d) Los derivados del Registro Civil y del Registro Central de penados y rebeldes.

e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

¿CÓMO SE REALIZA LA RECOGIDA DE DATOS DE CARÁCTER PERSONAL?

La Ley establece unos principios básicos a los que debe sujetarse todo empresario que pretenda realizar un tratamiento de datos. Los principios generales marcan las pautas a las que deben atenerse todas las operaciones que implican el tratamiento empezando por la recogida de datos y acabando por la cancelación.

¿EN QUÉ CONSISTE EL PRINCIPIO DE CALIDAD EN LA RECOGIDA DE DATOS DE CARÁCTER PERSONAL?

Desde el inicio del proceso de tratamiento de datos personales debe garantizarse este principio de calidad que significa que incluso en el momento de la recogida de los datos de sus clientes, trabajadores y proveedores se buscará la congruencia y la racionalidad, garantizando que los datos no puedan ser usados sino cuando lo justifique la finalidad para la que han sido recabados. También implica adoptar medidas para asegurar la veracidad de la información contenida en los datos almacenados.

Este principio general se traduce en otros principios que lo componen:

a) Principio de adecuación o pertinencia. Este principio indica que toda empresa que recaba datos de sus trabajadores, proveedores y clientes debe haber establecido exactamente cual es la finalidad y destino de los mismos. De esta forma, únicamente se solicitarán los datos estrictamente necesarios para el cumplimiento de tales objetivos. No serán solicitados datos irrelevantes para las finalidades establecidas por la empresa. Este principio debe ponerse en relación con el principio de información, que obliga al responsable del tratamiento a informar a los interesados de los que se soliciten datos personales de la finalidad de la recogida. Se tipifica como infracción grave iniciar la recogida de datos para finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.

b) Principio de legalidad. La calidad de los datos en el momento de su recogida se refleja también en una prohibición expresa de la Ley Orgánica de Protección de Datos de recoger datos por medios fraudulentos, desleales o ilícitos. En realidad, esta prohibición recoge un principio básico de legalidad en el tratamiento de datos de carácter personal. Sin perjuicio de las posibles responsabilidades penales que pueda acarrear la utilización de vías o métodos fraudulentos, desleales o ilícitos queda absolutamente prohibido el tratamiento de los datos así obtenidos. Esta consideración de medios ilícitos hay que entenderlo en sentido amplio como contrarios a derecho.

Por ejemplo, no sería lícito el tratamiento de datos de clientes obtenidos indebidamente de ficheros de la competencia (ya sea mediante accesos no autorizados, sustracciones o filtraciones de tales ficheros de la competencia).

Los medios engañosos o fraudulentos, serían aquellos que inducen a error o causan algún tipo de confusión en el titular de los datos o de un tercero con la finalidad de obtener determinados datos de los mismos. Por ejemplo, resultaría engañoso o fraudulento el ofrecer públicamente premios o participación en sorteos, juegos o concursos ocultando o encubriendo que la finalidad principal o única es recabar datos de carácter personal de los posibles interesados para posteriores tratamientos o cesiones. Cualquier tipo de simulación de negocio inexistente para recoger datos de los posibles interesados sería utilizar medios engañosos o fraudulentos.

Respecto a la alusión a los medios desleales se debe poner en relación con el principio de información. En realidad existirá deslealtad en cualquier caso en el que el interesado no esté en condiciones de conocer la existencia del tratamiento, y no se les ha facilitado una información precisa y completa sobre las circunstancias de la obtención de datos. Se tipifica como infracción muy grave la recogida de datos de forma engañosa y fraudulenta.

¿EN QUÉ CONSISTE EL PRINCIPIO DE INFORMACIÓN EN LA RECOGIDA DE DATOS DE CARÁCTER PERSONAL?

Uno de los primeros deberes que se impone al empresario que quiere iniciar un tratamiento de datos es el de informar directamente a los interesados o afectados y respecto de los datos obtenidos de terceros. Estos deberes de información suponen un deber de lealtad en la recogida de los datos. Información respecto de los **datos obtenidos directamente de los interesados o afectados.** 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 dé datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

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

3. La creación de ficheros

Estas exigencias se establece que deben cumplirse en el momento previo a la recogida de los datos y no a posteriori. Para el correcto cumplimiento de estas obligaciones de facilitar la información implica que se incorporen cláusulas informativas en los formularios, impresos y contratos tipo. Para el caso de las comunicaciones telefónicas o telemáticas también se ha de informar de todas estas circunstancias antes de comenzar a recabar los datos de los afectados.

No se exige una forma especial para hacer llegar la información a los afectados y se deja a la libre elección de la empresa. Sin embargo, convendrá que se tomen las medidas adecuadas para poder acreditar que la comunicación de esa información se produjo antes de la recogida de datos y que se hizo de modo expreso, preciso e inequívoco. Por esta razón, es altamente recomendable que para evitar problemas de prueba se busquen medios que dejen constancia del momento y del contenido de la información suministrada. De esta forma se evitarán sanciones por haber cometido una infracción leve. En concreto, si se usan cuestionarios para obtener los datos deberán constar de forma clara y legible todas las advertencias que se han enumerado. En los casos en los que las empresas obtengan los datos de clientes o proveedores de conversaciones personales o telefónicas o tarjetas de visita será conveniente aprovechar la primera comunicación que se establezca posteriormente con los interesados para incorporar o incluir la información debida correspondiente.

Por otro lado, existen excepciones al deber de información cuando los datos se obtienen directamente del interesado. Así, también se establece que no será necesaria la información relativa al carácter obligatorio o facultativo de las respuestas a las cuestiones planteadas, las consecuencias de la obtención de datos o de la negativa a suministrarlos y de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, siempre y cuando el contenido de esta información exigible se deduzca claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban. No obstante, hay que señalar que la Agencia Española de Protección de Datos se ha pronunciado sobre el carácter de esta excepción para puntualizar que hay que interpretarla en un sentido notablemente restrictivo, ya que un consentimiento consciente e informado por parte del afectado

se gesta desde la recogida de datos. En realidad, es la información sobre la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, la que resulta más difícil o complicada a la hora de justificar su dispensa o exoneración a través de esta excepción.

En cuanto a la información respecto de los **datos obtenidos de terceros**, existe la posibilidad de que una empresa consiga datos de otras empresas o de fuentes de acceso al público, en lugar de recabarlos directamente de los afectados. Aunque los datos obtenidos por la empresa no se hayan obtenido directamente de los interesados o afectados también resulta obligatorio cumplir el principio de información.

En definitiva, la Ley también establece el deber de informar a los afectados de forma expresa, precisa e inequívoca y en tiempo oportuno de:

1º) la existencia del fichero o tratamiento en el que se han incluido sus datos y la procedencia o fuentes de los mismos.

2º) del contenido y la finalidad del tratamiento y los destinatarios de la información.

3º) de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

4º) de la identidad y dirección del responsable del tratamiento o su representante.

Sin embargo, cuando las empresas obtienen datos de fuentes accesibles al público para destinarlos a actividades de publicidad o prospección comercial se reduce la información a suministrar. En estos casos especiales en los que se utiliza con fines de marketing los datos obtenidos de fuentes accesibles al público únicamente se tiene que informar a los interesados o afectados de tres circunstancias:

3. La creación de ficheros

1º) del origen de los datos, 2º) de la identidad del responsable del tratamiento y 3º) de los derechos que les asisten.

Este deber de información, además, para que sea efectivo debe realizarse en el plazo establecido de los tres meses siguientes al registro de los datos en el fichero, salvo que el afectado hubiese sido informado con anterioridad.

No se exige una forma especial para hacer llegar la información a los afectados y se deja a la libre elección de la empresa. Sin embargo, convendrá que se tomen las medidas adecuadas para poder acreditar que la comunicación de esa información se produjo, al menos, en el plazo de los tres meses siguientes al registro de los datos en el fichero. También se deberá probar que se hizo de modo expreso, preciso e inequívoco. Por esta razón, es altamente recomendable que para evitar problemas de prueba se busquen medios que dejen constancia del momento y del contenido de la información suministrada (carta, correo electrónico, grabación telefónica...). De esta forma se evitarán sanciones por haber cometido una infracción grave.

No obstante, también aquí hay excepciones al deber de información respecto de los datos obtenidos de terceros o de fuentes de acceso público siempre y cuando:

- Exista una Ley que exima del deber de informar.
- Que el tratamiento tenga fines históricos, estadísticos o científicos.
- Que la información a los interesados resulte imposible o exija esfuerzos desproporcionados.

La última de las excepciones es la que más indeterminación contiene puesto que se deja a criterio de la Agencia Española de Protección de Datos la concurrencia de esta circunstancia de imposibilidad o desproporción en la obligación de información. En cualquier caso, la empresa interesada en obtener esta exención o liberación del deber de información deberá someter su pretensión a la Agencia Española de Protección de Datos que se deberá pronunciar al respecto.

Esta circunstancia sería apreciable en los casos en los que el esfuerzo económico a realizar para el cumplimiento del deber de información hiciese totalmente inviable la creación del fichero o el tratamiento.

¿EN QUÉ CONSISTE EL PRINCIPIO DE CONSENTIMIENTO EN LA RECOGIDA DE DATOS DE CARÁCTER PERSONAL?

Se trata de un principio crucial sobre el que gira todo el sistema de la protección de datos personales. El consentimiento significa otorgar la facultad a cada persona para decidir el tratamiento al que han de estar sometidos sus datos y a quién se le permite realizar ese tratamiento. Este principio del consentimiento es verdaderamente el eje del derecho a la protección de datos de carácter personal puesto que casi podríamos hablar de poder o potestad de cada interesado a decidir libre y voluntariamente sobre el destino de aquella esfera de datos que le pueden llegar a identificar o caracterizar. Por esta razón se ha hablado incluso de autodeterminación de cada uno para con los datos que le son propios. Lo cierto es que esta concepción podría incluso observarse desde una óptica diferente a la tradicional, puesto que si estamos ante un derecho sobre el que su titular tiene poder de disposición sobre sus datos se podría considerar como algo parecido al derecho de propiedad, salvando las distancias. Es cierto que no estamos ante un derecho de propiedad en sentido estricto ni la facultad de disposición es total, ni cabe renuncia anticipada del derecho. Sin embargo, sí es cierto que cabe un margen de disposición y de negociación sobre los datos de carácter personal que significan un activo económico importante para las empresas interesadas en contar con ellos.

El principio general supone que para que una empresa pueda tratar datos de carácter personal de trabajadores, clientes y proveedores, ha de contar con el consentimiento de los mismos.

Además, este consentimiento de los titulares o interesados, necesario para el tratamiento, ha de reunir cuatro requisitos esenciales para considerarlo válidamente prestado

3. La creación de ficheros

- Ha de ser consentimiento libre. No debe contar con ningún vicio de los contemplados en el Código Civil. Es decir, no debe concurrir error, dolo, violencia o intimidación.

- Ha de ser consentimiento específico. Referido siempre a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento.

- Ha de ser consentimiento informado. De esta forma el afectado deberá conocer con antelación al tratamiento, la existencia del mismo, y las finalidades para las que se produce.

- Ha de ser consentimiento inequívoco. No se puede presumir o deducir la existencia del consentimiento de la mera conducta o comportamiento del afectado. Es preciso que exista expresamente una acción u omisión que implique la existencia del consentimiento.

De lo indicado se desprende que de las características del consentimiento no se infiere necesariamente su carácter expreso en todo caso, razón por la cual en aquellos supuestos en que el legislador ha pretendido que el consentimiento deba revestir ese carácter, lo ha indicado expresamente, mientras que el consentimiento podrá ser tácito en el tratamiento de datos que no sean especialmente protegidos.

¿PUEDEN LOS MENORES NO EMANCIPADOS CONSENTIR VÁLIDAMENTE EL TRATAMIENTO SOBRE SUS DATOS PERSONALES SIN NECESIDAD DEL COMPLEMENTO DE SU REPRESENTANTE LEGAL?

Se ha planteado a la Agencia Española de Protección de Datos la cuestión de si pueden los menores no emancipados consentir válidamente el tratamiento sobre sus datos personales sin necesidad del complemento de su representante

legal. En este sentido se ha distinguido entre los menores de edad mayores de catorce años, que pueden realizar válidamente algunos actos y negocios jurídicos y el resto. Como el Código Civil exceptúa de la representación legal a los actos referidos a derechos de la personalidad y otros que el hijo, de acuerdo con las leyes y con sus condiciones de madurez, puede realizar por sí mismo se considera que a esa edad se dispone de capacidad suficiente para consentir, por sí mismos, el tratamiento automatizado de sus datos de carácter personal. Respecto al resto de los menores de edad, que no alcancen los catorce años, no se ha pronunciado la Agencia Española de Protección de Datos, pero se ha de atender a lo dispuesto en el mismo artículo del Código Civil para considerar las condiciones de madurez y en caso de duda entender necesario el consentimiento de sus representantes legales.

¿CUÁNDO HA DE SOLICITARSE EL CONSENTIMIENTO?

Lo cierto es que la Ley Orgánica de Protección de Datos guarda silencio sobre el momento indicado para recabar el consentimiento de los afectados por el tratamiento de datos personales. Es decir, no establece expresamente si el consentimiento debe prestarse con carácter previo al tratamiento o si puede prestarse con posterioridad al mismo. Sin embargo, sí que puede deducirse de los principios inspiradores de la Ley que con carácter general el consentimiento debe ser previo aunque excepcionalmente podría solicitarse a posteriori. También parece razonable que sea la Agencia Española de Protección de Datos la que decida, en cada caso, cuándo no será necesario solicitar el consentimiento previo y resultaría conveniente realizarle la consulta antes de proceder al tratamiento.

¿QUÉ FORMA HA DE ADOPTAR EL CONSENTIMIENTO?

La regla general que parece inspirar la Ley Orgánica de Protección de Datos es la libertad en cuanto a la forma de recabar el consentimiento. Podemos deducir fácilmente este principio de libertad de forma si observamos la exigencia excepcional de que se recoja el consentimiento de forma expresa y, en algún caso, por escrito en el régimen especial de los datos sensibles o especialmente protegidos.

3. La creación de ficheros

Es decir, deberá contarse con el consentimiento expreso, aunque no se requiere que figure por escrito, cuando se recojan datos referidos al origen racial, salud y a la vida sexual del afectado. De otro lado, no sólo deberá contarse con el consentimiento expreso sino que deberá constar además por escrito cuando los datos de carácter personal revelen ideología, afiliación sindical, religión y creencias. En cambio, en sentido contrario, hemos de entender que para los datos que no estén incluidos entre los calificados como especialmente protegidos o sensibles no sólo cabrá considerar el consentimiento expreso sino incluso el consentimiento tácito.

El consentimiento tácito se entiende como aquél que se deriva de la inactividad, silencio o falta de oposición del afectado al tratamiento del que se le ha informado, no sirve para la cesión de datos y sólo cabe en el tratamiento de datos que no sean especialmente protegidos. Este tipo de consentimiento tiene, en ocasiones el inconveniente de la prueba de haber obtenido el mismo.

De otro lado, aunque se admita el consentimiento tácito del afectado, se exige que sea un consentimiento inequívoco. La Agencia Española de Protección de Datos entiende que, además, para que este consentimiento tácito sea inequívoco será necesario que se otorgue al interesado un plazo prudencial para que conozca y comprenda que su falta de oposición al tratamiento implica un consentimiento del mismo por omisión.

Sin embargo, no es admisible el consentimiento presunto o derivado de determinada conducta o comportamiento del interesado por el cual el responsable del tratamiento deduzca un consentimiento. En cualquier caso, faltaría el requisito de que el consentimiento del afectado sea inequívoco. Es decir la propia actuación del interesado no puede implicar por sí misma un determinado compromiso u obligación puesto que, en general, no cabe deducir o suponer un consentimiento claro y contundente de meros actos. En realidad, este consentimiento presunto sólo podría incluirse dentro de algunas excepciones a la necesidad de recabar el consentimiento de los interesados que están expresamente previstas en la Ley. En concreto podría entenderse implícito en la recogida de datos que 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.

En realidad, como corresponde a la empresa la carga de probar el consentimiento del tratamiento por parte de los interesados (clientes, trabajadores y proveedores) es aconsejable que lo recabe de forma expresa y por escrito al mismo tiempo y aprovechando las cláusulas informativas que debe crear al efecto cuando comiencen sus relaciones, contando así fácilmente con la firma del afectado en los documentos.

¿EN QUÉ SUPUESTOS NO ES NECESARIO RECABAR EL CONSENTIMIENTO DE LOS INTERESADOS?

Existen excepciones a la necesidad de recabar el consentimiento de los interesados. La Ley establece cuatro excepciones a la necesidad de recabar el consentimiento de los interesados, suprimiendo esta obligación del responsable del tratamiento:

1ª) No será necesario recabar el consentimiento cuando los datos se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias. Lo cierto es que esta excepción no tiene trascendencia para el sector privado. Únicamente afecta a los tratamientos efectuados por Administraciones y no afecta a los tratamientos empresariales.

2ª) No será necesario recabar el consentimiento cuando los datos 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. Esta es la excepción que suele darse con mayor frecuencia. Efectivamente, las empresas no tienen que solicitar el consentimiento de los trabajadores puesto que la relación laboral supone un otorgamiento genérico del consentimiento para el tratamiento de los datos, siempre que éstos sean necesarios para el mantenimiento de dicha relación deberá informarse, no obstante, a los trabajadores de la existencia del fichero donde serán incluidos los datos y el objeto del tratamiento. Se puede entender como adecuado que el empleador recabe los datos precisos para el normal desenvolvimiento de la empresa y, dentro de éstos, parece adecuado

3. La creación de ficheros

que se recaben los correspondientes al control de la productividad en el trabajo para que se pueda comprobar el grado de cumplimiento de las obligaciones que competen a los empleados. Sin embargo, cuando las empresas pretendan utilizar los datos obtenidos en virtud de la relación laboral con fines distintos a ésta deberán solicitar el consentimiento de los interesados. No se ha admitido dentro de esta excepción el tratamiento de datos para la realización de cursos de formación, la publicación de revistas internas o a efectos de publicidad o difusión. Hay que ser conscientes de que los hechos referidos a las relaciones sociales y profesionales en que se desarrolla la vida laboral, aunque están excluidas del ámbito de la intimidad personal y familiar, puede afectar al ámbito de la privacidad en la protección de datos personales.

Esta excepción de recabar el consentimiento también se aplica respecto a los datos de clientes o proveedores (personas físicas y personas de contacto o representantes legales de personas jurídicas) desde que existe una relación contractual o precontractual. En estos casos la justificación se encuentra en la necesidad de tener toda la información de la contraparte en una relación negocial. Es evidente que en los pactos o contratos deben identificarse las partes contratantes, siendo esta una regla básica para evitar posibles vicios en el consentimiento.

En cualquier caso, la dispensa de recabar el consentimiento en estos casos está directamente relacionada con el mantenimiento de la relación negocial y con el cumplimiento de las prestaciones que se deriven de la relación obligatoria. En este sentido, una vez extinguida la relación obligatoria y cumplido el contrato deberá cesar el tratamiento o deberá recabarse el consentimiento de los afectados para conservar los ficheros. Aunque es cierto que en estos casos, señalados por la Ley, las empresas no están obligadas a solicitar el consentimiento de los interesados para tratar sus datos, en la medida en que han de cumplir el deber de información pueden aprovechar las cláusulas o cartas informativas para recabar dicho consentimiento. Esta solución es aconsejable aunque no resulta exigible legalmente. En este sentido se pueden ver los códigos-tipo de protección de datos.

3ª) Tampoco es exigible que se recabe el consentimiento del afectado cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en el supuesto en que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

4ª) Por último, no será necesario solicitar el consentimiento cuando los datos figuren en fuentes de acceso 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 siempre que no se vulneren los derechos y libertades fundamentales del interesado.

Para que una empresa pueda valerse de esta excepción tienen que darse tres requisitos:

1. Que se hayan obtenido los datos de una fuente de acceso público (son fuentes de acceso público el censo promocional, los repertorios telefónicos, las listas de personas pertenecientes a grupos profesionales, los diarios y boletines oficiales y los medios de comunicación).

2. Que se traten los datos para satisfacer un interés legítimo propio o ajeno.

3. Que el tratamiento no vulnere ningún derecho o libertad fundamental.

En realidad, con esta excepción parece que la Ley Orgánica de Protección de Datos se está refiriendo a las empresas de publicidad que se dedican a recabar datos de carácter personal de fuentes accesibles al público bien para realizar envíos publicitarios, por sí mismas, bien para venderlos a otras empresas que los destinen a los mismos fines. Aunque en estos casos no es necesario contar con el consentimiento de los interesados sí que es imprescindible informarles del origen de los datos, de la identidad del responsable del tratamiento, así como de los derechos que les asisten. De esta forma podrán ejercitar, si lo desean, su derecho de oposición al tratamiento de datos.

3. La creación de ficheros

En cualquier caso, también se podrá aprovechar las cláusulas informativas que las empresas creen al efecto para recabar al mismo tiempo el consentimiento, aunque no sea obligatorio. Resulta relativamente sencillo obtener, de esta forma, el consentimiento tácito inequívoco si se pone un plazo para manifestarse en contra del tratamiento y no se obtiene respuesta alguna pasado el plazo.

Es un hecho comprobado que la publicidad bien enfocada a las personas interesadas en el tipo de productos y servicios ofertados se traduce en una mayor receptividad y éxito de respuesta en la demanda. En cambio, la publicidad lanzada en masa sin recabar el consentimiento de los interesados puede tener un efecto negativo en los destinatarios de la misma que si no desean recibir la publicidad no sólo no responderán a la oferta sino que pueden provocar cierta animosidad o animadversión.

No obstante, el primer contacto de la empresa publicitando productos o servicios, que puede hacerse sin consentimiento de los potenciales clientes y destinatarios de las ofertas si se cumplen los requisitos antedichos, puede servir como una buena forma de prospección comercial. En los subsiguientes contactos se puede dirigir la oferta a quienes se hayan mostrado interesados o hayan manifestado su consentimiento a la publicidad. En este sentido también se ha comprobado que es más efectiva, por conseguir mayor éxito de contratación y respuesta, la fórmula de recabar el consentimiento expreso que no la fórmula de obtener el consentimiento tácito.

¿CÓMO PUEDE REVOCARSE EL CONSENTIMIENTO PRESTADO?

Una vez que se ha obtenido el consentimiento de los interesados o afectados hay que ser conscientes de que no se trata de un consentimiento a perpetuidad e irrevocable. Sin embargo, la Ley Orgánica de Protección de Datos al otorgar al interesado la facultad de revocar su consentimiento le exige que exista una causa justificada para la revocación. No obstante, pese a requerir la revocación una justa causa, en la práctica empresarial suele aceptarse como causa suficiente la mera manifestación de voluntad del interesado anulando el consentimiento prestado con anterioridad. La filosofía en la admisión de la revocación parte de que habiéndose prestado el consentimiento con

plena libertad, debe permitirse retirarlo con idéntica libertad. Sin embargo, en aquellos casos en los que la revocación pueda causar algún perjuicio o afectar a la organización de la empresa, podrá exigirse la concurrencia de alguna causa justificada. Además, también se establece que a la revocación no se le atribuirá efectos retroactivos por lo que todo el tratamiento o los actos que se hayan producido a consecuencia del mismo hay que entender que serán perfectamente válidos y desplegarán toda su eficacia. En consecuencia, la revocación, al ser un acto de carácter recepticio, sólo tiene efectos desde que llega a conocimiento del responsable del fichero.

¿PUEDE OPONERSE EL AFECTADO AL TRATAMIENTO DE DATOS PERSONALES?

Junto con la manifestación del consentimiento se prevé la posibilidad de manifestar la oposición al tratamiento de datos personales. Evidentemente esta posibilidad de oposición tiene sentido en aquellos casos en los que las empresas no necesitan solicitar el consentimiento de los interesados para tratar sus datos por darse alguna de las excepciones previstas en la Ley. Estos casos en los que no se requiere recabar el consentimiento del afectado sí que será necesario que se le informe y así se le facilita la posibilidad de oponerse al tratamiento. Para oponerse al tratamiento se exige que existan motivos fundados y legítimos relativos a una concreta situación personal y que ninguna Ley disponga lo contrario. En estos casos el responsable del fichero excluirá del tratamiento los datos relativos al afectado sin coste alguno para éste último. La Agencia Española de Protección de Datos considera que estos motivos fundados y legítimos, en el caso de ficheros de publicidad y prospección comercial no serán necesarios y basta una simple petición previa.

Sin embargo, será difícil acceder a hacer efectivo este derecho de oposición haciendo excluir los datos del interesado de sus ficheros cuando los mismos son necesarios o esenciales para mantener o cumplir la relación que vincula al interesado con la empresa. Por ejemplo, resultaría imposible mantener una relación laboral ante la solicitud de un trabajador de la empresa de que se eliminen sus datos de los ficheros de la misma. En estos casos podría ejercitarse parcialmente y eliminar los datos que no resulten estrictamente necesarios para que la relación pudiera

3. La creación de ficheros

existir y cumplirse correctamente. No obstante, el motivo personal en estos casos puede ser la intención de extinguir las relaciones que vinculan al interesado con la empresa, aunque en este caso más bien procedería ejercitar el derecho de cancelación.

Donde tiene una clara aplicación esta posibilidad de oposición es en los supuestos en los que los datos son recabados por la empresa de una fuente de acceso público para satisfacer un interés legítimo y, en concreto, cuando se utilizan los datos con fines de publicidad y prospección comercial. En este campo tiene especial sentido el denominado derecho de oposición.

¿DE QUÉ FORMA SE PUEDEN RECOGER LOS DATOS PERSONALES CUMPLIENDO LA LEY?

Corresponde al empresario que obtiene datos personales la prueba del cumplimiento de los principios de información y consentimiento. En concreto, será el responsable del fichero o tratamiento quien tenga la carga de la prueba de la observancia de los requisitos legales.

Establecer los criterios para recoger correctamente los datos personales implica analizar las diferentes formas o medios utilizados para este fin que suelen ser los medios habituales de comunicación entre responsables del fichero y titulares de los datos.

¿QUIÉN ES EL ENCARGADO DEL TRATAMIENTO?

La Ley recoge la figura del encargado del tratamiento, persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento (encargado del responsable del fichero, persona física o jurídica, de naturaleza pública a privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento). Hay que tener en cuenta,

además, que el encargado del tratamiento no tiene que limitar sus funciones a la recogida y grabación de datos, sino que, en general, se extiende a cualquier prestación, por cuenta del responsable, que implique el acceso a datos personales. En la medida en que es previsible que se incremente por parte de las empresas la subcontratación de servicios relacionados con el tratamiento de datos, aumentará también la relevancia de esta figura. En este sentido, en el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente. El término que se utiliza también deja claro que no se establece un mecanismo de sustitución ni de derivación de responsabilidades sino de agregación, pues el responsable del fichero no pierde su condición de tal ni queda exonerado de responsabilidad por el hecho de que al encargado del tratamiento que incumpla lo estipulado se le atribuya también la consideración de responsable del tratamiento.

¿CÓMO SE RECOGEN LOS DATOS PERSONALES POR ESCRITO?

Éste es el medio idóneo para la acreditación del cumplimiento de los principios de información y consentimiento por parte del responsable del fichero, máxime si se obtiene de forma expresa, es decir, acompañado de la firma del titular de los mismos. Simplemente se trataría de añadir a los contratos, pólizas, pliegos de condiciones, formularios o impresos una cláusula informativa y otra de consentimiento.

Contar con la firma del afectado por el tratamiento es un medio de prueba definitivo. Por esta razón si se han recogido los datos de clientes o proveedores a través de las conocidas y habituales tarjetas de visita que éstos entreguen, aunque no es exigible legalmente, sería aconsejable que se les hiciese llegar después una sencilla carta, a modo de saluda, con una simple cláusula para informar y obtener un consentimiento tácito inequívoco.

3. La creación de ficheros

En cualquier caso, hay que ser conscientes de que se deberá conservar toda la documentación ante el supuesto de que la Agencia Española de Protección de Datos se la solicite. El objetivo debe encaminarse a obtener y guardar todos los medios de prueba posibles para acreditar la autorización efectuada por el titular.

Si se ha recurrido al consentimiento tácito, al menos deberá demostrarse que se ha efectuado el envío de la comunicación al interesado, que se le ha otorgado un plazo prudencial para que pueda tener conocimiento de que su falta de oposición al tratamiento implica consentimiento al mismo y asegurarse de que la dirección utilizada se corresponde con el domicilio actual o, al menos, el último conocido o comunicado por el propio afectado. Si se aprovecha una única cláusula o párrafo para obtener el consentimiento del interesado para tratar sus datos con distintas finalidades es recomendable que se ofrezca la posibilidad de no prestar el consentimiento para algunas de ellas. Ésta es la práctica aconsejada por la Agencia Española de Protección de Datos.

Los responsables de los ficheros deben ser consecuentes y realizar el tratamiento de los datos de forma adecuada al consentimiento obtenido y la información suministrada, sin extralimitarse interpretando que el consentimiento conseguido es el más amplio posible y habilita al encargado del fichero a realizar cualquier tratamiento.

¿CÓMO SE RECOGEN LOS DATOS PERSONALES POR TELÉFONO?

En muchas ocasiones las empresas obtienen los datos de sus clientes o proveedores a través de las conversaciones mantenidas con ellos por teléfono. Esta forma de recogida de datos presenta, con carácter general, dos grandes problemas, el de la prueba sobre la información suministrada y el consentimiento recibido y el de la prueba de la identificación de la persona que se presenta como titular de los datos.

Respecto a la prueba de la información y el consentimiento telefónicos se puede obtener mediante grabaciones de la conversación. No obstante, debe tenerse en cuenta que los ficheros de voz son ficheros de carácter personal

y, en consecuencia también están sujetos a la Ley Orgánica de Protección de Datos. En este sentido, debe cumplirse con los requisitos ya señalados y dar la posibilidad al interesado de que se oponga al tratamiento. Respecto al problema de la falta de identificación del interlocutor hay que precisar que el sistema de contratación telefónica es un método válido y perfectamente admitido en derecho. En estos casos aunque no se requiere la existencia de firma convencional sí que hay que acreditar la aceptación de todas y cada una de las cláusulas del contrato. Después de la contratación deberá enviarse inmediatamente justificación escrita de la contratación efectuada, donde constarán todos los términos de la misma. Por esta razón y para evitar problemas en la identificación de los interlocutores es conveniente que la empresa acredite que se ha ratificado documentalmente por el titular. Como la carga de la prueba recae sobre el empresario se establecen como medios de prueba cualquier soporte como las cintas de grabación sonoras, los disquetes y, en particular, los documentos electrónicos y telemáticos, siempre que quede garantizada su autenticidad, la identificación fiable de los manifestantes, su integridad, la no alteración del contenido de los manifestado, así como el momento de su emisión y recepción.

Finalmente si los datos se recogen a través de mensajes cortos SMS es evidente que el emitente del mensaje no recibe en ese momento la preceptiva información sobre protección de datos. Para estos casos la Agencia Española de Protección de Datos indica que la información obligatoria deberá ser facilitada con carácter previo con independencia de la vía a través de las cuales se recaben los datos personales. En consecuencia se establece por la Agencia Española de Protección de Datos que la información deberá facilitarse en el mismo momento en que se promociona el servicio, cuando se le da publicidad, en los anuncios públicos o medios de comunicación, al número de teléfono al que se remiten los mensajes.

Para recabar el consentimiento del afectado se requerirá su consentimiento inequívoco y cuando facilita voluntariamente sus datos consiente en el tratamiento de los mismos pero siempre en los estrictos términos y condiciones de los que ha sido convenientemente informado en el momento de la recogida. Deberán conservarse todas las informaciones y advertencias suministradas en la publicidad del servicio.

3. La creación de ficheros

Siempre deben quedar a salvo los derechos de los afectados a oponerse al tratamiento, previa petición y sin gastos. En estos casos se deberá proceder a cancelar los datos ante la solicitud de oposición. Normalmente la oposición del interesado se formaliza por escrito, aportando copia de su DNI para acreditar su personalidad, con acuse de recibo.

¿CÓMO SE RECOGEN LOS DATOS PERSONALES POR INTERNET?

Cada vez es más frecuente la recogida de datos a través de páginas web o correos electrónicos. Ciertamente, el hecho de utilizar internet para recabar datos personales no afecta a la aplicación de todos los principios contenidos en la Ley Orgánica de Protección de Datos. Es decir, deberán observarse los requisitos del derecho de información, deberá recabarse el consentimiento cuando sea necesario y todo ello deberá acreditarse debidamente por el responsable del fichero.

¿CÓMO SE NOTIFICAN LOS FICHEROS A LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS?

Una vez identificados los ficheros automatizados de datos de carácter personal que pretende crear una empresa, ésta ha de proceder a la notificación de los mismos a la Agencia Española de Protección de Datos. Esto se puede hacer mediante soporte escrito, sopote magnético o a través de Internet empleando el modelo normalizado aprobado por la Agencia Española de Protección de Datos. En general, los modelos de notificación que deben cumplimentarse para proceder a la notificación deben contener las siguientes referencias:

- Nombre, denominación o razón social, D.N.I, N.I.F. ó C.I.F, dirección y actividad u objeto social del Responsable del Fichero.

- Ubicación del fichero.

- Identificación de los datos que se pretendan tratar, detallando los supuestos de datos especialmente protegidos que previsiblemente contendrán.

- Dirección de la oficina o dependencia en la cual pueden ejercitarse los derechos de acceso, rectificación, cancelación u oposición.

- Origen o procedencia de los datos.

- Finalidad del fichero.

- Cesiones de datos previstas.

- Encargados del tratamiento.

- Transferencias temporales o definitivas que se prevean realizar a otros países, indicando los mismos.

- Destinatarios o usuarios previstos para cesiones o transferencias.

- Sistemas de tratamiento que se vayan a utilizar.

- Medidas de seguridad que se van a implantar.

Una vez efectuada la notificación, si ésta contiene la información preceptiva y reúne las demás exigencias legales,

3. La creación de ficheros

el Director de la Agencia, a propuesta del Registro General de Protección de Datos, acordará la inscripción. En caso contrario requerirá al Responsable del Fichero para que en el plazo de 10 días subsane el defecto, advirtiéndole de que si no lo hace, se le tendrá por desistido de su petición.

No solicitar la inscripción de un fichero constituye una infracción leve. Si la inscripción no se efectúa después de haber sido requerido para ello por el Director de la Agencia Española de Protección de Datos, la infracción puede ser calificada como grave.

¿CÓMO SE DEBEN GESTIONAR LOS FICHEROS?

En primer lugar hay que tener siempre presente que los dos principios a los que debe someterse todo tratamiento de datos en la empresa son el de información y consentimiento.

En segundo lugar, debe observarse y cumplir con el principio de calidad en el tratamiento de los datos.

¿EN QUÉ CONSISTE EL PRINCIPIO DE CALIDAD EN LA GESTIÓN DE FICHEROS?

La primera manifestación de este principio se refiere al principio de adecuación o pertinencia. Mediante este principio se establece que debe haber una recogida de datos ajustada a los que resulten estrictamente necesarios para el ámbito y finalidades determinadas, explícitas y legítimas para los que se obtenían. No obstante, no se limita este principio al momento de la recogida sino que también lo extiende a cualquier tratamiento posterior que debe tomar únicamente datos adecuados, pertinentes y no excesivos. Asimismo, este principio de calidad se traduce, a su vez, en el principio de utilización no excesiva ni abusiva, que indica que los datos recabados no pueden ser desviados de la finalidad para la que inicialmente se recogieron. Aunque la Ley se refiere expresamente a la prohibición de los datos para finalidades incompatibles, hay que matizar que el empleo de este término por la Ley

no autoriza a utilizar los datos para fines distintos para los que no se hubieran obtenido, pese a que fueran compatibles con estos. Así, la recogida de datos solo puede hacerse con fines determinados, explícitos y legítimos, y el tratamiento posterior no puede hacerse de manera incompatible con dichos fines. En este sentido, se tipifica como infracción grave iniciar la recogida de datos para finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.

Existe una única excepción a la regla extraída de este principio de utilización no excesiva ni abusiva. No se considerará incompatible el tratamiento posterior de los datos con fines históricos, estadísticos o científicos, con independencia del fin para el que hubieran sido recabados.

La calidad en el tratamiento de datos también se traduce en el principio de exactitud o actualidad. El principio de calidad del dato comienza a infringirse en el momento en que se mantienen datos erróneos. En todo fichero los datos de carácter personal han de ser exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. La consecuencia de que los datos que obren en los ficheros resulten ser inexactos en todo o en parte, o incompletos, es su cancelación de oficio y su sustitución por los correspondientes datos rectificados o completados.

¿QUÉ OBLIGACIONES SE DESPRENDEN DEL CUMPLIMIENTO DE PRINCIPIO DE CALIDAD PARA EL RESPONSABLE DEL TRATAMIENTO?

Dos obligaciones se desprenden de este principio para el responsable del tratamiento. En primer lugar, debe garantizar la veracidad de los datos que se contienen en sus ficheros. En segundo lugar, debe proceder constantemente a la rectificación o cancelación de oficio de aquellos datos que detecte que resultan inexactos o incompletos. Toda empresa desde el momento de creación de los ficheros y durante todo el periodo que dure el tratamiento

3. La creación de ficheros

ha de garantizar la exactitud y veracidad de los datos que figuran en sus ficheros. Para poder cumplir con estas obligaciones resulta necesario que el responsable del fichero tenga conocimiento (de oficio o a instancia de parte) de la inexactitud de los datos que obran en sus ficheros. En los casos en los que existan datos en los ficheros que resulten inexactos o falsos pero el responsable del tratamiento no ha conocido ni podido conocer de estas circunstancias no le será exigible responsabilidad alguna. Es lógico que si se ha obtenido un dato de una fuente accesible al público en la que existía un error no puede exigirse que se sospeche de la inexactitud ni que se verifique o averigüe la exactitud de todos los datos publicados. En realidad, esta obligación surge desde el mismo momento en que el responsable del fichero haya conocido o pueda llegar a conocer de forma fiable la inexactitud. Para alcanzar este conocimiento de las posibles inexactitudes o cambios en los datos personales se deben articular sistemas de verificación periódica al cabo de un tiempo razonable, recordando a los interesados sus derechos de acceso, rectificación, cancelación y oposición.

Mayor cuidado y atención se exige en el cumplimiento de la obligación de exactitud y actualidad de los datos recogidos en los ficheros de solvencia patrimonial y crédito o ficheros comunes. Debiéndose extremar, en estos casos, la diligencia de los empresarios que utilicen ficheros que indiquen este tipo de datos debiéndose hacer barridas periódicas que garanticen la cancelación automática de los datos inexactos. Hay que ser conscientes que la inclusión de una persona en uno de estos ficheros limita enormemente su capacidad económica en los mercados crediticios provocándole indudables perjuicios que pueden ser reclamados ante la jurisdicción ordinaria.

Por último, la calidad de los datos se refleja en una prohibición expresa de recoger datos por medios fraudulentos, desleales o ilícitos. En realidad, esta prohibición recoge un principio básico de legalidad en el tratamiento de datos de carácter personal. Sin perjuicio de las posibles responsabilidades penales que pueda acarrear la utilización de vías o métodos fraudulentos, desleales o ilícitos queda absolutamente prohibido el tratamiento de los datos así obtenidos. Esta consideración de medios ilícitos hay que entenderlo en sentido amplio como contrarios a derecho. (Principio de legalidad. Ver págs. 44 y ss. de la Guía).

Guía de Protección de Datos para Empresas

4. El tratamiento de datos de carácter personal

¿QUÉ SE ENTIENDE POR TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL?

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. Por tanto, cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados y aplicadas a datos personales (de ahí se deriva que incluir datos personales en una página web debe considerarse un tratamiento de este carácter).

De esta forma, parece que se abarcan todas las posibilidades porque lo cierto es que hoy en día resulta prácticamente imposible realizar cualquier actividad profesional o empresarial sin la utilización de la informática y en el momento en el que existan en estas herramientas datos identificativos de cualquier tipo estaremos ante un tratamiento.

¿CUÁLES SON LAS OBLIGACIONES GENERALES DE UNA EMPRESA EN EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL?

Podrían resumirse, a grandes rasgos, las obligaciones relacionadas con la protección de datos en adoptar todas las medidas necesarias para impedir el abuso o mal empleo de la información recabada en el ejercicio de su actividad económica. También implicaría el realizar un tratamiento de datos legal y leal respecto a todos y cada uno de los individuos afectados por el tratamiento. De esta forma, se exige que el afectado pueda, en todo momento, tener conocimiento real y exacto de la suerte y situación de sus datos en el fichero, la finalidad o el destino que se les da, así como que se le facilite el ejercicio de sus derechos.

Los datos de carácter personal podrán ser obtenidos directamente del afectado, o por medio de un tercero, siempre y cuando se haya recabado previamente a la cesión el consentimiento inequívoco e informado del interesado. Consentimiento es toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el

interesado consienta el tratamiento de datos personales que le conciernen. A este respecto, una empresa que mantenga un fichero o archivo informático está obligada, entre otras cosas, a:

a) Notificar e inscribir sus ficheros en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos.

b) Procurar, con diligencia y rapidez, el correcto ejercicio de los derechos al interesado, adoptando las medidas oportunas para que todas las personas de la organización empresarial que tienen acceso a los datos, puedan informar del procedimiento establecido para facilitar ese ejercicio en plazo.

c) Cumplir con los principios de calidad, información, consentimiento, etc., redactando en los contratos, facturas, albaranes, recibos o publicidad, las cláusulas informativas y obligatorias que garanticen el cumplimiento de la Ley.

d) Guardar y respetar el deber de confidencialidad o secreto respecto de los datos que trata, formando en este sentido a sus empleados que acceden a datos respecto a las obligaciones relacionadas con el tratamiento. En este sentido, se impone al responsable del fichero y a quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal, secreto profesional respecto de los mismos y 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.

e) Implantar en su sistema de información las medidas de seguridad exigidas de nivel bajo, medio o alto dependiendo de los datos manejados; medidas de orden técnico, operativas y jurídicas, entre ellas crear documentos de seguridad para impedir el acceso a los ficheros, en particular, y a los datos, en general, a personas no autorizadas, o para evitar el desvío de la información hacia destinos no previstos.

f) Redactar los contratos necesarios con terceros para permitir el acceso a los datos en caso del necesario mantenimiento de los equipos y programas informáticos, servicios de mensajería, pagos bancarios y publicidad.

g) Informar y recabar el previo consentimiento de los interesados para proceder a la cesión o comunicación de datos. Así, los datos de carácter personal objeto del tratamiento sólo pueden 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. Este consentimiento, no obstante, no será preciso que sea previo:

- cuando la cesión está autorizada en una ley

- cuando se trate de datos recogidos de fuentes accesibles al público

- 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

- 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.

- cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos y científicos

- 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.

¿QUÉ SE ENTIENDE POR TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL ESPECIALMENTE PROTEGIDOS?

Existen una serie de datos a los que la Ley orgánica de protección de datos ha dotado de unas especiales garantías para su tutela. Son los datos que se consideran sensibles porque su tratamiento puede suponer un mayor riesgo de vulneración de los derechos y libertades del interesado y requieren de un mayor grado de protección.

En realidad, lo que se trata de garantizar con la especial protección de estos datos es la posibilidad de ejercitar derechos y libertades ulteriores sin ser objeto de discriminación o exclusión (por ejemplo, obtener un trabajo en condiciones de igualdad, posibilidad de contratar un seguro de vida, etc.).

Existen tres categorías de datos que cuentan con una protección reforzada: los datos de carácter personal relativos a la ideología, religión, creencias y afiliación sindical, los datos de carácter personal relativos al origen racial o étnico, salud y vida sexual y los datos de carácter personal relativos a la comisión de infracciones penales o administrativas

¿QUÉ SE EXIGE PARA EL TRATAMIENTO DE LOS DATOS DE CARÁCTER PERSONAL RELATIVOS A LA IDEOLOGÍA, RELIGIÓN, CREENCIAS Y AFILIACIÓN SINDICAL?

Estos datos no tienen porqué ser directamente datos relativos a ideología, religión, creencias y afiliación sindical, sino que basta con que sean datos que los puedan revelar o de los que se puedan inferir. En este sentido, la Agencia Española de Protección de Datos hace una interpretación muy amplia e incluye en su ámbito de aplicación los datos que, dentro de este contexto, proporcionen indicios sobre alguno de estos aspectos. En esta interpretación extensa de los derechos fundamentales a favor de su titular que hace la Agencia se está llevando a la práctica el mandato

recogido en el artículo 16.2 de nuestra Constitución cuando establece que nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

Para el tratamiento de datos de carácter personal que revelen ideología, religión, creencias y afiliación sindical es necesario que el interesado haya prestado su consentimiento de forma expresa y por escrito. Por consiguiente, no se acepta ninguna forma de consentimiento tácito. Es decir, no bastará con la no oposición al tratamiento pese a que se le haya informado. Deberá, en todo caso, incluirse en un soporte escrito una cláusula de protección de datos en la que se mencione de forma clara y explícita que los datos recabados van a formar parte de un tratamiento para que el interesado preste su consentimiento y firme el documento.

Las excepciones a esta exigencia de contar con el consentimiento expreso y por escrito del afectado son:

A) Los partidos políticos, los sindicatos, las iglesias, las confesiones o comunidades religiosas y las asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, religiosa o sindical, están autorizadas al tratamiento de los datos de sus propios asociados, miembros o afiliados que obran en sus ficheros sin tener que recoger su consentimiento expreso y por escrito. Sin embargo, para la cesión de estos datos a terceros estas entidades si que deberán recabar el consentimiento expreso y por escrito de los afectados si se revela su ideología, afiliación sindical, religión o creencias. Hay que ser conscientes que sólo constando la procedencia de los datos ya se revelan estos datos especialmente protegidos.

B) En los supuestos en los que el tratamiento sea necesario para salvaguardar un interés vital del afectado o de otra persona, en el supuesto en el que el afectado está física o jurídicamente incapacitado para dar su consentimiento, siempre que no se vulneren los derechos y libertades fundamentales del interesado. Esta excepción se ha de interpretar en el sentido más restrictivo en situaciones de emergencia y estando en juego la supervivencia o la integridad física del afectado o de otra persona en peligro. En todo caso, también deberá informarse al afectado de que, conforme lo dispuesto en el artículo 16.2 de la Constitución española, no está

obligado a declarar sobre los datos relativos a su ideología, religión o creencias y que, en consecuencia, está en su derecho de no prestar su consentimiento al tratamiento de estos datos. Esta advertencia deberá incluirse en la cláusula de protección de datos.

Otra de las restricciones impuestas para asegurar la protección de este tipo de datos consiste en una prohibición general de proceder al tratamiento de datos con la finalidad exclusiva de almacenar datos que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico o vida sexual. Esta prohibición contiene las siguientes excepciones:

A) El tratamiento realizado por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto cuando resulte necesario para los siguientes fines: la prevención médica, el diagnóstico médico, la prestación de asistencia sanitaria, tratamientos médicos y la gestión de servicios sanitarios.

B) Cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

¿QUÉ SE EXIGE PARA EL TRATAMIENTO DE LOS DATOS DE CARÁCTER PERSONAL RELATIVOS AL ORIGEN RACIAL O ÉTNICO, SALUD Y VIDA SEXUAL?

La Agencia española de protección de datos interpreta de forma extensiva la noción de datos que hagan referencia a la salud del interesado, ya que se entiende que es dato de salud cualquier información relativa a la salud actual, pasada o futura, física o mental, pudiendo incluirse trastornos del comportamiento, tales como alcoholismo o toxicomanías, así como cualquier tipo de información genética. El empresario no podrá acceder en ningún caso a

la información sanitaria resultante de los reconocimientos médicos dirigidos a la prevención de riesgos laborales, puesto que están dirigidos específicamente a salvaguardar la salud del trabajador.

Únicamente se permite la recogida, tratamiento o la cesión de datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual cuando el interesado lo consienta expresamente o cuando, por razones de interés general, así lo disponga una Ley. Debe tenerse en cuenta que para el tratamiento de estos datos no se exige propiamente que el consentimiento expreso se obtenga por escrito. No obstante, por la propia necesidad de acreditación de la existencia de dicho consentimiento expreso es aconsejable que se incluyan cláusulas de protección de datos aprovechando el texto de los formularios, fichas, cuestionarios, contratos o cualquier otra forma de recogida de este tipo de datos. Queda excluida la posibilidad del consentimiento tácito con lo que el consentimiento ha de ser previo al tratamiento y emitido de forma expresa e inequívoca.

Existen excepciones a la regla del consentimiento expreso para proceder al tratamiento de datos que hagan referencia al origen racial, a la salud y a la vida sexual:

A) Cuando el tratamiento esté previsto en una norma jurídica con rango de Ley.

B) En los supuestos en los que el tratamiento sea necesario para salvaguardar un interés vital del afectado o de otra persona, en el supuesto en el que el afectado está física o jurídicamente incapacitado para dar su consentimiento, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

Aunque concurriendo alguna de las dos excepciones mencionadas no haga falta el requisito de la obtención del consentimiento expreso, continua existiendo el deber de información al interesado del tratamiento de sus datos y de los derechos que le asisten. Asimismo, los datos de carácter personal que hagan referencia al origen racial, a la salud, y a la vida sexual del interesado, podrán ser objeto de tratamiento siempre que se realice por un profesional sanitario sujeto al secreto profesional o por otra persona, sujeta asimismo a una obligación equivalente

de secreto, cuando resulte necesario para los siguientes fines: la prevención médica, el diagnóstico médico, la prestación de asistencia sanitaria, tratamientos médicos y la gestión de servicios sanitarios.

¿QUÉ SE EXIGE PARA EL TRATAMIENTO DE LOS DATOS DE CARÁCTER PERSONAL RELATIVOS A LA COMISIÓN DE INFRACCIONES PENALES O ADMINISTRATIVAS?

Estos datos comprenden cualquier información que revele la comisión de las infracciones sancionadas por la jurisdicción penal o la autoridad administrativa. No pueden tratarse estos datos por empresas privadas ni por entidades que no estén consideradas como Administración Pública en sentido estricto. Las Administraciones públicas son las únicas autorizadas a tratar este tipo de datos.

¿QUÉ SE EXIGE PARA EL TRATAMIENTO DE LOS DATOS DE CARÁCTER PERSONAL DE LOS MENORES DE EDAD?

El tratamiento de datos de menores presenta la dificultad específica respecto a la obtención de un consentimiento libre, inequívoco, específico e informado por parte del menor.

Se ha planteado a la Agencia Española de Protección de Datos la cuestión de si pueden los menores no emancipados consentir válidamente el tratamiento sobre sus datos personales sin necesidad del complemento de su representante legal. En este sentido se ha distinguido entre los menores de edad mayores de catorce años, que pueden realizar válidamente algunos actos y negocios jurídicos y el resto. Como el Código Civil exceptúa de la representación legal a los actos referidos a derechos de la personalidad y otros que el hijo, de acuerdo con las leyes y con sus condiciones de madurez, puede realizar por sí mismo, se considera que a esa edad se dispone de capacidad suficiente para consentir, por sí mismos, el tratamiento automatizado de sus datos de carácter personal. Respecto al resto de los

menores de edad, que no alcancen los catorce años, no se ha pronunciado la Agencia Española de Protección de Datos, pero se ha de atender a lo dispuesto en el mismo artículo del Código Civil para considerar las condiciones de madurez y en caso de duda entender siempre necesario el consentimiento de sus representantes legales.

¿QUÉ SE EXIGE PARA EL TRATAMIENTO DE LOS DATOS DE CARÁCTER PERSONAL CON FINES DE PUBLICIDAD y MARKETING?

Los tratamientos de datos de carácter personal con fines de publicidad comprenden las siguientes actividades:

1. Alquiler de direcciones a terceros

2. La publicidad propia o de terceros

3. La venta directa o a distancia

4. La recopilación de direcciones

5. El reparto de documentos

6. La prospección comercial y otras actividades análogas

La Ley Orgánica de Protección de Datos limita los tratamientos de datos con fines de publicidad y prospección comercial a los datos de carácter personal, en particular a los nombres y direcciones, que figuren en fuentes accesibles al público o que hayan sido facilitados por los propios interesados y obtenidos con su consentimiento. Los datos provenientes de fuentes accesibles al público son aquellos ficheros cuya consulta puede ser realizada

por cualquier persona, no impedida por una norma limitativa, o sin más exigencias que el abono de una contraprestación. La Ley Orgánica de Protección de Datos enumera las fuentes que tienen consideración de accesibles al público y a las cuales se aplicarán las disposiciones especiales a las mismas:

1. El censo promocional

2. Los repertorios telefónicos

3. Las listas de personas pertenecientes a grupos profesionales

4. Los diarios y boletines oficiales

5. Los medios de comunicación

La recogida de datos de carácter personal que figuren en fuentes accesibles al público constituye una excepción a la obligación de recabar el consentimiento previo del interesado para proceder a su tratamiento, siempre y cuando el 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, y que no se vulneren los derechos y libertades fundamentales del interesado.

Tratándose de fuentes accesibles al público que se destinan a la actividad de marketing, en cada comunicación que se dirija al interesado se le deberá informar del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten. Si no se destinan a la actividad de marketing, se le deberá informar del contenido del tratamiento, de la procedencia de los datos, 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, de

la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición y de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. Este deber de información garantiza que el afectado no quede indefenso, así podrá ejercer sus derechos de acceso, rectificación, cancelación u oposición. La copia de los datos que figuren en la fuente accesible al público pierde tal carácter transcurrido un año desde el momento de su obtención. Se pretende así asegurar la actualización de los datos.

La actividad de subcontratación en el ámbito de la publicidad y promoción comercial provoca a menudo situaciones complejas en las que puede resultar difícil determinar quién es el responsable de tratamiento y por lo tanto a quien incumbe el cumplimiento de las obligaciones impuestas en materia de protección de datos y la responsabilidad ante posibles infracciones.

La Agencia Española de Protección de Datos, en el ámbito de la publicidad y de la prospección comercial, designa como responsable del tratamiento a la entidad beneficiaria de la publicidad. La entidad beneficiaria de la publicidad interesada en promocionar sus productos y servicios a los usuarios clientes o potenciales usuarios de los mismos y, a tales efectos, o bien emplea datos personales contenidos en sus propios ficheros, o bien recurre a la contratación de ficheros externos, responsabilidad y titularidad de terceras empresas. Si los datos personales utilizados en la campaña provienen de la base de datos de una tercera entidad, esta última será la responsable del fichero o tratamiento.

En todo caso, el responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de la misma a los afectados, indicando la finalidad del fichero, la naturaleza de los datos que han sido cedidos y de la dirección del cesionario. La Ley Orgánica de Protección de Datos marca la obligación para el responsable del tratamiento de cancelar los datos cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. En caso de que el responsable del tratamiento quiera seguir conservando los datos, éstos deberán ser conservados de forma disociada.

¿QUÉ SE EXIGE PARA EL TRATAMIENTO DE LOS DATOS DE CARÁCTER PERSONAL DEL CENSO PROMOCIONAL?

El censo promocional designa al fichero elaborado a partir del censo electoral, limitado a los datos de empadronamiento. Este fichero tiene que ser actualizado por los órganos competentes trimestralmente, excluyendo los datos de los interesados que los hayan solicitado.

Conforme dispone la normativa de Bases de Régimen Local, los datos del Padrón municipal se cederán a otras Administraciones Públicas que lo soliciten, sin consentimiento previo del afectado, solamente cuando les sean necesarios para el ejercicio de sus respectivas competencias, y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes.

También pueden servir para elaborar estadísticas oficiales sometidas al secreto estadístico. Fuera de estos supuestos, los datos del Padrón son confidenciales y el acceso a los mismos se regirá por lo dispuesto en la normativa de datos de carácter personal. Es claro, por lo tanto, que los datos del Padrón son confidenciales, pues contienen datos propios del ámbito de privacidad de los empadronados.

En consecuencia, los datos contenidos en el Padrón solo podrán ser cedidos para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del afectado. Toda la obtención de datos resultante de la consulta de un fichero, debe considerase cesión. Teniendo en cuenta que existen excepciones tasadas a la regla general, de forma que no será necesario el consentimiento del afectado (empadronado) cuando la cesión tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal o los Jueces y Tribunales, en el ejercicio de las funciones que tienen atribuidas.

4. El tratamiento de datos de carácter personal

¿QUÉ SE EXIGE PARA EL TRATAMIENTO DE LOS DATOS DE CARÁCTER PERSONAL DE LOS REPERTORIOS TELEFÓNICOS?

Las guías de abonados deben limitarse a los datos estrictamente necesarios para identificar a un abonado concreto, no pudiendo recogerse más que datos de mera identificación, a no ser que el abonado preste su consentimiento. Los abonados pueden exigir a los operadores ser excluidos de las guías, que se omita parcialmente su dirección, o bien que se indique que sus datos personales no pueden utilizarse para fines de venta directa.

¿QUÉ SE EXIGE PARA EL TRATAMIENTO DE LOS DATOS DE CARÁCTER PERSONAL DE LAS LISTAS DE LOS COLEGIOS PROFESIONALES?

Los grupos profesionales pueden elaborar y publicar las listas de sus miembros sin necesidad de recabar el consentimiento del interesado, siempre que los datos de carácter personal contenidos en las mismas sean los estrictamente necesarios para cumplir con la finalidad del listado. Si el grupo profesional deseara incluir datos adicionales deberá solicitar el consentimiento expreso, preciso e inequívoco del interesado quien podrá revocarlo en cualquier momento. Los interesados tienen derecho a que la entidad responsable del mantenimiento de los listados de los colegios profesionales indique gratuitamente que sus datos personales no pueden ser utilizados para fines de publicidad o prospección comercial.

La Ley Orgánica de Protección de Datos dispone que exclusivamente se considerarán fuentes accesibles al público, las listas de personal pertenecientes a grupos de profesionales que contengan únicamente los siguientes datos: nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo.

Los colegios profesionales podrán utilizar los datos personales de sus miembros con fines de publicidad y de prospección comercial únicamente si el envío tiene una relación directa con el ejercicio profesional.

¿QUÉ SE EXIGE PARA EL TRATAMIENTO DE LOS DATOS DE CARÁCTER PERSONAL DE LOS DIARIOS Y BOLETINES OFICIALES?

Los datos de carácter personal que aparezcan en todos los diarios y boletines oficiales pueden ser tratados en un fichero con fines de publicidad y marketing. Esta autorización no incluye los Libros de Registro o de tablones de los Juzgados.

¿QUÉ SE EXIGE PARA EL TRATAMIENTO DE LOS DATOS DE CARÁCTER PERSONAL CONTENIDOS EN LOS MEDIOS DE COMUNICACIÓN?

Se pueden tratar sin consentimiento del afectado los datos de carácter personal contenidos en los medios de comunicación. Considerando medio de comunicación la prensa, televisión o la radio. Los datos que figuren en una página web no pueden incluirse en ficheros con fines de publicidad y prospección comercial, a no ser que se haya recabado previamente al tratamiento, el consentimiento del interesado.

¿EN QUÉ CONSISTE EL FICHERO SOBRE SOLVENCIA PATRIMONIAL Y CRÉDITO?

Existen diversas entidades cuya actividad social consiste en la prestación de servicios de información sobre solvencia patrimonial y crédito, quedando sujetas a un régimen especial. Aquellas entidades que se dediquen a la prestación de servicios de información sobre solvencia patrimonial y crédito sólo pueden tener tres tipos de fuentes de las que obtener los datos que registran o incorporan a sus ficheros:

- fuentes accesibles al público

- informaciones facilitadas por el afectado

- datos facilitados por el acreedor o por quien actúe por su cuenta o interés

Se distinguen dos supuestos claramente diferenciados:

1. Ficheros de solvencia

2. Ficheros de cumplimiento e incumplimiento de obligaciones dinerarias

A los ficheros de cumplimiento e incumplimiento de obligaciones dinerarias le es aplicable en su totalidad la Instrucción 1/1995 de la Agencia Española de Protección de Datos. En este supuesto, nos encontramos ante dos ficheros diferentes; de un lado, el fichero del acreedor, del que provienen los datos, y, del otro, el fichero que almacena los datos sobre el cumplimiento de obligaciones dinerarias y que presta información en esa materia. A este último fichero se le denomina Fichero de morosos o Fichero común. Estos ficheros tienen como finalidad dar a conocer en el tráfico mercantil la solvencia patrimonial, así como el grado de cumplimiento o incumplimiento de las obligaciones dinerarias contraídas por los afectados con sus acreedores, informando y emitiendo, así mismo, evaluaciones y apreciaciones sobre la solvencia patrimonial y crédito de las personas. Las empresas asociadas a las entidades prestadoras de servicios de información sobre solvencia patrimonial y crédito, son Bancos, Cajas de Ahorro, Cooperativas de Crédito, Entidades Aseguradoras, Sociedades y Agencias de Valores o Entidades Financieras de Crédito. Su relación es bidireccional, es decir, los asociados a este tipo de entidades hacen consultas a los ficheros, solicitando información de morosidad sobre una determinada persona, pero también como acreedores les proporcionan datos de personas con las que mantengan una deuda cierta, vencida, exigible y cuyo pago haya sido previamente requerido y no satisfecho. Además, sólo pueden cederse los datos personales de hasta seis años atrás y que sean determinantes para enjuiciar la solvencia económica de los afectados.

Los requisitos para la inclusión de datos en un fichero común son:

a) Existencia previa de una deuda cierta, vencida y exigible, que haya resultado impagada

b) Requerimiento previo de pago a quien corresponda, en su caso, en cumplimiento de la obligación

c) Que el acreedor se asegure de que concurren todos los requisitos anteriores en el momento de notificar los datos adversos al responsable del fichero común

En relación con el modo de comunicar los datos al fichero común, la Agencia Española de Protección de Datos señala que las entidades asociadas generalmente los facilitan en soportes magnéticos, que pueden ser entregados a través de servicios de mensajería o de transferencia de ficheros, con una periodicidad, al menos, mensual.

De manera que por una parte, el acreedor es el responsable de la veracidad y exactitud de la información que incorporan a los ficheros comunes, de la rectificación, actualización de estos datos y de la cancelación de los mismos. Por otra parte el responsable de fichero es el responsable de enviar una notificación a los interesados con posterioridad a su inclusión, en el que les informe que los datos han sido incluidos en su fichero por cuenta de terceros, de tratar con celeridad los datos que le son suministrados por los acreedores, de atender adecuadamente a los ejercicios de derechos de acceso, rectificación y cancelación que efectúen los interesados y de comunicar los nombres y direcciones de los terceros que han consultado la información del interesado, así como, en su caso las valoraciones y apreciaciones que del mismo se hayan vertido. La entidad suministradora de los datos al fichero común, es el responsable del contenido de la información y le corresponde a éste responder de la carga de la certeza y exactitud del dato introducido en el fichero común. Por su parte el responsable del fichero común no tiene competencia para modificar o cancelar los datos inexactos que se encuentran en su fichero.

4. El tratamiento de datos de carácter personal

¿CUÁLES SON LAS OBLIGACIONES DEL RESPONSABLE DEL FICHERO SOBRE SOLVENCIA PATRIMONIAL Y CRÉDITO?

- Actualización de datos

- Las normas de calidad de la Ley Orgánica de Protección de Datos establecen la obligación de actualizar los datos de carácter personal, de forma que respondan con veracidad de la situación actual del interesado. La norma Primera de la Instrucción 1/1995, dispone que la comunicación del dato inexistente o inexacto, con el fin de obtener su cancelación o modificación, deberá efectuarse por el acreedor o quien actúe por su cuenta al responsable del fichero común en el mínimo tiempo posible, y en todo caso en una semana. Esto significa que si se hallasen datos inexactos en todo o en parte o incompletos, serán cancelados y sustituidos por el responsable del fichero común por los correspondientes datos rectificados o completos, siempre a instancias de la entidad informante o acreedor. La inclusión de datos inexactos y la permanencia de datos desactualizados en los ficheros de cumplimiento de obligaciones dinerarias configuran una infracción grave de la Ley Orgánica de Protección de Datos.

- Cancelación de datos y prohibición de la constancia de saldo cero. De conformidad con la Ley Orgánica de Protección de Datos, los datos adversos de carácter personal incluidos en el fichero común no podrán referirse a más de seis años. En la práctica, la agencia de Protección de Datos, en sus distintas resoluciones, ha señalado que el plazo de seis años comienza a computar desde el vencimiento del último plazo de la obligación. Por otra parte, una vez satisfecho el pago por el deudor, debe ser excluido del fichero mediante la cancelación de sus datos. En este sentido, se prohíbe que los ficheros dejen constancia de la existencia de deudas pasadas, puesto que se debe reflejar, siempre y en todo caso, la situación actual del afectado, con lo que si la deuda ha sido cumplida o se ha extinguido se deberán cancelar inmediatamente todos los datos existentes en el fichero como si nunca hubiesen estado incluidos en ficheros de esa naturaleza. En este mismo sentido se ha pronunciado la

Audiencia Nacional en reiteradas ocasiones al entender que si la situación real y actual del afectado es la de no tener deudas pendientes no puede considerarse que tengan ningún saldo, ni siquiera como saldo cero. Se ha de entender que está prohibida la anotación de situaciones de abono de deudas, pago o cumplimiento porque significa informar, de forma indirecta, sobre la condición de deudor en el pasado del afectado.

- Comunicación de la inclusión en el fichero común. No es necesario el consentimiento del afectado para que sus datos sean cedidos a las entidades responsables del fichero común. Sin embargo, es obligada la notificación al afectado de los datos más relevantes de su inclusión. El plazo es de treinta días desde que se registran los datos personales en el fichero común. Se le notificará una referencia de los datos personales que han sido incluidos, informándole así mismo del derecho que le asiste a recabar la información de la totalidad de los mismos. La notificación establece la obligación del responsable del fichero común de efectuar una notificación por cada deuda concreta y determinada con independencia de que ésta se tenga con el mismo o con distintos acreedores.

Todas las personas incluidas en un fichero sobre solvencia patrimonial y crédito tienen reconocidos los derechos de acceso, rectificación y cancelación de sus datos y podrán ejercerlos bien ante el responsable de dicho fichero o bien ante la entidad acreedora.

Derecho de acceso. Cuando el interesado lo solicite, el responsable le comunicará los datos, así como las evaluaciones y apreciaciones que se hayan comunicado sobre el afectado en los últimos seis meses, así como el nombre y dirección de los cesionarios. En este caso el responsable del fichero común deberá resolver sobre la solicitud de acceso en el plazo máximo de un mes y si la resolución fuere estimatoria deberá hacer efectivo el acceso en el plazo de diez días siguientes a la notificación de aquélla. Cualquier otra entidad participante en el sistema, ante una solicitud de acceso, deberá comunicar al afectado todos los datos relativos al mismo a los que ella pueda acceder, así como la identidad del responsable del fichero común para que pueda completar el ejercicio de su derecho de acceso. El plazo que tiene la entidad acreedora para resolver la solicitud de acceso es de un mes. Si

la resolución es estimatoria, el acceso se hará efectivo en el plazo de diez días siguientes a la notificación de aquélla.

Derecho de rectificación y cancelación. En los ficheros de prestación de servicios de información de solvencia patrimonial y crédito, cualquiera que sea el origen de los datos, cuando el afectado lo solicite, el responsable del fichero común deberá cumplir la obligación de satisfacer los derechos de rectificación y cancelación. Si la solicitud del ejercicio de los derechos de rectificación o cancelación de datos se dirige al responsable del fichero común, éste tomará las medidas oportunas para trasladar dicha solicitud a la entidad que haya facilitado los datos, para que ésta resuelva.

En el caso de que el responsable del fichero común no haya recibido contestación por parte de la entidad en el plazo de diez días, procederá a la rectificación o cancelación cautelar de los mismos. Si la solicitud del ejercicio de los derechos de rectificación o cancelación de datos se dirige a cualquier otra entidad participante en el sistema y hace referencia a datos que dicha entidad haya facilitado al fichero común, procederá a la rectificación o cancelación de los mismos en sus ficheros y a notificarlo al responsable del fichero común en el plazo de diez días. Si la solicitud hace referencia a datos que la entidad no hubiera facilitado al fichero común, dicha entidad informará al afectado sobre este hecho, proporcionándole, además, la identidad del responsable del fichero común para que pueda completar el ejercicio de sus derechos.

¿QUÉ SE EXIGE PARA EL TRATAMIENTO DE LOS DATOS DE CARÁCTER PERSONAL DEL FICHERO SOBRE SOLVENCIA PATRIMONIAL Y CRÉDITO?

Al realizar una consulta al fichero común por parte de alguna entidad participante en el sistema, se recibe una gran cantidad de datos que también son objeto de tratamiento, sobre todo si se obtiene copia completa de un fichero.

La Ley Orgánica de Protección de Datos no establece nada sobre la posibilidad de conservar los datos obtenidos de estos ficheros comunes, pero no cabe duda de que el acreedor que ha hecho la consulta será el responsable del fichero o ficheros que crease a partir de la información obtenida del fichero común, así como la legalidad de su creación y tratamiento. En este sentido, existen tres riesgos potenciales respecto de la creación, mantenimiento y posterior tratamiento de estos ficheros por las entidades acreedoras:

1. Comunicación o cesión de datos a terceros- Es muy común, entre empresas dedicadas a la actividad de financiación, la comunicación o cesión de datos obtenidos de ficheros sobre solvencia patrimonial y crédito a terceras empresas, de manera que dicha comunicación pueda ser considerada ilícita, al no ser consentida por los afectados. Los afectados en el ejercicio del derecho que les asiste de poder acceder y consultar los ficheros comunes, pueden comprobar que hay una entidad con la que no mantienen relación, que ha consultado el fichero común y obtenido información sobre su persona. La infracción sería muy grave.

2. Falta de actualización de los datos que conserven y constancia del saldo cero. En aquellos casos en los que una entidad acreedora hace una consulta a un fichero común, recibiendo una gran cantidad de datos, existe un riesgo de falta de actualización adecuada de los datos que afecta a la calidad. Hay dos formas de comunicación de datos a las entidades asociadas o afiliadas: la consulta singular y la obtención de una copia completa del fichero. La Agencia de Protección de Datos establece que deberán cumplirse las siguientes recomendaciones:

   a) Garantizar que todas las copias de los ficheros existentes en cada entidad informantes sean idénticas

   b) Habilitar los procedimientos necesarios para garantizar que a los afectados se les informa de forma cabal y actualizada de todos los destinatarios de la información contenida en el fichero

   c) Adoptar todas aquellas medidas que impidan la existencia de copias de dichos ficheros en manos de personas físicas jurídicas no autorizadas a acceder a las mismas

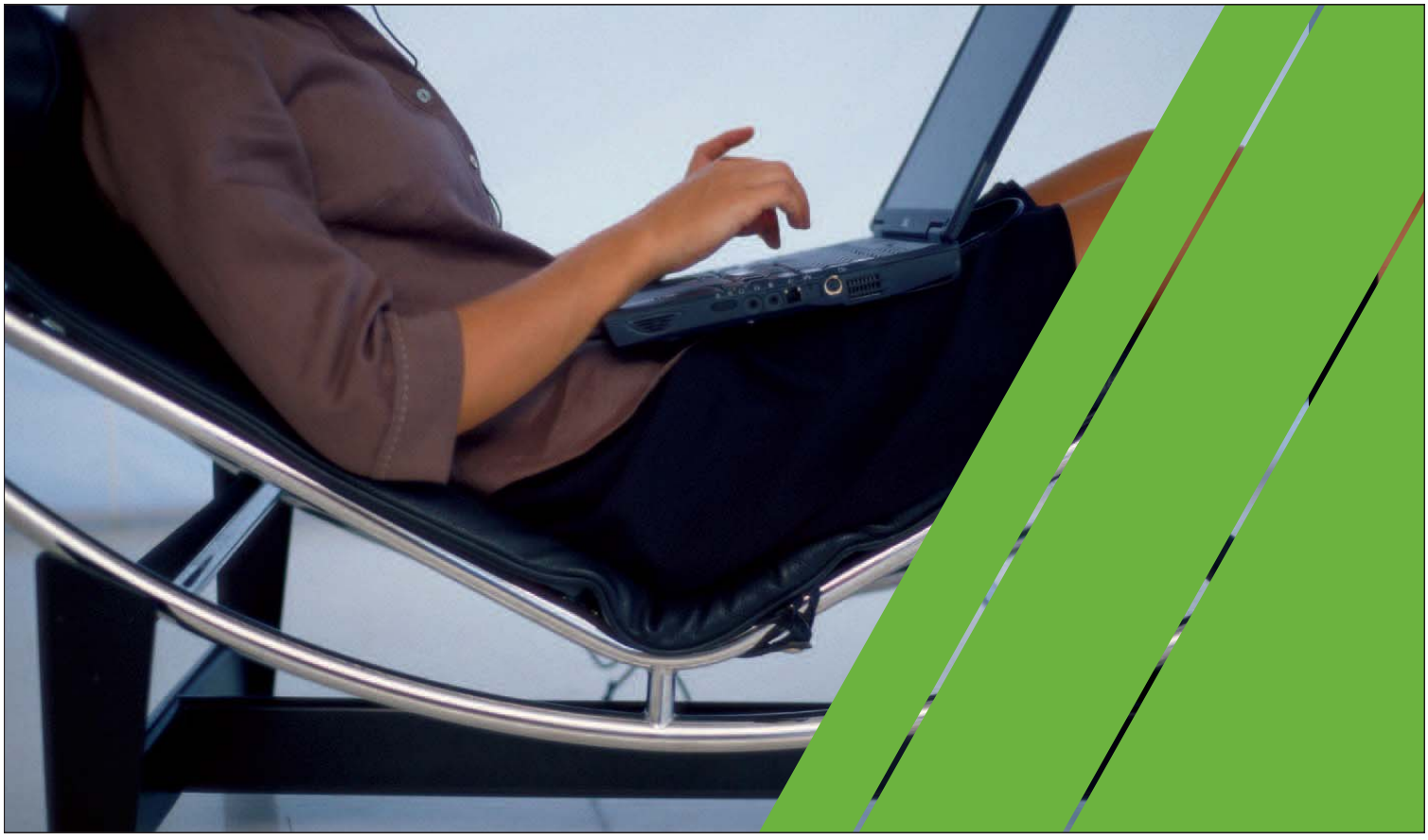
3. Uso de aplicaciones informáticas para la gestión de créditos (scoring). Se trata de herramientas informáticas que incorporan una serie de factores de riesgo, cuya adecuada combinación entre sí ofrece como resultado una puntuación de la calidad crediticia de la operación que se pretende realizar con un cliente. En relación con estas y otras prácticas similares, se reconocen los siguientes derechos de los afectados:

   - Derecho a no verse sometido a decisiones con efectos jurídicos sobre ellos, que se basen únicamente en un tratamiento de datos personales destinados a evaluar determinados aspectos de su personalidad.

   - Derecho a impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos personales que ofrezca una definición de sus características o personalidad.

   - Derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizado en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.

Guía de Protección de Datos para Empresas



¿EN QUÉ CONSISTE EL PRINCIPIO DE SEGURIDAD DE LA INFORMACIÓN?

La seguridad y protección de la información procesada en sistemas electrónicos e informáticos y la seguridad de las redes de comunicación a través de las cuales viaja la información, constituye cada vez más una prioridad para los responsables y encargados del tratamiento, debido a la necesidad de proteger datos y seguir procurando el uso de los medios electrónicos para la gestión y explotación de los mismos.

Uno de los principios básicos recogidos en la legislación vigente en materia de protección de datos es el de la seguridad de la información. Se prohíbe textualmente el registro de datos de carácter personales 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. Tanto el responsable del fichero como, 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 están expuestos, ya provengan de la acción humana o del medio físico o natural.

Tan importante ha sido el principio de seguridad de la información que la propia Agencia de Protección de Datos inició los trabajos tendentes a la redacción del texto del Reglamento de Medidas de Seguridad, que ha venido a establecer las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal sujetos al régimen de la Ley Orgánica de Protección de Datos.

¿CUÁLES SON LOS NIVELES DE SEGURIDAD?

El Reglamento de Medidas de Seguridad establece tres niveles de seguridad, con algunos matices, y para cada uno de estos niveles asigna la obligación de adoptar una serie de medidas de seguridad tanto técnicas como organizativas. Estos niveles han sido establecidos atendiendo a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

¿A QUÉ FICHEROS SE EXIGE UN NIVEL DE SEGURIDAD ALTO?

Los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud, vida sexual, afiliación sindical así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deben reunir, además de las medidas de nivel básico y medio, las calificadas como de nivel alto. Cualquier entidad que tenga informatizado el tratamiento relativo las nóminas de sus empleados está sujeto al nivel alto de seguridad.

¿A QUÉ FICHEROS SE EXIGE UN NIVEL DE SEGURIDAD MEDIO?

Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y aquellos ficheros cuyo funcionamiento se rija por el artículo 28 de la Ley Orgánica 5/1992, deben reunir, además de las medidas de nivel básico, las calificadas como de nivel medio.

¿A QUÉ FICHEROS SE EXIGE UN NIVEL DE SEGURIDAD BÁSICO?

Los ficheros que contengan datos de carácter personal deben adoptar las medidas de seguridad calificadas como de nivel básico. Si hay un conjunto de datos que, cruzándose, permiten obtener una evaluación de la personalidad del individuo, se requiere auditoría bianual.

5. La seguridad de los ficheros

¿EN QUÉ CONSISTEN LAS MEDIDAS DE SEGURIDAD?

El Reglamento de Medidas de Seguridad sólo establece los mínimos legales exigibles, de manera que, los responsables y encargados del tratamiento, en todo momento podrán superar lo dispuesto en el Reglamento con la implantación de medidas que sobrepasen los niveles señalados.

¿CUÁLES SON LAS MEDIDAS DE SEGURIDAD GENERALES PARA TODOS LOS NIVELES?

1. Los accesos a datos de carácter personal a través de redes de comunicaciones deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

2. La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero debe ser autorizada expresamente por el responsable del fichero y, en todo caso, debe garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

3. Los ficheros temporales deben cumplir el nivel de seguridad que les corresponda con arreglo a los criterios establecidos en el Reglamento de Medidas de Seguridad, siendo borrados una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

¿CUÁLES SON LAS MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO?

MEDIDAS DE NIVEL BÁSICO (Ver Esquema nivel básico en Anexo II - Pág. 202)

1. Elaboración e implantación de toda la normativa de seguridad de la organización en el llamado Documento de Seguridad de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información.

2. Definición y documentación de las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información y deben adoptarse las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

3. Adopción de las medidas necesarias para que el personal con acceso a datos conozca las normas de seguridad que afecten al desarrollo de sus funciones.

4. Adopción de las medidas necesarias para que el personal con acceso a datos conozca las consecuencias en que pudiera incurrir en caso de incumplimiento.

5. Establecimiento de un procedimiento de notificación y gestión de incidencias con un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y los efectos que se hubieran derivado de la misma.

6. Elaboración y mantenimiento de una relación actualizada de usuarios que tengan acceso autorizado al sistema de información y establecimiento de procedimientos de identificación y autenticación para dicho acceso. En los casos en que el mecanismo de autenticación se base en la existencia de contraseñas deberá existir un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad debiendo cambiarse las contraseñas con la periodicidad que se determine en el documento de seguridad, almacenándose mientras estén vigentes de forma ininteligible. Para la elaboración de dicha relación, deberá tenerse en cuenta que, un usuario autorizado es cualquier sujeto o proceso autorizado para acceder a datos o recursos para la utilización de los mismos.

5. La seguridad de los ficheros

7. Implantación y mantenimiento de un control de acceso únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones, con establecimiento de mecanismos que eviten que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.

8. Establecimiento de un procedimiento para que exclusivamente el personal autorizado para ello en el documento de seguridad pueda conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el responsable del fichero.

9. Establecimiento e implantación de un sistema de almacenamiento de soportes informáticos que contengan datos de carácter personal que permita identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad.

10. Establecimiento e implantación de un sistema de almacenamiento de gestión de soportes que garantice que, la salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero, únicamente puede ser autorizada por el responsable del fichero.

11. Implantación de un procedimiento que verifique la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos que además garanticen la reconstrucción de los datos en el estado en que se encontraban al tiempo de producirse la perdida o destrucción.

12. Establecimiento de un procedimiento para la realización de copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

¿CUÁLES SON LAS MEDIDAS DE SEGURIDAD DE NIVEL MEDIO?

MEDIDAS DE NIVEL MEDIO (Ver Esquema nivel medio en Anexo II - Pág. 204)

1. Todas las anteriormente relacionadas para el nivel básico.

2. Realizar una auditoría interna o externa sobre los sistemas de información e instalaciones de tratamiento de datos, que verifique el cumplimiento del Reglamento y de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.

3. Incluir en el documento de seguridad, además de lo previsto para el nivel básico, la identificación del responsable o responsables de seguridad, los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento y las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado.

4. Nombramiento de uno o varios Responsables de Seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad, sin que en ningún caso, esta designación suponga una delegación de la responsabilidad que corresponde al Responsable del Fichero de acuerdo con este Reglamento. Dicho Responsable de Seguridad será incluido en el Documento de Seguridad.

5. Establecer un sistema de control de acceso físico a las instalaciones donde se encuentren ubicados los sistemas de información, de manera que exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a dichos locales.

6. Para acceder al sistema de información deberá establecerse un sistema que permita identificar de forma inequívoca y personalizada a todo aquel usuario que intente acceder al sistema de información y verificar que está autorizado. Además deben estar limitadas las posibilidades de intento reiterado de acceso no autorizado al sistema de información.

7. Consignación en el registro de incidencias regulado para el nivel básico, además los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación, siendo necesaria en cualquier caso, la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de datos.

8. No podrán realizarse pruebas con datos reales de forma previa a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

9. Debe establecerse por un lado, un sistema de registro de entrada de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada, por otro lado un sistema de registro de salida de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

10. Implantación de un procedimiento y mecanismos necesarios para que, cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento,

se adopten las medidas necesarias que impidan cualquier recuperación indebida de la información almacenada en ellos.

11. Establecimiento de un procedimiento para el desechado o reutilización de soportes mediante el cual se adopten las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario.

¿CUÁLES SON LAS MEDIDAS DE SEGURIDAD DE NIVEL ALTO?

MEDIDAS DE NIVEL ALTO (Ver Esquema nivel alto en Anexo II - Pág. 205)

1. Todas las establecidas anteriormente para los niveles básico y medio.

2. Implantación de un procedimiento y medidas necesarias para que la distribución de los soportes que contengan datos de carácter personal se realice cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

3. Establecimiento de un registro de acceso a los datos personales que permita guardar, durante un período mínimo de conservación de dos años, de cada acceso, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso, si ha sido autorizado o denegado y en caso en que el acceso haya sido autorizado, que guarde la información que permita identificar el registro accedido.

4. Establecimiento de un procedimiento que garantice que el registro de los datos detallados en los párrafos anteriores estará bajo el control directo del Responsable de Seguridad sin que se pueda permitir, en ningún caso, la desactivación de los mismos.

5. Revisión periódica por el Responsable de Seguridad competente de la información de control registrada y elaboración por el mismo Responsable de Seguridad de un informe de las revisiones realizadas y los problemas detectados, al menos una vez al mes.

6. Establecimiento de un procedimiento que permita conservar una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan cumpliendo en todo caso siempre, las medidas de seguridad exigidas en este Reglamento.

7. Implantación de los mecanismos técnicos necesarios así como un procedimiento para realizar toda transmisión de datos de carácter personal a través de redes de telecomunicaciones cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

¿EN QUÉ CONSISTE EL DOCUMENTO DE SEGURIDAD?

Este es un documento de obligado cumplimiento para todo el personal con acceso a los datos de carácter personal y a los sistemas de información, en el que deben describirse las siguientes cuestiones:

- Ámbito de aplicación del documento.

- Especificación detallada de los recursos protegidos.

- Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en el Reglamento.

- Funciones y obligaciones del personal.

- Estructura de los ficheros con datos de carácter personal.

- Descripción de los sistemas de información que tratan los datos de carácter personal.

- El procedimiento de notificación, gestión y respuesta ante las incidencias.

- Los procedimientos de realización de copias de respaldo.

- Los procedimientos de realización de recuperación de los datos.

Y para los **niveles medio y alto** además deberá reflejarse:

- La identificación del Responsable o Responsables de Seguridad.

- Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio Documento de Seguridad.

- Las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado.

La disposición de estos contenidos no está tasada por la legislación vigente, de manera que el autor del mismo podrá disponer de la información obrante en él del modo que más operativo le resulte.

La disposición del Reglamento de Medidas de Seguridad obliga a:

- Mantener en todo momento el Documento de Seguridad actualizado.

5. La seguridad de los ficheros

- Revisarlo siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

- Adecuar su contenido en todo momento a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

¿EN QUÉ CONSISTE LA AUDITORÍA BIANUAL?

El Reglamento de Medidas de Seguridad establece la obligación para todos los sistemas de información e instalaciones de tratamiento de datos correspondientes a los **niveles medio y alto de seguridad**, de ser sometidos a una auditoría interna o externa, que verifique el cumplimiento del propio Reglamento, de los procedimientos y de las instrucciones vigentes en materia de seguridad de datos, al menos cada dos años.

Esta auditoría bianual, como medida de seguridad, también es exigible legalmente al que se suele denominar **nivel básico superior**, que se aplica cuando la acumulación de datos permite "obtener una evaluación de la personalidad del individuo" y que suelen identificarse con los ficheros de **marketing** que se utilizan para la obtención de perfiles mediante la fusión o cruce de datos.

Este control o auditoría puede ser realizado por un auditor externo o interno de la propia entidad auditada, si bien debe ser imparcial, objetiva e independiente y realizada por personal profesionalmente cualificado.

Tras la realización de la auditoría, es necesario elevar los resultados de la misma a un informe que, en base a datos, hechos y observaciones expresamente descritas, dictamine sobre la adecuación de las medidas y controles al Reglamento de Medidas de Seguridad, identificar las deficiencias y proponer las medidas correctoras o complementarias necesarias.

Estos informes deben ser analizados por el responsable de seguridad nombrado en la organización auditada, quien elevará las conclusiones al responsable del tratamiento o en su caso al encargado del mismo, para que adopte las medidas correctoras adecuadas. Dichas conclusiones quedarán a disposición de la Agencia Española de Protección de Datos.

Estas medidas y controles son insuficientes a la vista de lo que en la práctica suele ocurrir y sólo el establecimiento de las medidas descritas no es suficiente. En este sentido en muy frecuente que tanto el responsable del fichero como el encargado del tratamiento incurran en infracciones cometidas por sus empleados en materia de seguridad, en cuyo caso el incumplimiento de las medidas puede ser sancionado a la empresa. (Ver Anexo II - Pág. 200).

6. Los derechos de los afectados por el tratamiento de datos de carácter personal

¿CÚAL ES EL CONTENIDO DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS?

El derecho fundamental a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer.

El contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales, los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular

del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele.

Así, la Ley Orgánica de Protección de Datos de Carácter Personal reconoce al ciudadano una serie de derechos en relación con el tratamiento de sus datos de carácter personal. Junto al derecho a ser informado cuando se recogen sus datos personales, se contemplan otros derechos que permiten comprobar su veracidad y exactitud y conocer el fin para el que han sido recabados y registrados, rectificar los datos falsos o inexactos y oponerse al tratamiento de los mismos. También se contempla un derecho de impugnación de las valoraciones personales basadas en un tratamiento de datos destinado a evaluar aspectos de su personalidad, y un derecho a solicitar la indemnización de los daños causados por actos contrarios a lo dispuesto en la Ley.

Estos derechos permiten garantizar el respeto al derecho constitucional a la libertad informática o autodeterminación informática que reconoce a la persona la facultad de decidir cuándo y cómo está dispuesta a permitir que sea difundida su información personal o a difundirla ella misma, es decir, la facultad de controlar y conocer los datos que sobre ella se encuentran en soportes informáticos o susceptibles de tratamiento automatizado. Este derecho fundamental se sustenta en el consentimiento que debe prestar el ciudadano y en el conjunto de derechos o facultades contemplados en la Ley.

¿CUÁLES SON LOS CONCRETOS DERECHOS QUE TIENEN RECONOCIDOS LOS CIUDADANOS RESPECTO A LA PROTECCIÓN DE DATOS PERSONALES?

Estos derechos del afectado son concretamente: **el derecho a la información** en la recogida de datos, los derechos de **consulta, acceso, oposición, rectificación y cancelación**. Si la propia Ley no legitima automáticamente el

6. Los derechos de los afectados por el tratamiento de datos de carácter personal

tratamiento se requerirá el consentimiento del interesado, previo a la recogida o para la cesión de datos a terceros. Dentro de estos derechos también se encuentra el **derecho a no ser valorados** o considerados sobre la base exclusiva de un tratamiento de datos personales para adoptar decisiones que les afecten. Tal y como establece la Ley se trata de que los ciudadanos no tengan que verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.

Como consecuencia del derecho anterior articula la Ley un instrumento que deja en manos del ciudadano para hacer efectivo su cumplimiento. En este sentido, se otorga un **derecho a impugnar actos administrativos y/o decisiones privadas** que impliquen una valoración de su comportamiento cuyo fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad. En definitiva, se trata de evitar que mediante asociación y cruce de datos se obtengan perfiles de ciudadanos que sirvan para emitir decisiones importantes únicamente fundadas en prejuicios sobre los afectados. Se trata de evitar que el tratamiento de datos afecte seriamente la libertad de los ciudadanos de elegir o actuar.

Como último de los derechos contemplados y consecuencia necesaria de la necesidad de resarcimiento o compensación por la vulneración de cualquiera de los derechos anteriormente expuestos está el **derecho a obtener una indemnización por los daños y perjuicios** producidos ante los tribunales. Esta posibilidad además incluye el daño moral del afectado que, aunque no resulta expresamente previsto, viene siendo considerado de la misma manera que en la vulneración a los derechos al honor, intimidad y propia imagen.

¿EN QUÉ CONSISTE EL DERECHO DE INFORMACIÓN?

El responsable del fichero o tratamiento tiene la obligación de informar al ciudadano cuando pretenda acceder a

sus datos personales. Se trata de un derecho esencial en cuanto permitirá el ejercicio de otros derechos en la fase posterior de tratamiento de los datos (acceso, rectificación y cancelación y oposición).

¿CÓMO SE REGULA EL DERECHO DE INFORMACIÓN EN EL CASO DE SOLICITUD DE DATOS AL PROPIO INTERESADO?

El ciudadano al que se solicite datos personales debe ser informado por el responsable del tratamiento de los datos de las siguientes circunstancias:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Se trata de una obligación ineludible para el responsable del tratamiento de los datos, que **debe informar de modo expreso, preciso e inequívoco.** De este modo, se impone al responsable del tratamiento un comportamiento leal, transparente y abierto que permita al afectado hacerse una perfecta representación del alcance, contenido y consecuencias del suministro de los datos y de los derechos que le asisten.

6. Los derechos de los afectados por el tratamiento de datos de carácter personal

En caso de incumplimiento de esta obligación, el afectado que haya prestado su consentimiento podrá anular el mismo, sin perjuicio de las sanciones administrativas que en su caso procedan. Para el frecuente caso en que se utilicen cuestionarios u otros impresos para recoger los datos, se precisa que deberán figurar en los mismos en forma claramente legible tales menciones.

¿QUÉ EXCEPCIONES EXISTEN A LA OBLIGACIÓN DE INFORMACIÓN EN EL CASO DE SOLICITUD DE DATOS AL PROPIO INTERESADO?

No obstante, se establecen determinadas excepciones a esta obligación de información del responsable. No será necesario proporcionar información sobre el carácter obligatorio o facultativo de la respuesta a las cuestiones planteadas, sobre las consecuencias de la obtención de los datos o de la negativa a suministrarlos, ni sobre la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban. Aunque, en todo caso, la existencia de un fichero o tratamiento de datos, la finalidad de la recogida de éstos y los destinatarios de la información, así como la identidad y dirección del responsable del tratamiento o, en su caso, de su representante, son siempre circunstancias de obligada información a los interesados, sin que quepa su exclusión por el hecho de que los datos sean dados voluntariamente por los interesados y éstos conozcan su finalidad.

En el caso de ficheros de titularidad pública, el deber de información del responsable del tratamiento desaparece cuando la recogida de datos afecte a la defensa nacional, a la seguridad pública o a la persecución de infracciones penales. En este caso, el responsable del tratamiento deberá motivar adecuadamente el uso de la excepción, siendo en otro caso revisable su decisión.

El incumplimiento de este deber de informar a los afectados en la recogida de datos constituye una infracción leve.

¿CÓMO SE REGULA EL DERECHO DE INFORMACIÓN EN EL CASO DE QUE LOS DATOS NO SE RECABEN DIRECTAMENTE DEL CIUDADANO?

Cuando los datos de carácter personal no se recaban del interesado, el responsable del fichero o su representante debe informar, también de forma expresa, precisa e inequívoca, **y en los tres meses siguientes** al momento del registro de los datos, del contenido del tratamiento, de la procedencia de los datos, así como 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, de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición y de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. Este deber de información no surge si el afectado ha sido informado de tales circunstancias con anterioridad.

Se trata de una norma que pretende garantizar que el consentimiento exigido sea informado y libre.

¿QUÉ EXCEPCIONES EXISTEN A LA OBLIGACIÓN DE INFORMACIÓN EN EL CASO DE QUE LOS DATOS NO SE RECABEN DIRECTAMENTE DEL CIUDADANO?

No obstante, la Ley Orgánica de Protección de Datos también enumera para este supuesto excepciones. No hay obligación de informar al interesado:

- Cuando una ley expresamente lo prevea. La excepción será aplicable a supuestos en que el tratamiento o la cesión de los datos aparece expresamente recogida en una norma con rango de Ley, pero no a aquellos supuestos en que la Ley autorice o habilite la cesión de los datos pero no la recoja de modo expreso y taxativo en su articulado.

- Cuando el tratamiento tenga fines históricos, estadísticos o científicos.

6. Los derechos de los afectados por el tratamiento de datos de carácter personal

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

  La apreciación de tal excepción sólo será posible a través de un acto administrativo de la citada Agencia en que se decida acerca de la procedencia o improcedencia de la misma. Dicho acto implicará la tramitación del correspondiente procedimiento administrativo que, en todo caso, se iniciará por la propia solicitud del interesado. En la tramitación del procedimiento deberá requerirse al solicitante para que acredite efectivamente la desproporcionalidad del esfuerzo que conllevaría la práctica de la notificación. Los criterios que deberá valorar la Agencia son la antigüedad de los datos, el número de afectados y las medidas compensatorias que se adopten por el responsable del tratamiento. Por ello será necesario que en la fase probatoria se cuantifique realmente el coste que conllevaría la notificación y se solicite la expresión del modo en que se adoptarán, en su caso, las medidas compensatorias.

  La facultad de decisión de la Agencia se limita a determinar si, dadas las circunstancias del caso, la notificación implicase un esfuerzo desproporcionado, pero no conlleva la resolución sobre las medidas que hayan de adoptarse. En la propuesta de Resolución, además, podrá señalarse cuál sería el criterio de la Agencia para delimitar las medidas que, en su caso, pudieran ser suficientes para estimar la solicitud planteada, a fin de que el interesado pueda, en el trámite de audiencia aclarar, si lo estima necesario, las medidas propuestas o si procede proponer nuevas medidas. La Resolución del procedimiento deberá ser dictada por el Director de la Agencia Española de Protección de Datos y será susceptible de recurso contencioso-administrativo ante la Audiencia Nacional.

- Cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos

y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

El incumplimiento de este deber constituye una infracción grave.

¿QUÉ ESPECIALIDADES EXISTEN EN EL CASO DE PRESTACIÓN DE SERVICIOS DE INFORMACIÓN SOBRE SOLVENCIA PATRIMONIAL Y CRÉDITO?

Cuando se traten 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, deberá notificarse 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.

Si el interesado cursa la oportuna solicitud, 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. La obligatoriedad de la comunicación de los datos al interesado entra en juego tanto en el caso de quienes presten servicios de información sobre la solvencia patrimonial y el crédito, como en el de los que se dediquen a facilitar información relativa al cumplimiento o incumplimiento de obligaciones dinerarias.

El incumplimiento de esta obligación constituye una infracción administrativa. Se trata de una infracción continuada que sólo puede comenzar a prescribir cuando la misma cesa, lo que tiene lugar con el cumplimiento de la obligación. De otro modo, sería de mejor derecho aquél que incumple tal obligación que aquel otro que sólo se retrasa en el cumplimiento pues vería prescrita la infracción antes el que ha incumplido.

6. Los derechos de los afectados por el tratamiento de datos de carácter personal

En cuanto a la notificación de la inclusión en un fichero a los afectados, cuando el destinatario niega la recepción recae sobre el responsable del fichero la carga de acreditar la comunicación. Aunque ningún precepto legal ni reglamentario exige que la comunicación deba cursarse por correo certificado con acuse de recibo o por cualquier otro medio que deje constancia documental de la recepción, existiendo preceptos legales que imponen como obligatoria tal comunicación y que tipifican como infracción grave su incumplimiento debe concluirse de tal manera.

¿QUÉ ESPECIALIDADES TIENE EL DERECHO DE INFORMACIÓN EN EL CASO DE TRATAMIENTO CON FINES DE PUBLICIDAD Y DE PROSPECCIÓN COMERCIAL?

Para el caso de tratamiento con fines de publicidad y de prospección comercial (marketing), la Ley Orgánica de Protección de Datos precisa que cuando los datos procedan de fuentes accesibles al público, en cada comunicación que se dirija al interesado, en virtud de la obligación de información, habrá que informar del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.

¿A QUÉ REQUISITOS SE SOMETE LA NOTIFICACIÓN DE LA PRIMERA CESIÓN DE DATOS?

El responsable del fichero está obligado a informar de la primera cesión de datos a los afectados en el momento en que se efectúe, indicando, asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.

La previsión es un reflejo del principio de finalidad y del consentimiento y viene a establecer un método de control de los actos del responsable (cedente), posteriores al consentimiento prestado y que se corresponden con los fines manifestados por el mismo y con la voluntad del afectado, sin constituir una excepción a la necesidad del consentimiento del afectado. Dando por supuesto que cada cesionario que recibe los datos se convierte en

responsable del tratamiento y tiene la obligación de notificar si cede los datos, se concluye que la determinación del cesionario será exigible cuando se realice a favor de un sujeto concreto y no cuando las cesiones pueden ser realizadas de forma genérica, a modo de divulgación de la información.

Las excepciones a este deber de notificar la primera cesión, que coinciden con algunos de los supuestos en los que no existe obligación de recabar el consentimiento del afectado para la cesión, son:

- 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. Debe entenderse que la necesidad viene referida a que la cesión sea un requisito imprescindible para que la relación existente entre las partes pueda llevarse a cabo.

- 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 tienen atribuidas.

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

- Tampoco habrá que informar de esta primera cesión cuando la comunicación se efectúe previo procedimiento de disociación. En este caso, el conocimiento de los datos no puede conectarse con la persona a quien pertenecen, por lo que no puede causar perjuicio a su titular

- O cuando la cesión venga impuesta por la ley. La reserva de ley debe ser interpretada en el sentido de que el legislador no podrá, sin más, efectuar una delegación genérica de los límites del derecho fundamental a la protección de datos a favor de otro de los poderes del Estado. No cabe que un Reglamento imponga la cesión.

6. Los derechos de los afectados por el tratamiento de datos de carácter personal

¿EN QUÉ CONSISTE EL DERECHO DE CONSULTA AL REGISTRO GENERAL DE PROTECCIÓN DE DATOS?

La Ley Orgánica de Protección de Datos permite que cualquier persona pueda conocer la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento, solicitando la información oportuna al Registro General de Protección de Datos.

El derecho de consulta permite acceder de forma amplia al Registro, es decir, permite informarse sobre un tratamiento, su finalidad y la identidad de su responsable, aunque no permite comprobar la exactitud y veracidad de los datos en él almacenados respecto de una situación concreta. Se trata de un derecho de información de carácter general, sobre datos objetivos, que se atribuye a cualquier persona, y para cuyo ejercicio no parece necesario acreditar un interés legítimo.

La consulta al Registro General de Protección de Datos es pública y gratuita y puede realizarse "on line" en la página web de la Agencia de Protección de Datos. El Registro es un órgano integrado en la Agencia de Protección de Datos, donde se inscriben los tratamientos notificados (ficheros de titularidad pública y privada) y, en particular, los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

El Registro es el órgano al que corresponde velar por la publicidad de la existencia de los ficheros con el objeto de hacer posible el ejercicio de los derechos reconocidos a los afectados.

¿EN QUÉ CONSISTE EL DERECHO DE ACCESO?

El afectado tiene derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal objeto de tratamiento. Podrá conocer el origen de dichos datos, las comunicaciones realizadas o lo que se prevea hacer de los mismos. El ejercicio del derecho de acceso permitirá comprobar si se han cumplido las prescripciones legales o se han dado eventuales incumplimientos. Con referencia al origen de los datos debe matizarse que, aunque ya deben conocerse por el afectado, bien porque los proporcionó el mismo, bien porque le fue comunicado, esta previsión permitirá al afectado contrastar lo que ya comunicó o que le fue comunicado, así como, en su caso, conocer datos no conocidos en virtud de las excepciones contempladas. Con relación a las comunicaciones realizadas o que se prevean hacer, ha de entenderse que la norma se refiere tanto a aquellas comunicaciones realizadas con el consentimiento del afectado, incluidas aquellas que no hayan atendido a lo dispuesto en la Ley (v.g. finalidades distintas) como aquellas exceptuadas de él y las que se hayan realizado sin mediar el consentimiento siendo necesario.

El Real Decreto 1332/1994 precisa el contenido de la información que deberá proporcionarse a quien ejercite tal derecho de acceso. Incluye 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. En el caso de que los datos provengan de fuentes diversas, deberán especificarse las mismas, identificando la información que proviene de cada una de ellas.

En cuanto a la forma en que ha de proporcionarse la información, cualquiera que sea el soporte en que se facilite, ha de ser en forma legible e inteligible, previa trascripción en claro de los datos del fichero, en su caso. La información podrá obtenerse bien mediante la mera consulta de los datos por medio de su visualización, bien mediante la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada

o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos. El afectado podrá optar por uno o varios de los sistemas de consulta del fichero que se han relacionado o por cualquier otro procedimiento que sea adecuado a la configuración e implantación material del fichero, ofrecido por el responsable del mismo. En todo caso, será el afectado quien decida la modalidad de información sin que el responsable del fichero pueda oponerse a la forma elegida salvo que existan imposibilidades técnicas.

Además, hay que tener en cuenta que la Ley Orgánica de Protección de Datos establece una limitación temporal al ejercicio del derecho de acceso, que **únicamente podrá ejercitarse a intervalos no inferiores a doce meses, salvo** que el interesado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarse antes. Si se entiende que cualquier petición producida antes de expirar el plazo ha de ser calificada como **interés legítimo** si en ese plazo ha tenido lugar algún **cambio en los datos personales** que exija ser reflejado en el fichero, de manera que se cumplan los principios de exactitud y de actualización, el responsable del fichero debe limitarse a verificar si la variación del dato ha de realizarse antes del dilatado plazo.

El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información solicitada, así como mantener los datos inexactos o no efectuar las rectificaciones o cancelaciones que procedan, constituye infracción grave. No atender u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación y oposición constituye infracción muy grave.

¿CUÁLES SON LAS REGLAS GENERALES PARA EL EJERCICIO DEL DERECHO DE ACCESO?

El acceso puede denegarse en los siguientes supuestos:

1. En el caso de acceso a los datos de carácter personal registrados en ficheros de titularidad pública, cuando se dé alguno de los siguientes supuestos, en los que se establecen excepciones relativas a los ficheros de las Fuerzas y Cuerpos de Seguridad del Estado y a los ficheros de la Hacienda Pública.

a) Los responsables de los ficheros que contengan determinados datos podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando. Se trata de datos referidos a:

- La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

- La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias, y de los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que correspondan a los órganos jurisdiccionales.

- Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

6. Los derechos de los afectados por el tratamiento de datos de carácter personal

b) Los responsables de los ficheros de la Hacienda Pública también podrán denegar el ejercicio de tales derechos cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado está siendo objeto de actuaciones inspectoras.

El afectado al que se deniegue, total o parcialmente, el ejercicio de los citados derechos podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.

2. En el caso de datos registrados en ficheros de titularidad privada, se señala que únicamente se denegará el acceso cuando la solicitud sea formulada por persona distinta del afectado. En particular, el responsable del fichero podrá denegar el acceso a los datos de carácter personal cuando el derecho se haya ejercitado en un intervalo inferior a doce meses y no se acredite un interés legítimo al efecto, debidamente justificado, así como cuando la solicitud sea formulada por persona distinta del afectado.

Para el caso de tratamiento con fines de publicidad y de prospección comercial, en el ejercicio del derecho de acceso los interesados tendrán derecho a conocer el origen de sus datos de carácter personal, así como del resto de información.

En cuanto al procedimiento para ejercitar el derecho de acceso, se establece la gratuidad del ejercicio de los derechos de oposición, acceso, rectificación y cancelación.

¿CUÁLES SON LAS REGLAS GENERALES PARA EL EJERCICIO DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN Y CANCELACIÓN?

a) Los derechos de acceso, rectificación y cancelación de datos y oposición son personalísimos y serán ejercidos por el afectado frente al responsable del fichero, sin otras limitaciones que las que se prevén en la normativa. Se persigue, en definitiva, que únicamente el interesado pueda decidir si quiere ejercitar los derechos que la Ley le otorga.

Se permite no obstante que actúe el representante legal del afectado cuando éste se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de tales. A estos efectos, tanto la identidad del afectado como la condición de representante legal deberá acreditarse frente al responsable.

b) Los derechos de acceso, rectificación y cancelación y oposición son derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

c) El ejercicio de los derechos debe llevarse a cabo mediante solicitud dirigida al responsable del fichero. A estos efectos, el interesado tendrá que utilizar un medio que permita acreditar el envío y la recepción de la solicitud. La solicitud debe contener los datos personales del interesado y fotocopia del DNI del mismo o, en su caso, representante legal, un domicilio a efectos de notificación; la petición en que se concreta la solicitud (acceso, rectificación, cancelación u oposición), los documentos acreditativos de la eventual petición, si existen, la fecha y la firma del solicitante. El responsable del fichero tiene la obligación de contestar la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado en sus ficheros, debiendo utilizar cualquier medio que permita acreditar el envío y la recepción. Si la solicitud no reúne los requisitos especificados en el apartado tercero, el responsable del fichero debe solicitar la subsanación de los mismos. En todo caso, el

responsable tiene la obligación de adoptar las medidas oportunas para garantizar que todas las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

¿CUÁL ES EL PROCEDIMIENTO PARA EJERCITAR EL DERECHO DE ACCESO?

El ejercicio del derecho de acceso consiste en la petición de información sobre los datos personales incluidos en un fichero. A través del mismo, el interesado solicita que se le facilite gratuitamente el acceso a los oportunos ficheros y que se le remita determinada información sobre los mismos. Este derecho se ejerce ante el responsable del fichero (organismo público o entidad privada) que es quien dispone de los datos:

1º) Al ejercitar el derecho de acceso, el afectado podrá optar por uno o varios de los siguientes sistemas de consulta del fichero, siempre que la configuración o implantación material del fichero lo permita:

a) Visualización en pantalla.

b) Escrito, copia o fotocopia remitida por correo.

c) Telecopia.

d) Cualquier otro procedimiento que sea adecuado a la configuración e implantación material del fichero, ofrecido por el responsable del mismo.

2º) El responsable del fichero resolverá sobre la solicitud de acceso en el **plazo máximo de un mes**, a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición de acceso,

ésta podrá entenderse desestimada a los efectos de la interposición de reclamación ante la Agencia de Protección de Datos. Es importante destacar que aunque no disponga de datos de carácter personal del afectado, el responsable está obligado a comunicárselo en el mismo plazo.

3º) Si la **resolución** fuera **estimatoria, el acceso se hará efectivo en el plazo de los diez días siguientes a la notificación** de aquella.

4º) El responsable del fichero podrá denegar el acceso a los datos de carácter personal cuando el derecho se haya ejercitado en un intervalo inferior a doce meses y no se acredite un interés legítimo al efecto, debidamente justificado, así como cuando la solicitud sea formulada por persona distinta del afectado.

Tratándose de ficheros de titularidad pública se podrá denegar el acceso en los supuestos en los que se establecen excepciones relativas a los ficheros de las Fuerzas y Cuerpos de Seguridad del Estado y a los ficheros de la Hacienda.

¿EN QUÉ CONSISTEN LOS DERECHOS DE RECTIFICACIÓN Y CANCELACIÓN?

El interesado tiene derecho a solicitar la rectificación o cancelación de los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la Ley orgánica de protección de datos y, en particular, cuando tales datos resulten inexactos o incompletos. Si los datos de carácter personal del afectado son inexactos o incompletos, inadecuados o excesivos, podrá éste solicitar del responsable del fichero la rectificación o, en su caso, la cancelación de los mismos. Estos derechos vienen a concretar el principio sobre calidad de los datos, conforme al cual los datos de carácter personal deberán ser exactos y puestos al día de manera que respondan con veracidad a la situación actual del afectado.

6. Los derechos de los afectados por el tratamiento de datos de carácter personal

Realmente, la rectificación tendrá cabida en los supuestos en que los datos resulten inexactos o incompletos, mientras la cancelación procederá en los casos en que el tratamiento de los datos no se ajuste a la ley. Conforme a la Agencia Española de Protección de Datos, el modelo de ejercicio del derecho de rectificación se utilizará para el caso en que se deban rectificar datos inexactos o incompletos en un fichero, siendo necesario aportar la documentación que acredite el carácter inexacto o incompleto de los datos. El modelo para el ejercicio del derecho de cancelación se utilizará por el afectado cuando desee cancelar y bloquear datos inexactos existentes en un fichero. También será necesario aportar la documentación que acredite al responsable del fichero de carácter inexacto de los datos que figuran en los ficheros.

En todo caso, **el responsable del tratamiento debe hacer efectivo este derecho en el plazo de diez días**. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión. De este modo, la cancelación no se concibe como supresión o destrucción sino como su retirada del conocimiento público general a través de su bloqueo, quedando limitado su acceso a los órganos administrativos o judiciales para delimitar responsabilidades nacidas de su tratamiento. Sólo cuando hayan transcurridos los plazos previstos a estos efectos, podrá procederse a la eliminación de los datos.

En los casos en que siendo procedente la cancelación de los datos, no sea posible su extinción física, tanto por razones técnicas como por causa del procedimiento o soporte utilizado, el responsable del fichero procederá al **bloqueo de los datos**, con el fin de impedir su ulterior proceso o utilización. Se exceptúa, no obstante, el supuesto en el que se demuestre que los datos han sido recogidos o registrados por medios fraudulentos, desleales o ilícitos, en cuyo caso la cancelación de los mismos comportará siempre la destrucción del soporte en el que aquéllos figuren.

La Agencia Española de Protección de Datos considera que existirán determinados supuestos en que la cancelación o bien no podrá tener lugar, dada la obligación de conservación impuesta por la Ley, o bien deberá suponer una fase previa del bloqueo de datos que, produciendo unos efectos similares al borrado físico de los mismos, salvo en determinadas circunstancias, no implicará automáticamente ese borrado.

El sujeto obligado a rectificar o cancelar es tanto el responsable del fichero como el encargado del tratamiento, que es aquél que trate datos personales por cuenta del responsable del tratamiento. Además, no sólo está obligado a rectificar o cancelar los datos. Si los datos rectificados o cancelados hubieran sido comunicados previamente, tiene el deber de notificar la rectificación o cancelación efectuada a quien se hayan comunicado. Adicionalmente el cesionario, si mantiene el tratamiento de los datos, deberá proceder a la cancelación o rectificación oportuna. Esta notificación será vinculante sin que el cesionario pueda oponerse a la rectificación o cancelación ya que su objetivo es el cumplimiento del principio de veracidad. Por otro lado, y aunque la norma no lo prevé, también parece necesaria la comunicación de la realización de estos trámites al afectado.

En cuanto al plazo para realizar esta comunicación, se precisa que si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero debe notificar la rectificación o cancelación efectuada al cesionario, en idéntico plazo que el que dispone para hacer efectivos tales derechos, para que éste, a su vez, la lleve a cabo en su fichero. Por analogía debe considerarse que este es el plazo del que dispone el cesionario para efectuar la oportuna rectificación o cancelación.

Como ocurre con el derecho de acceso, los responsables de los ficheros podrán denegar la rectificación o cancelación en los mismos supuestos que el derecho de acceso. En el caso de acceso a los datos de carácter personal registrados en ficheros de titularidad pública, cuando se dé alguno de los siguientes supuestos:

6. Los derechos de los afectados por el tratamiento de datos de carácter personal

- Los responsables de los ficheros que contengan determinados datos podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

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

Se establece una disposición especial para el supuesto de denegación en el caso de ficheros mantenidos por Cuerpos de Policía, o por las Administraciones tributarias autonómicas. En este caso el afectado al que se deniegue, total o parcialmente, el ejercicio de los citados derechos podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de cada Comunidad Autónoma, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.

Sin perjuicio del ejercicio del derecho de cancelación, existe la obligación de conservar los datos de carácter personal durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

Contra la resolución por la que el responsable del fichero acuerde el bloqueo de los datos procederá reclamación ante el Director de la Agencia de Protección de Datos.

Mantener los datos inexactos o no efectuar las rectificaciones o cancelaciones que procedan, constituye infracción grave. No atender u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación y oposición constituye infracción muy grave.

¿CUÁL ES EL PROCEDIMIENTO PARA EJERCITAR LOS DERECHOS DE RECTIFICACIÓN Y CANCELACIÓN?

Los derechos de rectificación y cancelación **se harán efectivos** por el responsable del fichero **dentro de los diez días siguientes al de la recepción de la solicitud**. Se precisa que si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá notificar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que éste, a su vez, la lleve a cabo en su fichero.

La solicitud de rectificación debe indicar el dato que es erróneo y la corrección que debe realizarse y debe ir acompañada de la documentación justificativa de la rectificación solicitada, salvo que la misma dependa exclusivamente del consentimiento del interesado. En la solicitud de cancelación, el interesado deberá indicar si revoca el consentimiento otorgado, en los casos en que la revocación proceda, o si, por el contrario, se trata de un dato erróneo o inexacto, en cuyo caso deberá acompañar la documentación justificativa.

Para el caso en que el responsable del fichero considere que no procede atender la solicitud del afectado, debe comunicárselo motivadamente dentro del plazo de los diez días siguientes al de la recepción de la misma, a fin de que por éste se pueda hacer uso de la reclamación. Transcurrido el plazo de diez días sin que de forma expresa se responda a la solicitud de rectificación o cancelación, ésta podrá entenderse desestimada a los efectos de la interposición de la reclamación que corresponda.

La cancelación exige el borrado físico de los datos, sin que sea suficiente a estos efectos una marca lógica o el mantenimiento de otro fichero alternativo en el que se registren las bajas producidas. En los casos en que siendo procedente la cancelación de los datos, no sea posible su extinción física, tanto por razones técnicas como por causa del procedimiento o soporte utilizado, el responsable del fichero procederá al bloqueo de los datos, con el fin de impedir su ulterior proceso o utilización.

6. Los derechos de los afectados por el tratamiento de datos de carácter personal

Se exceptúa, no obstante, el supuesto en el que se demuestre que los datos han sido recogidos o registrados por medios fraudulentos, desleales o ilícitos, en cuyo caso la cancelación de los mismos comportará siempre la destrucción del soporte en el que aquéllos figuren.

¿QUÉ NORMAS ESPECIALES RESULTAN APLICABLES A LOS FICHEROS DE PRESTACIÓN DE SERVICIOS DE INFORMACIÓN SOBRE SOLVENCIA PATRIMONIAL?

Existen algunas normas especiales relativas al ejercicio de los derechos de acceso, rectificación y cancelación en el caso de los ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito. El responsable de un fichero de prestación de servicios de solvencia patrimonial y crédito con datos obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el afectado o con su consentimiento, estará obligado a satisfacer, en cualquier caso, los derechos de acceso, rectificación y cancelación. Las personas y entidades a las que se presta el servicio únicamente estarán obligadas a comunicar al afectado aquellos datos relativos al mismo a los que ellas tengan acceso y a comunicar la identidad del responsable del fichero común para que pueda completar el ejercicio de sus derechos.

El responsable del fichero común en el que se traten automatizadamente datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés, ante una solicitud de ejercicio del derecho de acceso, deberá comunicar al afectado todos los datos relativos al mismo que obren en el fichero. Cualquier otra entidad participante en el sistema, ante tal solicitud, deberá comunicar al afectado todos los datos relativos al mismo a los que ella pueda acceder, así como la identidad del responsable del fichero común para que pueda completar el ejercicio de su derecho de acceso.

Si la solicitud del ejercicio de los derechos de rectificación o cancelación de datos se dirige al responsable del fichero común, éste tomará las medidas oportunas para 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 cinco días**, procederá a la rectificación o cancelación cautelar de los mismos.

Si la solicitud del ejercicio de los derechos de rectificación o cancelación de datos se dirige a cualquier otra entidad participante en el sistema y hace referencia a datos que dicha entidad haya facilitado al fichero común, procederá a la rectificación o cancelación de los mismos en sus ficheros y a notificarlo al responsable del fichero común en **el plazo de cinco días**. Si la solicitud hace referencia a datos que la entidad no hubiera facilitado al fichero común, dicha entidad informará al afectado sobre este hecho, proporcionándole, además, la identidad del responsable del fichero común para que pueda completar el ejercicio de sus derechos.

En los ficheros de prestación de servicios de información de solvencia patrimonial y crédito, cualquiera que sea el origen de los datos, cuando el afectado lo solicite el responsable del fichero común deberá cumplir la obligación de facilitar, las evaluaciones y apreciaciones que sobre el afectado se hayan comunicado en los últimos seis meses y el nombre y dirección de los cesionarios.

¿QUÉ NORMAS ESPECIALES RESULTAN APLICABLES A LOS FICHEROS CON FINES DE PUBLICIDAD, PROSPECCIÓN COMERCIAL O MARKETING?

El responsable del fichero que presta el servicio de publicidad estará obligado a satisfacer los derechos de acceso, rectificación y cancelación. En este caso, la entidad beneficiaria de la publicidad está obligada a indicar al afectado la identidad del responsable del fichero del que provienen los datos. A tal efecto, se entenderá suficiente que dicha información se haga constar en la campaña publicitaria.

6. Los derechos de los afectados por el tratamiento de datos de carácter personal

Por otro lado, se establece que cuando el interesado manifieste su deseo de no recibir publicidad, y no ejerza expresamente el derecho de cancelación el responsable del fichero podrá conservar los mínimos datos imprescindibles para identificarlo y adoptar las medidas necesarias que eviten el envío de publicidad.

¿EN QUÉ CONSISTE EL DERECHO DE OPOSICIÓN?

En todos los casos en que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal.

A estos efectos, el consentimiento del interesado no es necesario 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.

- 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.

- Tenga por finalidad proteger un interés vital del interesado debido a que el tratamiento resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios.

- 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.

Pues bien, en estos supuestos, si el afectado efectúa la oportuna solicitud, el responsable deberá excluir del tratamiento los datos relativos al solicitante. Parece que el objetivo es que el afectado pueda oponerse a cualquier posible tratamiento de datos, cuando dicho tratamiento no requiera su consentimiento. Además, se contempla la comunicación a la Agencia Española de Protección de Datos u organismo autonómico competente de la denegación, total o parcial, del ejercicio del derecho de oposición.

El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición constituyen infracción grave. No atender u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación y oposición constituye infracción muy grave.

¿QUÉ NORMAS ESPECIALES RESULTAN APLICABLES A LOS FICHEROS CON FINES DE PUBLICIDAD Y DE PROSPECCIÓN COMERCIAL Y A LOS QUE CONSTEN EN EL CENSO PROMOCIONAL?

La Ley Orgánica de Protección de Datos regula el derecho de oposición en supuestos especiales relativos al tratamiento de datos con fines de publicidad y de prospección comercial y a los que consten.

En el primer caso, se establece que 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.

6. Los derechos de los afectados por el tratamiento de datos de carácter personal

En el segundo supuesto, relativo a datos incluidos en las fuentes de acceso público, se establece el derecho de los afectados a exigir gratuitamente la exclusión de la totalidad de sus datos personales que consten en el censo promocional por las entidades encargadas del mantenimiento de dichas fuentes.

La atención a la solicitud de exclusión de la información innecesaria o de inclusión de la objeción al uso de los datos para fines de publicidad o venta a distancia deberá realizarse en el plazo de diez días respecto de las informaciones que se realicen mediante consulta o comunicación telemática y en la siguiente edición del listado cualquiera que sea el soporte en que se edite. Con referencia a esta cuestión ha de tenerse en cuenta que la Ley Orgánica de Protección de Datos se remite al desarrollo reglamentario de los procedimientos por los que los interesados podrán solicitar no aparecer en el censo promocional. Se especifica que entre estos procedimientos, que serán gratuitos para los interesados, se incluirá el documento de empadronamiento y que trimestralmente se editará la lista actualizada del censo promocional, excluyendo los nombres y domicilios de los que así lo hayan solicitado. En este punto, se contempla que pueda exigirse una contraprestación por la facilitación de la citada lista en soporte informático.

¿CUÁL ES EL PROCEDIMIENTO PARA EL EJERCICIO DEL DERECHO DE OPOSICIÓN?

Conforme al modelo oficial de la Agencia Española de Protección de Datos, para el ejercicio del derecho de oposición, el afectado debe exponer, junto a los datos del responsable del fichero y, en su caso, los del representante legal, la situación en que se produce el tratamiento de sus datos personales y enumerar los motivos por los que se opone al mismo. El afectado deberá acreditar documentalmente la situación descrita.

También existe un modelo oficial sobre ejercicio del derecho de exclusión de la utilización de los datos para fines de publicidad y prospección comercial, que contempla la petición de supresión total o parcial de los datos personales incluidos en algunas fuentes de acceso al público como son el Censo Promocional, los listados de Colegios

Profesionales y los repertorios telefónicos. En este caso, se contempla la obligación de notificar por escrito al afectado el resultado de la exclusión practicada. Adicionalmente, para el caso en que los datos objeto de exclusión hubieran sido comunicados previamente, se prevé que se notifique al responsable del fichero la exclusión practicada con el objetivo de que éste proceda a hacer las correcciones oportunas para que se respete el principio de calidad de los datos.

Por último, existe un último modelo sobre derecho de exclusión en los repertorios telefónicos de acceso público. A través del mismo, puede solicitarse que se proceda gratuitamente a la exclusión total o parcial de los datos relativos al interesado que se encuentren en los repertorios de abonados de servicios telefónicos y de telecomunicación, ya sean impresos en papel o disponibles por otros medios de la compañía en cuestión. Destaca que el modelo incluye la petición del afectado de que sus datos personales no sean cedidos a ninguna persona, física o jurídica, así como que su utilización se limite exclusivamente a la relación contractual que mantenga con la entidad en cuestión, por ser la finalidad para la que fueron recogidos.

¿EN QUÉ CONSISTE EL DERECHO DE IMPUGNACIÓN DE VALORACIONES PERSONALES?

La Ley orgánica de protección de datos contempla el denominado derecho de impugnación de valoraciones. Los ciudadanos 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 de datos destinado a evaluar determinados aspectos de su personalidad.

Han de darse, por tanto, dos requisitos para que sea aplicable: que produzca efectos jurídicos o le afecte de manera significativa y que se base sólo en un tratamiento destinado a evaluar aspectos de su personalidad.

6. Los derechos de los afectados por el tratamiento de datos de carácter personal

En lo que respecta a la producción de efectos jurídicos, cabe predicar una interpretación amplia, conforme a la cual lo será aquella que afecte desde cualquier punto de vista la esfera personal de los derechos fundamentales de las personas y las libertades públicas. En torno a la afección de manera significativa, que dependerá de la persona y circunstancias concretas, su apreciación será susceptible de revisión jurisdiccional.

En relación al segundo requisito se advierte que, si existiera cualquier otro argumento añadido al tratamiento destinado a evaluar aspectos de su personalidad, no sería posible aplicar el mismo. Ha de concluirse al respecto que tales informaciones complementarias tendrán que tener un nivel de calidad suficiente como para evitar la aplicación.

A continuación, la Ley permite al interesado impugnar o combatir los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.

En el ejercicio de este derecho, el afectado podrá solicitar información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto. La iniciativa del afectado le habilitará para obtener cualquier información sobre los criterios de valoración y del programa utilizado en el tratamiento. La impugnación es trascendental si se tiene en cuenta que no está tipificada como infracción administrativa este tipo de conducta.

Como cláusula de cierre, se indica que, en definitiva, la valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado. De este modo cualquier negativa del afectado impedirá dicha utilización.

¿EN QUÉ CONSISTE EL DERECHO A INDEMNIZACIÓN?

La Ley Orgánica de Protección de Datos contempla expresamente el derecho de los afectados a reclamar al responsable del fichero o al encargado del tratamiento los posibles daños y perjuicios que les haya causado el incumplimiento de la Ley en el tratamiento de sus datos de carácter personal.

Cuando la lesión provenga de organismos públicos la indemnización se exigirá de acuerdo a la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas. Cuando la lesión provenga de entidades privadas se solicitará ante la jurisdicción ordinaria. A estos efectos, ante el silencio de la Ley, parece claro que no es necesario reclamar previamente ante la Agencia Española de Protección de Datos para acudir a los Tribunales.

Cosa distinta es que sea conveniente en orden a obtener medidas preventivas o que terminen con la agresión, o a obtener pruebas que podrán utilizarse en el oportuno procedimiento.

Los requisitos para que pueda solicitarse la indemnización son dos: el incumplimiento de la Ley Orgánica de Protección de Datos y un daño o lesión en los bienes o intereses del afectado. Se viene admitiendo el resarcimiento del daño moral en términos análogos a los previstos para el derecho al honor, intimidad y propia imagen.

¿EN QUÉ CONSISTE LA PROTECCIÓN CONSTITUCIONAL DE LOS DATOS DE CARÁCTER PERSONAL?

El artículo 18.4 de la Constitución española incorpora una garantía constitucional para responder a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona. Además de un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, es también, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos. La garantía de la intimidad, latu sensu, adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona.

La llamada libertad informática es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención. En efecto, el articulo 18.4 en su último inciso establece las limitaciones al uso de la informática para garantizar el pleno ejercicio de los derechos, lo que significa que el artículo citado es, por así decirlo, un derecho instrumental ordenado a la protección de otros derechos fundamentales. Éste no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, sino que además, consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona -a la privacidad - pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos.

¿EN QUÉ CONSISTE LA PROTECCIÓN CIVIL DE LOS DATOS DE CARÁCTER PERSONAL?

Además de la posible responsabilidad contractual y extracontractual se prevé el cauce impugnatorio, tras el reconocimiento del derecho del perjudicado a ser indemnizado, ante la jurisdicción ordinaria. Los jueces y tribunales civiles son los competentes para reclamar las indemnizaciones.

¿EN QUÉ CONSISTE LA PROTECCIÓN PENAL DE LOS DATOS DE CARÁCTER PERSONAL?

El Código Penal de 1995 no recoge un sistema unitario de delitos relacionados con los sistemas informáticos (el llamado cibercrimen), pero si tipifica determinados supuestos:

- El acceso indebido y el ataque a los sistemas de información.

- La denuncia del agraviado y perdón del ofendido.

- Considera reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero, sancionando, en consecuencia, la estafa informática.

- El uso de equipo terminal de telecomunicación.

- Castiga la causación de daños al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

¿EN QUÉ CONSISTE LA PROTECCIÓN ADMINISTRATIVA DE LOS DATOS DE CARÁCTER PERSONAL?

Ley Orgánica de Protección de Datos establece una serie de obligaciones en aras a la protección de los datos personales contenidos en ficheros automatizados que poseen empresas y administraciones públicas, y que son tratadas por éstas con diferentes finalidades (gestión de personal, proveedores, clientes, campañas de publicidad, etc.):

7. La protección de los datos de carácter personal

1. Legalización: Los ficheros de datos de carácter personal deben estar inscritos y legalizados ante la Agencia Española de Protección de Datos.

2. Legitimación: Los datos de carácter personal recogidos por la empresa no sólo deben contar con el consentimiento del afectado (principio del consentimiento del afectado) sino que también han de cumplir una serie de principios básicos: principio de información y principio de calidad de los datos.

Si la empresa que almacena y trata datos de carácter personal cumple con los principios básicos, facilita al interesado el ejercicio de sus derechos en los plazos y en los extremos señalados por la ley (derecho a solicitar y obtener gratuitamente información de sus datos sometidos a tratamiento, la modificación, cancelación u oposición a su tratamiento o cesión, el origen de dichos datos, así como las comunicaciones realizadas y las que se prevén realizar) y legaliza el fichero ante el Registro de la Agencia de Protección de Datos, estableciendo unas medidas de seguridad para la protección del mismo, estará totalmente segura de no incurrir en las infracciones previstas. Además, hay que tener en cuenta las precauciones a adoptar en el caso de que los datos de carácter personal vayan a ser cedidos a otras empresas, o bien cuando el tratamiento de estos datos se va a efectuar por cuenta de tercero, ya que deberán realizarse contratos específicos.

El cumplimiento de cada una de estas obligaciones tan sólo exige un pequeño esfuerzo de las empresas y profesionales, que junto al asesoramiento adecuado, evitará consecuencias negativas y la imposición de duras sanciones económicas. En este sentido, la Agencia de Protección de Datos es el ente público encargado de velar por el cumplimiento de la legislación en materia de protección de datos disponiendo para ello del Registro de Protección de Datos, en el que el empresario ha de inscribir todos los ficheros que contengan datos personales. A todos estos efectos, se contempla la posibilidad de reclamar ante la Agencia de Protección de Datos, cuyas resoluciones son impugnables ante la jurisdicción contencioso-administrativa.

¿EN QUÉ CONSISTE LA PROTECCIÓN INTERNACIONAL DE LOS DATOS DE CARÁCTER PERSONAL?

En la transmisión de datos de carácter personal a nivel internacional debe garantizarse que los niveles de protección son equivalentes en el lugar de origen y de destino (principios de puerto seguro). Así se prevé que no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

No obstante, esta regla tiene excepciones:

a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.

b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.

c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico o la gestión de servicios sanitarios.

d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.

f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.

g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.

h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público (tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias).

i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.

k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

Además, las empresas españolas que puedan establecer relaciones con misiones diplomáticas extranjeras en España estarán sometidas a la Ley Orgánica de Protección de Datos, y en concreto en los supuestos en que dichas

relaciones jurídicas impliquen la comunicación o cesión de datos personales (por ejemplo, de sus empleados) que consten en ficheros o tratamientos de los que aquéllas sean responsables, debiendo en tal supuesto considerarse que la comunicación de datos se estará efectuando al Estado del que la misión sea representante y, en consecuencia, se estará en presencia de una transferencia internacional de datos.

Con carácter general, habrá transferencia internacional de datos en toda transmisión de los mismos fuera del territorio español. En particular, se consideran como tales las que constituyen una cesión o comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero.

Así, las transferencias internacionales de datos efectuadas desde España están sometidas a la obtención de autorización del Director de la Agencia Española de Protección de Datos cuando las mismas se vayan a efectuar a países que no proporcionan un nivel de protección equivalente al de la Ley Orgánica de Protección de Datos y no concurra uno de los supuestos excepcionales previstos en la misma.

8. La Agencia Española de Protección de Datos

¿QUÉ ES LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS?

La Agencia de Protección de Datos es un ente independiente encargado de velar por el cumplimiento de la legislación sobre protección de datos personales y privacidad, controlando su aplicación (www.agenciaprotecciondatos.org).

Nuestra Ley ha optado por un régimen de protección de datos de carácter personal respecto de los que figuren en ficheros automatizados, tanto de titularidad pública como privada, así como las modalidades de su uso posterior. Y en dicho régimen su dimensión institucional es la referida a la Agencia de Protección de Datos y a los órganos que en ella se integran, tanto de dirección, como operativos e Inspección de Protección de Datos. Además, los puestos de trabajo de los órganos y servicios que integren la Agencia de Protección de Datos serán desempeñados por funcionarios de las Administraciones públicas y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo. Este personal está obligado a guardar secreto de los datos de carácter personal de que conozca en el desarrollo de su función.

En el ejercicio de sus funciones públicas, y en defecto de lo que disponga la Ley Orgánica de Protección de Datos y sus disposiciones de desarrollo, la Agencia de Protección de Datos actuará de conformidad con la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En sus adquisiciones patrimoniales y contratación estará sujeta al derecho privado.

¿QUÉ FUNCIONES Y POTESTADES SE ATRIBUYEN A LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS?

En lo que respecta a las funciones y potestades atribuidas a la Agencia de Protección de Datos, con carácter general se le encomienda velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial respecto a los derechos de información, acceso, rectificación y cancelación de datos. Y en

cuanto especificación de esta función de carácter tuitivo en orden a la protección de datos personales, a continuación se le atribuyen tanto funciones de intervención o control respecto a ciertos sujetos y actividades como funciones registrales y consultivas. Se trata de un conjunto de funciones especializadas en cuanto a su objeto, la protección de los datos personales y, además, de funciones de carácter público, al determinar que la Agencia de Protección de Datos actuará de conformidad con la Ley de Procedimiento Administrativo, sin perjuicio de que sus adquisiciones patrimoniales y contratación estén sometidas al Derecho privado. En correspondencia con el carácter público de sus funciones, la Agencia de Protección de Datos dispone de potestades administrativas expresamente atribuidas por dicha Ley:

En primer lugar, la potestad de investigación o de inspección para obtener información y, en su caso, pruebas sobre los hechos que contravengan lo dispuesto en la Ley.

En segundo término, la potestad sancionadora.

En tercer lugar, una potestad de resolución de las reclamaciones de los afectados por incumplimiento de las previsiones de dicha Ley.

Y, por último, una potestad normativa, ceñida en lo esencial a dictar las instrucciones precisas para adecuar los tratamientos automatizados a los principios de la Ley.

De lo que se acaba de exponer se desprende un rasgo significativo de la Agencia de Protección de Datos: el carácter básicamente preventivo de sus funciones en orden a la protección de datos personales. El legislador, sin excluir en modo alguno el recurso último a los órganos jurisdiccionales para la tutela de los derechos individuales, no ha querido sin embargo que la protección de datos personales frente al uso de la informática se lleve a cabo exclusivamente en la vía judicial, esto es, cuando ya se ha producido una lesión del derecho fundamental. Por el contrario, ha querido que dicha protección se lleve a cabo mediante el ejercicio por la Agencia de Protección de

8. La Agencia Española de Protección de Datos

Datos, con carácter básicamente preventivo, de las funciones de control de los ficheros tanto de titularidad pública como privada que la Ley le atribuye y, en su caso, a través de las reclamaciones de los afectados ante la Agencia de Protección de Datos, las que provocarán la posterior actuación de este órgano. Cabe estimar que existe una correspondencia entre las funciones y potestades que la Ley ha atribuido a la Agencia de Protección de Datos y el carácter preventivo de sus actuaciones. Pues es este carácter tuitivo o preventivo el que, en última instancia, justifica la atribución de tales funciones y potestades a la Agencia de Protección de Datos para asegurar, mediante su ejercicio, que serán respetados tanto los límites al uso de la informática como la salvaguardia del derecho fundamental a la protección de datos personales en relación con todos los ficheros, ya sea de titularidad pública o privada.

Además, la Agencia de Protección de Datos contará, para el cumplimiento de sus fines, con las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado, los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo y cualesquiera otros que legalmente puedan serle atribuidos. La Agencia de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno para que sea integrado, con la debida independencia, en los Presupuestos Generales del Estado.

Son funciones de la Agencia de Protección de Datos:

a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.

c) Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley.

d) Atender las peticiones y reclamaciones formuladas por las personas afectadas.

e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.

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

g) Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley.

h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.

i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.

k) Redactar una memoria anual y remitirla al Ministerio de Justicia.

l) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

m) Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad de ejercer tareas disciplinarias ante las infracciones de Administraciones Públicas.

n) Cuantas otras le sean atribuidas por normas legales o reglamentarias.

Las funciones de la Agencia de Protección de Datos, a excepción de las mencionadas en los apartados j), k) y l), y en los apartados f) y g) en lo que se refiere a las transferencias internacionales de datos, así como en relación con sus específicas competencias serán ejercidas, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial, por los órganos correspondientes de cada Comunidad, que tendrán la consideración de autoridades de control, a los que garantizarán plena independencia y objetividad en el ejercicio de su cometido. El Director de la Agencia de Protección de Datos podrá convocar regularmente a los órganos correspondientes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación. El Director de la Agencia de Protección de Datos y los órganos correspondientes de las Comunidades Autónomas podrán solicitarse mutuamente la información necesaria para el cumplimiento de sus funciones.

Cuando el Director de la Agencia de Protección de Datos constate que el mantenimiento o uso de un determinado fichero de las Comunidades Autónomas contraviene algún precepto de esta Ley en materia de su exclusiva competencia podrá requerir a la Administración correspondiente que se adopten las medidas correctoras que determine en el plazo que expresamente se fije en el requerimiento. Si la Administración pública correspondiente no cumpliera el requerimiento formulado, el Director de la Agencia de Protección de Datos podrá impugnar la resolución adoptada por aquella Administración.

La Agencia Española de Protección de Datos está compuesta, además de por el Director, por el Consejo Consultivo

(órgano de asesoramiento), el Registro General de Protección de Datos (órgano de instrucción de expedientes), la Inspección de Datos (órgano que ejerce la potestad de inspección) y la Secretaria General. En este sentido, una de las facultades más necesarias para velar por el cumplimiento de la normativa en esta matera, es la potestad inspectora, de cuyos resultados, además, derivan las correspondientes infracciones y sanciones.

¿CÓMO REALIZA SU ACTIVIDAD INSPECTORA LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS?

La actividad inspectora puede dar comienzo: de oficio o a instancia de los afectados (encuadrada o no dentro de los llamados planes sectoriales de oficio), notificándose previamente o por sorpresa (una recomendación para las empresas consiste en elaborar un manual de actuaciones frente a una inspección de la Agencia), teniendo en cuenta que la inspección puede personarse en las instalaciones no del responsable del fichero, sino en las del encargado del tratamiento. Finalizada la inspección, se extiende un acta por duplicado que podrá constatar:

- La inexistencia de infracciones y el consiguiente cierre del expediente informativo.

- La existencia de indicios de una posible infracción y la correspondiente apertura de un procedimiento.

- La tutela de derechos requiriendo a la entidad a la adopción de una decisión en materia de protección de datos.

- La apertura de un procedimiento sancionador.

Los procedimientos administrativos incoados por la Agencia Española de Protección de Datos son de tres tipos:

- Procedimientos sancionadores contra responsables de ficheros privados.

8. La Agencia Española de Protección de Datos

-Procedimientos sancionadores contra responsables de ficheros de titularidad pública.

-Procedimientos de tutela de derechos, que, en la práctica, se inician a instancia del afectado.

El procedimiento sancionador finaliza con Resolución del Director de la Agencia Española de Protección de Datos. Contra la resolución que pone fin a la vía administrativa cabe interponer, de forma potestativa, recurso de reposición (ante el Director de la Agencia) o, directamente, recurso contencioso-administrativo ante la Sala de lo contencioso-administrativo de la Audiencia Nacional.

¿EN QUÉ TÉRMINOS SE RECONOCE EL DERECHO A RECLAMAR ANTE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS?

La Ley Orgánica de Protección de Datos reconoce a los afectados la posibilidad de reclamar ante la Agencia Española de Protección de Datos en relación a actuaciones contrarias a la ley.

Aunque se hace alusión expresa a los supuestos de denegación, total o parcial, del ejercicio de los derechos de oposición, acceso, rectificación o cancelación, el ámbito de aplicación alcanza a otras actuaciones ilegítimas que suponen desconocimiento o violación de los derechos del afectado. Es el caso del incumplimiento de las reglas establecidas en torno al derecho de información. La tutela alcanza también a los supuestos de recogida de datos en forma engañosa o fraudulenta, incumplimiento del deber de secreto respecto de los datos del reclamante, la cesión o comunicación de datos sin conocimiento del afectado, el tratamiento de datos sin consentimiento del afectado cuando este sea necesario, la continuidad en el tratamiento pese a la revocación en el consentimiento notificada fehacientemente al responsable del fichero, etc.

Debe destacarse que se regula un supuesto de reclamación que hay que diferenciar de una eventual denuncia del

incumplimiento de la Ley, que puede interponerse por parte incluso de quien no sea titular de los derechos lesionados. No se olvide que el afectado puede limitarse a ser denunciante de determinados hechos poniéndolos en conocimiento de la Agencia.

A estos efectos es oportuno recordar que la Ley Orgánica de Protección de Datos tipifica como infracciones administrativas susceptibles de ser sancionadas por la Agencia Española de Protección de Datos algunas relativas al incumplimiento de las obligaciones establecidas en relación a los derechos de los afectados. Constituyen infracciones leves, no atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda, y proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información indicada. Constituyen infracciones graves, impedir u obstaculizar el ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada; mantener datos inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan; e incumplir el deber de información que establece la Ley cuando los datos hayan sido recabados de persona distinta del afectado. Son infracciones muy graves no atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición; y no atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

En concreto, en los casos de denegación, total o parcial, del ejercicio de los derechos de oposición, acceso, rectificación o cancelación, el afectado podrá ponerlo en conocimiento de la Agencia Española de Protección de Datos, o del organismo autonómico correspondiente, que deberá comprobar la procedencia o improcedencia de la denegación. En el caso del derecho de acceso, la reclamación podrá tener su origen en la no contestación en el plazo de un mes desde la recepción de la solicitud, o en la contestación no satisfactoria o en la denegación expresa del acceso.

En el caso de los derechos de rectificación y cancelación, puede haber ocurrido que el responsable no haya contestado en el plazo de diez días, haya denegado la rectificación o cancelación total o parcialmente sin justificación,

haya denegado la rectificación o cancelación total o parcialmente motivadamente, o no haya rectificado o cancelado el dato de modo efectivo.

Si el órgano competente concluye que la denegación es improcedente, deberá adoptar las medidas oportunas para que las garantías y derechos del afectado queden debidamente reparadas. En su caso, la Agencia deberá abrir expediente administrativo sancionador con independencia de si el interesado lo haya solicitado con anterioridad. Si se estima que la denegación es procedente, tal circunstancia deberá comunicarse al responsable y al afectado, que podrá recurrir la decisión en los términos que se analizan más adelante.

El plazo establecido para que la Agencia Española de Protección de Datos u organismo autonómico dicte resolución expresa es de seis meses. Las resoluciones se harán públicas una vez que hayan sido notificadas a los interesados. La publicidad se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones.

Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo. En particular, contra este tipo de resolución, que pone fin a la vía administrativa, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de la resolución, o directamente, recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, en el plazo de dos meses a contar desde el día siguiente a la notificación del acto.

Sin embargo, el responsable del fichero de titularidad pública sólo podrá interponer directamente recurso contencioso-administrativo.

¿CÓMO SE REGULA EL PROCEDIMIENTO DE RECLAMACIÓN ANTE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS?

El procedimiento se iniciará a instancia del afectado o afectados, expresando con claridad el contenido de su reclamación y de los preceptos de legislación aplicable que se consideran vulnerados. La Agencia dispone de impresos en el caso de reclamación de tutela por denegación del derecho de acceso, para que la Agencia Española de Protección de Datos pueda iniciar el procedimiento de tutela de derechos, resulta necesario que haya transcurrido un mes desde la presentación de la solicitud por la que se ejercita el derecho de acceso, sin que se haya producido contestación alguna, y que se aporte algún documento que permita comprobar tal circunstancia.

En el caso de reclamación de tutela por denegación del derecho de rectificación, para que la Agencia Española de Protección de Datos pueda iniciar el procedimiento de tutela resulta necesario que hayan transcurrido diez días sin que el responsable haya hecho efectivo el derecho, y que el afectado aporte, junto con el escrito que en su caso haya realizado el responsable del fichero, algún documento que permita comprobar la negativa del mismo a la rectificación de los datos. También para el caso de reclamación de tutela por denegación del derecho de cancelación, es necesario que hayan transcurrido diez días sin que el responsable haya hecho efectivo el derecho para que la Agencia Española de Protección de Datos pueda iniciar el procedimiento de tutela. Como en los supuestos anteriores, el afectado deberá adjuntar algún documento que permita comprobar la negativa del mismo a la cancelación de los datos.

Recibida la reclamación en la Agencia de Protección de Datos, se dará traslado de la misma al responsable del fichero, para que, en el plazo de quince días, formule las alegaciones que estime pertinentes. Recibidas las alegaciones o transcurrido el plazo de quince días citado, la Agencia de Protección de Datos, previos los informes, pruebas y otros actos de instrucción pertinentes, incluida la audiencia del afectado y nuevamente del responsable del fichero, resolverá sobre la reclamación formulada, dando traslado de la misma a los interesados. Contra la resolución del Director procederá potestativamente, recurso de reposición o recurso contencioso-administrativo ante la Sala de lo Contencioso- administrativo de la Audiencia Nacional.

9. El régimen de infracciones y sanciones en el ámbito de la protección de datos

¿CUÁL ES EL RÉGIMEN DE INFRACCIONES Y SANCIONES PREVISTO?

El régimen de infracciones y sanciones de la Ley orgánica de Protección de Datos parte de que los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador. Las infracciones se califican como leves, graves o muy graves

¿CUÁLES SON LAS INFRACCIONES LEVES?

a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.

b) No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.

c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.

d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información requerida.

e) Incumplir el deber de secreto, salvo que constituya infracción grave.

¿CUÁLES SON LAS INFRACCIONES GRAVES?

a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el «Boletín Oficial del Estado» o Diario Oficial correspondiente.

b) Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.

c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.

d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituye infracción muy grave.

e) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.

f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que

contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.

h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

i) No remitir a la Agencia de Protección de Datos las notificaciones previstas en la Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.

j) La obstrucción al ejercicio de la función inspectora.

k) No inscribir el fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos.

l) Incumplir el deber de información, cuando los datos hayan sido recabados de persona distinta del afectado.

¿CUÁLES SON LAS INFRACCIONES MUY GRAVES?

a) La recogida de datos en forma engañosa y fraudulenta.

b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.

c) Recabar y tratar determinados datos de carácter personal cuando no medie el consentimiento expreso del

afectado; recabar y tratar los datos referidos cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición de ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico o vida sexual.

d) No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.

e) La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.

f) Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.

h) No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.

i) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

9. El régimen de infracciones y sanciones en el ámbito de la protección de datos

¿CUÁLES SON LAS SANCIONES ESTABLECIDAS PARA LAS INFRACCIONES?

Esquema de cuantías de las multas según la categoría de las infracciones.

Categoría Infracciones	Importe Sancionador
Leves	desde 601,01 a 60.101,21 euros
Graves	desde 60.101,21 a 300.505,05 euros
Muy Graves	desde 300.506,05 a 601.012,10 euros

Es decir, tenemos una clasificación de las categorías de las infracciones que gradúa, conforme a la gravedad de las mismas, la cuantía de las multas a imponer:

Infracciones leves: Multa de 601,01 € a 60.101,21 €

Infracciones graves: Multa de 60.101,21 € a 300.505,05 €

Infracciones muy graves: Multa de 300.506,05 € a 601.012,10 €

En los supuestos, constitutivos de infracción muy grave, de utilización o cesión ilícita de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia de Protección de Datos podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido, la Agencia de Protección de Datos podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de **restaurar los derechos de las personas afectadas.**

En todo caso, **la cuantía de las sanciones se gradúa** atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora. Si, en razón de las circunstancias concurrentes, se aprecia una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate. En ningún caso puede imponerse una sanción más grave que la fijada en la Ley para la clase de infracción en la que se integre la que se pretenda sancionar. El Gobierno actualizará periódicamente la cuantía de las sanciones de acuerdo con las variaciones que experimenten los índices de precios.

Cuando las infracciones fuesen cometidas en ficheros de los que sean responsables las Administraciones públicas, el Director de la Agencia de Protección de Datos dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera. El Director de la Agencia podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones públicas. Se deberán comunicar a la Agencia las resoluciones que recaigan en relación con las medidas y actuaciones a que

se refieren los apartados anteriores. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores.

¿CUÁL ES EL PLAZO DE PRESCRIPCIÓN DE LAS INFRACCIONES?

Las infracciones muy graves prescribirán a los tres años, **las graves a los dos años** y **las leves al año**. El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.

Las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que adquiera firmeza la resolución por la que se impone la sanción. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

Guía de Protección de Datos para Empresas

10. La monitorización informática

¿PUEDEN LOS EMPRESARIOS CONTROLAR LAS COMUNICACIONES ELECTRÓNICAS DE SUS TRABAJADORES?

La generalización en el uso del correo electrónico en las empresas ha suscitado importantes discusiones en cuanto a su posible utilización incorrecta por parte de los trabajadores, lo que ha derivado en la implantación en las empresas de controles sobre el uso de las comunicaciones y medios electrónicos que el trabajador utiliza en su empresa. En esta situación, se plantea un conflicto entre:

- Derecho fundamental al secreto de las comunicaciones: en el lugar de trabajo poseen también los trabajadores derecho a la vida privada y a la protección de sus datos.

- Principio de libertad de empresa: el empresario debe poder velar por la eficiencia de su empresa controlando las comunicaciones electrónicas de sus trabajadores, la llamada monitorización informática.

- Derecho a la libertad sindical: la empresa está obligada a poner a disposición sindical tablones de anuncios y locales y el acceso a intranet y extranet de la empresa dependerá de lo que se acuerde y, si no hay nada acordado, la empresa puede prohibir el uso de la red.

La doctrina más evolucionada de los tribunales considera que el control empresarial del uso por parte de sus trabajadores de los medios informáticos vulnera el derecho fundamental a la intimidad de estas comunicaciones, de modo que el objetivo es determinar los límites a los que esté sujeto este control que realicen los empresarios. La utilización de los medios de trabajo, propiedad de la empresa y puestos a disposición del trabajador por parte del empresario, para fines particulares constituye una vulneración de la buena fe contractual.

Ahora bien, en la medida en que el control empresarial del uso de estas herramientas informáticas puede vulnerar derechos fundamentales de la persona, es necesario determinar los límites de este control. Así, para que una actividad de control empresarial sea legal y pueda estar justificada, deben respetarse una serie de principios:

- Necesidad: Sólo debe recurrirse a una forma de vigilancia cuando sea absolutamente necesaria y no haya una forma alternativa de lograr el objetivo.

- Finalidad: Al igual que sucede en la normativa sobre protección de datos, deben recogerse los datos con fines determinados, explícitos y legítimos, cuyo tratamiento posterior solo puede ajustarse a los fines previamente fijados.

- Transparencia: El control secreto de las comunicaciones electrónicas está prohibido. Se impone la obligación de proporcionar información al interesado (la empresa informará a los trabajadores sobre su política de control), la notificación a las autoridades competentes del tratamiento de datos que se pretende efectuar con carácter previo a su inicio y el derecho de acceso de los trabajadores a archivos del empleador. Al establecimiento de las reglas de uso de las herramientas informáticas que la empresa pone a disposición del trabajador se la denomina condiciones de uso de Internet (Internet use policy), formula que permite a la empresa comunicar a sus trabajadores de manera clara e indubitada los objetivos para los que se suministren las herramientas informáticas y que uso podrán hacer de las mismas, prohibiendo (o admitiendo con o sin condiciones) su utilización para fines personales.

- Legitimidad: El objetivo ha de ser de interés cierto y licito y no perjudicar los derechos fundamentales de los trabajadores. Aunque haya un interés legitimo en la finalidad de la empresa será ilegitima la intromisión que viole los derechos.

- Proporcionalidad: El control debe ser adecuado, pertinente y no excesivo en relación con los objetivos, en donde es fundamental tener en cuenta el tipo de riesgos a los que se enfrenta la empresa concreta que realiza el control

o vigilancia. En este contexto, el control general de las comunicaciones electrónicas queda excluido, salvo si es absolutamente necesario para la seguridad del sistema.

- Exactitud y conservación de los datos: Todos los datos recabados deberán ser precisos, estar actualizados y no podrán conservarse más tiempo del necesario.

- Seguridad: El empresario debe adoptar todas las medidas necesarias para proteger los datos personales que estén en su poder de intromisiones exteriores.

Guía de Protección de Datos para Empresas

11. El régimen jurídico de las comunicaciones comerciales (electrónicas y no electrónicas) no solicitadas y spam

¿QUÉ SON LAS COMUNICACIONES COMERCIALES VÍA ELECTRÓNICA?

Las comunicaciones comerciales son 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. Del concepto de comunicaciones comerciales se excluyen los datos que permiten acceder directamente a la actividad de una persona, empresa u organización, tales como el nombre de dominio o la dirección de correo electrónico y las comunicaciones relativas a los bienes, los servicios o la imagen que se ofrezcan cuando sean elaboradas por un tercero y sin contraprestación económica. Por tanto, se excluyen, los enlaces o "links" hacia páginas "web" de contenido publicitario, las indicaciones de direcciones de correo electrónico y las actividades desarrolladas por terceros independientes del titular cuyos bienes o servicios son publicitados. Además, aunque no se excluyan explícitamente, quedarían fuera del concepto de comunicaciones comerciales todos aquellos mensajes de carácter informativo, ausentes de toda finalidad comercial o empresarial como, por ejemplo, la publicidad institucional y la propaganda política o religiosa.

En consecuencia, al hacer referencia a la expresión toda forma de comunicación se aboga por un concepto amplio de comunicación comercial, que incluye todas las comunicaciones comerciales emitidas "on line", salvo las excepciones analizadas, independientemente de la forma y el formato que los mensajes presenten, bien gráfico, audio o ambos dos.

¿QUÉ NORMATIVA SE APLICA A LAS COMUNICACIONES COMERCIALES VÍA ELECTRÓNICA?

A las comunicaciones comerciales vía electrónica se les aplica no sólo la normativa del régimen de los servicios de la sociedad de la información, sino que además se regirán por su normativa propia y la vigente en materia

comercial y de publicidad y por la Ley Orgánica de Protección de Datos de carácter personal. Por tanto, serán de aplicación a las comunicaciones comerciales vía electrónica la Ley general que regula la publicidad; la normativa específica del producto o servicio en cuestión; la Ley General de Defensa de los Consumidores y Usuarios, en cuanto a la posible consideración de las comunicaciones comerciales como propuestas de la contratación destinadas a perfeccionar el contrato y la Ley Orgánica de Protección de Datos en lo que concierne al tratamiento de datos personales, ya que para enviar comunicaciones comerciales por vía electrónica es necesaria la previa averiguación de los datos personales de los destinatarios de dichas comunicaciones.

¿CUÁL ES EL RÉGIMEN GENERAL APLICABLE A LAS COMUNICACIONES COMERCIALES VÍA ELECTRÓNICA NO SOLICITADAS?

No supone ningún problema el envío de comunicaciones comerciales vía electrónica siempre que hayan sido previamente solicitadas por los destinatarios, los inconvenientes surgen cuando los destinatarios reciben numerosas comunicaciones comerciales que no han solicitado.

Existen dos modalidades para enviar comunicaciones comerciales no solicitadas lícitamente, los denominados sistemas **"opt-in" y "opt-out"**. Los denominados sistemas "opt-in", también conocidos como listas blancas o sistemas de inclusión voluntaria o de consentimiento explícito, donde sólo será lícito el uso comercial de las mismas cuando se autoriza expresamente. Los sistemas "opt-out" que parten de la licitud del envío de comunicaciones comerciales que no hayan sido solicitadas, siempre que el destinatario no hubiera expresado previamente su oposición. La legislación comunitaria ha optado por el establecimiento del sistema "opt-in" y, obviamente, nuestro ordenamiento jurídico establece el mismo sistema. En concreto, se establece que queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas. La expresión señalada -otro medio de comunicación electrónica equivalente- incluye el envío de mensajes mediante

telefonía móvil, como los mensajes cortos de teléfonos móviles o los mensajes multimedia pero se excluyen los servicios de telefonía vocal, fax o télex.

Por consiguiente, esta prohibición y todos los demás requisitos se aplican a todos los servicios de la sociedad de información, es decir, tanto al envío de correos electrónicos como al envío de mensajes mediante telefonía móvil.

¿CÓMO SE OBTIENE EL CONSENTIMIENTO PARA EL ENVÍO DE COMUNICACIONES COMERCIALES NO SOLICITADAS?

La Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico establece la prohibición de enviar comunicaciones comerciales publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas. En consecuencia, se establece la obligación para las empresas de obtener el consentimiento expreso de los destinatarios de las comunicaciones comerciales, no siendo lícito enviar comunicaciones comerciales no solicitadas ofreciendo simplemente la posibilidad de darse de baja del servicio enviando un mensaje de correo electrónico o bien accediendo a determinados enlaces.

Entre los distintos métodos de recepción de la autorización hay variantes en el grado de lealtad de las prácticas utilizadas que van desde las casillas marcadas previamente; pasando por las llamadas casillas seleccionables; hasta el extremo de solicitar que el visitante manifieste dos veces su deseo de ser incluido como destinatario de comunicaciones comerciales no solicitadas confirmando su inscripción.

Por tanto, las empresas que deseen enviar comunicaciones comerciales no solicitadas deben revisar sus técnicas de envío de comunicaciones comerciales no solicitadas, ya que deben recordar que la Ley de Comercio Electrónico

establece como requisito indispensable la obtención del consentimiento expreso, no siendo admisible el consentimiento tácito e implícito en el envío de comunicaciones comerciales no solicitadas.

¿QUÉ SIGINIFICA QUE EL CONSENTIMIENTO ESTÉ INCLUIDO DENTRO DE UN PROCESO CONTRACTUAL?

La Ley de Servicios de la Sociedad de la Información excluye el requisito de la necesidad de obtener el consentimiento expreso del destinatario de las comunicaciones comerciales no solicitadas cuando los destinatarios de las comunicaciones comerciales hayan sido clientes de la empresa remitente de la publicidad.

Por tanto, en la actualidad, no será necesario obtener el consentimiento expreso del destinatario de comunicaciones comerciales no solicitadas cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.

¿QUÉ REQUISITOS ADICIONALES SON NECESARIOS PARA ENVIAR COMUNICACIONES COMERCIALES?

Además, de la necesidad de que se obtenga el consentimiento expreso para enviar comunicaciones comerciales por vía electrónica cuando no hayan sido solicitadas es imprescindible cumplir otros requisitos adicionales:

- Las comunicaciones comerciales deberán ser claramente identificables como tales. Concretamente, se deberá incluir al comienzo del mensaje la palabra publicidad cuando se envíen comunicaciones comerciales a través de

correo electrónico o medios equivalentes. La Ley sólo hace referencia a que dicho requisito deba constar al comienzo del mensaje sin especificar el lugar concreto. Al respecto se ha pronunciado el Ministerio de Ciencia y Tecnología señalando que se debe realizar una interpretación restrictiva de la norma y la palabra publicidad debe aparecer claramente en el apartado destinado al asunto del correo electrónico.

- Las comunicaciones comerciales deberán indicar la persona física o jurídica en nombre de la cual se realizan los envíos. La finalidad de la inclusión de este requisito, es, obviamente, que el destinatario de las comunicaciones comerciales conozca el origen del mensaje. Por ello, es importante que las empresas que promocionen sus productos a través de empresas de publicidad y enviando comunicaciones comerciales no solicitadas se aseguren de con quién contratan los servicios de distribución de su publicidad, puesto que el incumplimiento de este requisito por la agencia publicitaria le conllevaría sanciones a la empresa anunciante –y no para la agencia de publicidad- por infracción de la Ley de comercio electrónico, además, de un deterioro de la imagen. No obstante, aunque la Ley no detalla qué datos deben constar, quizás sería oportuno incluir una dirección válida y funcional de correo electrónico con el objeto de dar una mayor transparencia al envío, puesto que con un vínculo hipertexto con una página identificativa de la empresa sería suficiente.

- En el supuesto de que las comunicaciones comerciales sean ofertas promocionales, como las que incluyan descuentos, premios y regalos y a los concursos o juegos promocionales se exige que se identifiquen claramente como tales y que las condiciones de acceso o participación se expresen de forma clara e inequívoca. Además de cumplir con las exigencias contenidas en el apartado anterior, se debe tener en cuenta que también las actividades de promoción de ventas están reguladas en la Ley del Comercio Minorista y en la Ley de Defensa de los Consumidores. Debe entenderse por condiciones de acceso, la necesaria fijación de la duración de la oferta y, en su caso, las reglas especiales aplicables a las mismas, ya que se persigue garantizar que el anuncio de una promoción contenga un contenido realmente ventajoso al que se pueda acceder con facilidad.

¿CÓMO PUEDE REVOCARSE EL CONSENTIMIENTO?

Se ofrece la posibilidad al destinatario de comunicaciones comerciales de revocar, en cualquier momento, el consentimiento prestado a la recepción de las mismas con la simple notificación de su voluntad al remitente. De este modo se reconoce un derecho de revocación en la Ley de Servicios de la Sociedad de la Información de manera análoga, e incluso reiterativa, a lo dispuesto en la Ley Orgánica de Protección de Datos personales para la modificación o cancelación de los datos. Este requisito se cumple por el remitente del mensaje mediante la habilitación de un procedimiento sencillo y gratuito para facilitar la revocación del consentimiento que hubieran prestado.

Asimismo, deberán facilitar información accesible por medios electrónicos sobre dichos procedimientos. El citado procedimiento, en la práctica, puede consistir en la inclusión de una dirección de correo electrónico de respuesta con instrucciones para el borrado, pero nada impide que se pueda buscar otro procedimiento por el remitente de las comunicaciones comerciales no solicitadas para que el destinatario de las mismas pueda ejercitar su derecho de revocación.

¿CUÁLES SON LAS INFRACCIONES PREVISTAS EN EL ÁMBITO DE LAS COMUNICACIONES COMERCIALES NO SOLICITADAS?

Al envío de comunicaciones comerciales vía electrónica son aplicables tanto la Ley de servicios de la sociedad de la información como la Ley Orgánica de Protección de Datos, establecido ambas un régimen disciplinario. En todo caso, en relación al envío de comunicaciones comerciales no solicitadas, la Ley de Servicios de la Sociedad de la Información contempla las siguientes infracciones:

Infracciones graves:

11. El régimen jurídico de las comunicaciones comerciales (electrónicas y no electrónicas) no solicitadas y spam

- El envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente o el envío, en el plazo de un año, de más de tres comunicaciones comerciales por los medios aludidos a un mismo destinatario, cuando en dichos envíos no se cumplan los requisitos legales. Por tanto, considera dicho precepto dos supuestos como infracciones graves:

- El envío masivo de comunicaciones comerciales. Esta expresión, sin duda, recoge los casos en que se envía un solo mensaje a muchos destinatarios y, en ningún caso el supuesto de que se envíen muchos mensajes a un solo destinatario, en cuyo caso estaríamos en el siguiente supuesto.

- Y el envío de más de tres comunicaciones comerciales en el plazo de un año. Como se observa en este supuesto concreto, el número de comunicaciones comerciales enviadas es determinante para proceder a calificar la infracción cometida, ya que si sólo se puede demostrar el envío de tres comunicaciones comerciales sería calificada como infracción leve, ya que es explícito el precepto al señalar en el enunciado el adverbio más de tres comunicaciones comerciales, recordemos que deben ser en el plazo de un año.

- El incumplimiento significativo de la obligación del prestador de servicios, en relación con los procedimientos para revocar el consentimiento prestado por los destinatarios.

- El incumplimiento significativo de las obligaciones de información o de establecimiento de un procedimiento de rechazo del tratamiento de datos.

Infracciones leves:

- El incumplimiento de lo previsto para las comunicaciones comerciales, ofertas promocionales y concursos.

- El envío de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica

equivalente cuando en dichos envíos no se cumplan los requisitos legales y no constituya infracción grave.

- El incumplimiento de las obligaciones de información o de establecimiento de un procedimiento de rechazo del tratamiento de datos, cuando no constituya una infracción grave.

- El incumplimiento de la obligación del prestador de servicios, en relación con los procedimientos para revocar el consentimiento prestado por los destinatarios, cuando no constituya infracción grave.

Las infracciones graves prescribirán a los dos años y las leves a los seis meses.

¿CUÁLES SON LAS SANCIONES PREVISTAS PARA LAS INFRACCIONES EN EL ÁMBITO DE LAS COMUNICACIONES COMERCIALES NO SOLICITADAS?

La sanción por la comisión de infracciones graves es de multa de 30.001 hasta 150.000 euros y por la comisión de infracciones leves, multa de hasta 30.000 euros.

El plazo de prescripción de las mismas es de **dos años por faltas graves y un año por faltas leves**.

Junto con el establecimiento de las sanciones, se establecen unos criterios de graduación para poder concretar la cuantía de las sanciones dentro del amplio intervalo de las mismas. Dichas reglas de valoración son las siguientes:

a) La existencia de intencionalidad.

b) El plazo de tiempo durante el que se haya venido cometiendo la infracción.

c) La reincidencia por comisión de infracciones de la misma naturaleza, cuando así haya sido declarado por resolución firme.

d) La naturaleza y cuantía de los perjuicios causados.

e) Los beneficios obtenidos por la infracción.

f) El volumen de facturación a que afecte la infracción cometida.

Además de las sanciones señaladas, las infracciones graves podrán llevar aparejada la publicación, a costa del sancionado, de la resolución sancionadora en el «Boletín Oficial del Estado», o en el diario oficial de la Administración Pública que, en su caso, hubiera impuesto la sanción o en dos periódicos cuyo ámbito de difusión coincida con el de actuación de la citada Administración Pública o en la página de inicio del sitio de internet del prestador, una vez que aquélla tenga carácter firme.

Tampoco se puede obviar el hecho de que se prevé que en los procedimientos sancionadores por infracciones graves o muy graves se podrán adoptar, con arreglo a la normativa administrativa, las medidas de carácter provisional que se estimen necesarias para asegurar la eficacia de la resolución que definitivamente se dicte, el buen fin del procedimiento, evitar el mantenimiento de los efectos de la infracción y las exigencias de los intereses generales. En particular, podrá acordarse la suspensión temporal de la actividad del prestador de servicios y, en su caso, el cierre provisional de sus establecimientos; el precinto, depósito o incautación de registros, soportes y archivos informáticos y de documentos en general, así como de aparatos y equipos informáticos de todo tipo; e incluso se podrá advertir al público de la existencia de posibles conductas infractoras y de la incoación del expediente sancionador de que se trate, así como de las medidas adoptadas para el cese de dichas conductas.

Como siempre, se respetará, en todo caso, el principio de proporcionalidad de la medida a adoptar con los objetivos que se pretendan alcanzar en cada supuesto.

En el supuesto que no se cumplan las medidas provisionales, el órgano administrativo competente para resolver el procedimiento sancionador podrá imponer multas coercitivas por importe que no exceda de 6.000 euros por cada día que transcurra sin cumplir las medidas provisionales que hubieran sido acordadas.

Además, en casos de urgencia y para la inmediata protección de los intereses implicados, las medidas provisionales podrán ser acordadas antes de la iniciación del expediente sancionador. Las medidas deberán ser confirmadas, modificadas o levantadas en el acuerdo de iniciación del procedimiento, que deberá efectuarse dentro de los quince días siguientes a su adopción, el cual podrá ser objeto del recurso que proceda. En todo caso, dichas medidas quedarán sin efecto si no se inicia el procedimiento sancionador en dicho plazo o cuando el acuerdo de iniciación no contenga un pronunciamiento expreso acerca de las mismas.

Por último, debe señalarse que estas obligaciones que garantizan la licitud de las comunicaciones comerciales no solicitadas remitidas por vía electrónica, van a ser exigibles tanto a los prestadores de los servicios de la sociedad de la información emplazados en España, como a aquellos que se encuentren establecidos en un país miembro de la Unión Europea o del Espacio Económico europeo cuando el destinatario de los servicios radique en España.

¿QUIÉN ES EL ÓRGANO COMPETENTE PARA LA IMPOSICIÓN DE SANCIONES?

El órgano competente para imponer las sanciones será el Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información en el supuesto de infracciones graves y leves.

No obstante, la imposición de sanciones por incumplimiento de las resoluciones dictadas por los órganos competentes en función de la materia o entidad de que se trate corresponderá al órgano que dictó la resolución incumplida.

Igualmente, corresponderá a la Agencia de Protección de Datos la imposición de sanciones por la comisión de

11. El régimen jurídico de las comunicaciones comerciales (electrónicas y no electrónicas) no solicitadas y spam

determinadas infracciones y, desde marzo de 2004, a la Agencia Española de Protección de Datos se le han atribuido competencias de inspección y sanción en materia de SPAM.

¿QUÉ RESPONSABILIDAD SE ATRIBUYE A LAS EMPRESAS DE INTERMEDIACIÓN?

A pesar de las innumerables ventajas que presenta la utilización de internet, también es el medio idóneo para transmitir, alojar o almacenar contenidos o informaciones que lesionan los derechos e intereses legítimos de terceros.

Los métodos utilizados para cometer estos daños y perjuicios son numerosos, desde el hacking, el cracking, el uso ilícito de cookies (en la medida en que, fundamentalmente, ofrecen un servicio personalizado al usuario -salvo la recopilación de información con fines estadísticos-, han de respetar el régimen jurídico previsto para la protección de los datos personales cuando la identidad del titular de la información recabada pueda ser conocida) y al spamming, entre otros.

Estos contenidos ilícitos elaborados por quienes son los destinatarios de los servicios de intermediación, pueden causar daños y perjuicios a terceros que se han de reparar y, en la medida en que, en la mayoría de las ocasiones resulta muy complicado identificar al autor de tales acciones lesivas, queda justificada la responsabilidad de los prestadores de servicios de intermediación (ISP derivado del término inglés internet Service Provider), que resultan mucho más fácilmente identificables y pueden impedir que sigan produciéndose las conductas ilícitas en el caso de los servicios de alojamientos.

En el ámbito comunitario, no se establece propiamente una regulación general de la responsabilidad de los prestadores de servicios de intermediación sino que se reconocen una serie de supuestos específicos de exención

de responsabilidad. Ello supone que si una conducta ilícita causa daños y han circulado por la red gracias a la intervención del prestador de servicios no implica que éste deba ser necesariamente responsable de aquellos perjuicios causados derivados tanto de ilícitos civiles como penales. En consecuencia, los intermediarios que quieran beneficiarse del régimen de exenciones, que constituyen una especialidad respecto del régimen general de responsabilidad, deberán cumplir cada uno de los requisitos establecidos para cada supuesto. Por el contrario, si no se cumplen los mismos se les aplicará el régimen general de responsabilidad.

¿CUÁLES SON LAS EXENCIONES DE RESPONSABILIDAD CIVIL POR CONTENIDOS AJENOS EN INTERNET?

La normativa comunitaria ha establecido unas exenciones de responsabilidad para los prestadores de servicios de la sociedad de la información que actúan como intermediarios, es decir, prestadores que posibilitan que los contenidos, que generan terceros, circulen, se alojen y sean accesibles por los usuarios de la Red.

Por tanto, el hecho de que los contenidos que un prestador de servicios de intermediación transmite o almacena hayan sido proporcionados por terceros, es decir, que sean contenidos ajenos al prestador de servicios de intermediación, resulta esencial para poder aplicar la correspondiente exención, puesto que en el supuesto que sea el propio prestador de servicios el autor de los contenidos que se trasmiten por la Red ya no estaríamos ante una función de intermediación y, por ende, no podrían aplicarse las exenciones de responsabilidad, acudiendo consecuentemente a las reglas generales de responsabilidad.

Tanto en la Directiva como en la normativa española que la traspone se pueden diferenciar las siguientes actividades: La simple transmisión de datos y la prestación del servicio de acceso, el alojamiento de datos o "hosting" y el almacenamiento automático y provisional de datos denominado "catching".

11. El régimen jurídico de las comunicaciones comerciales (electrónicas y no electrónicas) no solicitadas y spam

¿CUÁL ES EL ÁMBITO DE APLICACIÓN DE LA EXENCIÓN EN EL CASO DE SERVICIOS DE MERA TRANSMISIÓN DE DATOS Y DE PROVISIÓN DE ACCESO A INTERNET?

Este supuesto de exención consiste en transmitir en una red de comunicaciones de datos facilitados por el destinatario del servicio o en facilitar el acceso a una red de comunicaciones.

Por tanto, el prestador del servicio no podrá ser considerado responsable de los datos transmitidos cuando haya cumplido con los siguientes requisitos:

- No haber originado él mismo la transmisión, es decir, nos encontremos ante contenidos ajenos al prestador de servicios de intermediación porque el prestador del servicio no haya generado el contenido de la transmisión ni tampoco haya tomado la iniciativa de realizar la transmisión concreta. Por tanto, la decisión de la transmisión le corresponde a la persona que suministra los datos y solicita que sean transmitidos, por ejemplo, al titular de los productos y servicios promocionados en la comunicación comercial.

- No haber seleccionado al destinatario de la transmisión. Recordando el requisito esencial de que nos encontremos ante contenidos ajenos al prestador de servicios de intermediación, si éstos eligieran a los destinatarios de la transmisión, es decir, de las comunicaciones comerciales no solicitadas, supondría que ya no estaríamos ante una simple actividad de intermediación, pasiva y automática sino ante una actividad activa y de control sobre uno de los elementos de la transmisión: los destinatarios.

- Y no haber seleccionado ni modificado los datos transmitidos. No se entenderá por modificación la manipulación estrictamente técnica de los archivos que alberguen los datos que tiene lugar durante su transmisión.

Por último, es necesario señalar la posibilidad de que un Tribunal o una autoridad exijan al prestador de servicios que suspenda la transmisión de contenidos ilícitos. El cumplimiento de dicha orden no se establece como requisito para gozar de la exención y, por tanto, el incumplimiento de la orden por parte del prestador del servicio no implicará la pérdida de la exención de responsabilidad si se dan las condiciones establecidas, sino que el prestador podrá incurrir en responsabilidad como consecuencia de haber incumplido la orden y haber continuado con la transmisión o la provisión de acceso.

El prestador de servicios que colabore deliberadamente con uno de los destinatarios de su servicio a fin de cometer actos ilegales rebasa las actividades de mero transporte (mere conduit) o la forma de almacenamiento automático, provisional y temporal, denominada memoria tampón (catching) y no puede beneficiarse, por consiguiente, de las exenciones de responsabilidad establecidas para dichas actividades.

¿CUÁL ES EL ÁMBITO DE APLICACIÓN DE LA EXENCIÓN EN EL CASO DE PRESTACIÓN DEL SERVICIO DE ALOJAMIENTO DE DATOS O HOSTING?

El caso típico de esta exención es el supuesto en que un prestador de servicios hospede en su servidor, concretamente un servidor de correo electrónico, es decir, ofrezca al cliente un espacio de disco donde quedan alojados los mensajes recibidos, es decir, las comunicaciones comerciales enviadas.

Los requisitos necesarios para que se pueda aplicar esta exención de responsabilidad a los prestadores de servicios de alojamiento son las siguientes:

- Falta de conocimiento efectivo de la ilicitud de la actividad o de la información que se alberga. En el caso de una acción de reclamación de daños y perjuicios el prestador de servicios sólo quedará exento de responsabilidad si no ha tenido conocimiento de hechos o circunstancias por los que la actividad o la información revele su carácter ilícito.

11. El régimen jurídico de las comunicaciones comerciales (electrónicas y no electrónicas) no solicitadas y spam

- Y actuar con prontitud para retirar los datos o para hacer que el acceso a los mismos sea imposible tras que el prestador adquiere un conocimiento efectivo de la ilicitud, y en el caso de una acción de daños y perjuicios desde el momento en que conoció hechos o circunstancias reveladores de la ilicitud.

La Ley recoge otros dos grupos de supuestos que pueden dar lugar, en su caso, a un resultado equivalente:

- Los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios.

- Y otros medios de conocimiento efectivo que pudieran establecerse.

Por último, se debe señalar la posibilidad de que un tribunal o una autoridad administrativa, exijan al prestador de servicios poner fin a una infracción o impedirla, y a la posibilidad de que los Estados miembros establezcan procedimientos por los que se rija la retirada de datos o impida el acceso a ellos. En consecuencia, si la orden consiste en que se retire determinada información o que se bloquee el acceso a la misma y se hace caso omiso a la misma, supondría que no se ha actuado con prontitud para retirar los datos o hacer que el acceso a ellos sea imposible y, por ende, se incumpliría con uno de los requisitos establecidos para aplicar la exención.

¿EN QUÉ CONSISTE EL SPAM?

Por el momento, no existe unanimidad a la hora de definir esta realidad social. No obstante, una vez rechazado el genérico concepto de spam como cualquier correo no solicitado, hay dos definiciones ampliamente aceptadas sobre el spam:

- correos electrónicos comerciales no solicitados

- y correos electrónicos masivos no solicitados procedentes de una misma persona.

Lo que califica al correo no solicitado como spam es su carácter comercial, la cantidad enviada o ambas características.

¿QUÉ DIFERENCIAS EXISTEN ENTRE EL SPAM Y LA COMUNICACIÓN COMERCIAL?

En principio, se puede entender spam, en términos generales, como todo aquel correo no solicitado que nos llega a nuestro buzón de correo. Generalmente los mensajes spam son publicidad, ofertas, asistencia financiera, promociones, ventas con descuento, etc... Actualmente la expresión spam se utiliza para designar cualquier tipo de comunicación no solicitada, faxes, llamadas telefónicas, correo regular, etc. Desde este punto de vista, constituye, sin duda alguna, un método de prospección no solicitada. Sin embargo, se distingue de esta última por su carácter masivo, repetido y desleal.

Por otro lado, por comunicaciones comerciales se entiende toda forma de comunicación dirigida a la promoción directa o indirecta de la imagen o servicios de una organización o persona que realice una actividad comercial, industrial, artesanal o profesional. Podemos deducir en este sentido que una comunicación comercial no solicitada tiene dos características: ser comercial y no haber sido solicitada. Por tanto, la publicidad u oferta de productos y servicios a través del correo electrónico estaría incluido en este concepto y no el envío de boletines de noticias o simplemente informativos a menos que ofrezcan algún producto o servicio.

Así, no toda comunicación que se envíe a un grupo de usuarios tiene por qué ser comunicación comercial ni por tanto estar sujeta a los requerimientos de información y consentimiento que indica la Ley de Comercio Electrónico. Este supuesto, por tanto, no podría ser calificado de comunicación comercial no solicitada, ya que carece del carácter comercial, sino que nos encontramos ante una simple comunicación de información, calificada como spam

si reuniese la característica de masiva. De ello podemos deducir que el spamming exclusivamente comercial constituye prospección comercial no solicitada, pero no toda comunicación comercial no solicitada es spamming, ya que si se cumplen con los requisitos establecidos en el ordenamiento jurídico español se pueden enviar comunicaciones comerciales no solicitadas conforme a la legalidad establecida. En definitiva, mientras el envío de spam es totalmente contrario a la normativa comunitaria y española, si que está permitido enviar comunicaciones comerciales no solicitadas cuando se cumple la normativa vigente.

¿QUÉ PERJUICIOS ORIGINA EL SPAM?

Es evidente que recibir spam de cualquier clase -postal, telefónico, electrónico- es molesto para los receptores del mismo. Pero, además, el spam a través de correos electrónicos genera una mayor preocupación a los agentes sociales implicados, ya que, el número de comunicaciones comerciales no solicitadas recibidas es casi ilimitado debido a que el gasto que supone este tipo de campañas es ínfimo a diferencia de lo que ocurre con el buzoneo o spam postal.

Además, aunque aparentemente el spam electrónico no causa ningún perjuicio económico al usuario, esta pensamiento generalizado es incierto, ya que el receptor de spam, tanto los usuarios como los servidores de internet, carga con la mayoría de los costes, desde la pérdida de tiempo asociados a la lectura de los mensajes a los perjuicios derivados de dichos envíos como; la utilización de los servidores de SMTP para procesar y distribuir los mensajes, la utilización de la CPU y, en consecuencia, la pérdida de espacio en el disco del servidor y de los usuarios finales, la disminución del ancho de banda en la red, e incluso se generan mayores riesgos de recepción de virus.

Además de los costes ya señalados, los prestadores de servicios de la sociedad de la información tiene un gasto económico añadido, ya que deben adquirir los programas adecuados para evitar el uso abusivo de su conexión o para contrarrestar los colapsos provocados por los envíos masivos.

¿CUÁLES SON LOS MÉTODOS DE DISTRIBUCIÓN UTILIZADOS EN EL SPAM?

En principio, la acción de distribuir un mensaje a miles de destinatarios simultáneamente es una labor sencilla, además de económica, puesto que basta con conocer el diálogo de las transacciones SMTP, es decir, el spammer necesita solamente un programa sencillo que reproduzca un diálogo SMTP que falsifique el remite, una base de datos con las direcciones de correo electrónico de los destinatarios de los mensajes y un buzón desde donde distribuirá el spam.

No obstante, los métodos de distribución del spam son varios, tanto en el formato como en el grado de dificultad. Originariamente era bastante fácil reconocer el spam porque los primeros métodos de distribución se presentaban casi siempre de varias formas con unas características comunes: el campo from o de casi siempre contenía un nombre de fantasía, la dirección reply o bien el mensaje aparecía en mayúsculas o utilizaba en abundancia los puntos de exclamación.

Estas primeras técnicas rutinarias han evolucionado notablemente y durante estos días se está hablando continuamente en los medios de comunicación del llamado pishing. Las entidades bancarias deben estar alerta ante el envío de este nuevo spam, considerado ya como el timo del siglo XXI. Esta técnica consiste en enviar a través del un correo electrónico un mensaje, remitido con una apariencia de legalidad desde una supuesta entidad financiera, que indica al destinatario que, para mayor seguridad y mayor protección de su confidencialidad y debido a que ha habido un error en los sistemas de la citada entidad, debe enviar de nuevo sus datos personales a la supuesta entidad financiera, que realmente es un fraude y supone que acaben los datos bancarios del destinatario del mensaje en poder del spammer.

¿QUÉ MEDIDAS PUEDEN ADOPTARSE CONTRA EL SPAM?

En función de quienes sean los destinatarios de los envíos de spam se enfocan las posibles medidas al problema.

11. El régimen jurídico de las comunicaciones comerciales (electrónicas y no electrónicas) no solicitadas y spam

No son las mismas soluciones a adoptar para una empresa, para un proveedor de servicios de internet o para los usuarios.

Por este motivo se clasifican las medidas contra el spam en:

- Preventivas: Medidas que colaboran a evitar recibir o distribuir spam en o desde empresa o proveedores. Se englobaría dentro de estas medidas la eliminación del tag html en las páginas web y el fomento de las políticas de uso del correo electrónico en empresas y proveedores.

- Sancionadoras: Medidas que se toman después que el spam haya llegado a los servidores y buzones. Las principales medidas reactivas son los filtros de contenido, tanto para servidores como clientes de correo.

- Técnicas: Medidas que se toman antes que el correo no deseado llegue a los servidores, es decir, que la transacción SMTP entre el servidor origen y el destino no finalice con éxito y sea rechazado en función del perfil del servidor origen que pretende enviar el correo. Este tipo de medidas intentan evitar tanto la entrada de spam en nuestro dominio como presionar al origen para no enviarlo. Las medidas que se encuentran incluidas en este concepto son: la propia legislación de los países, las respectivas denuncias y sanciones y listas negras, e incluso, otras aplicaciones anti-spam más especializadas y que son bastante efectivas como, por ejemplo, el Spam Attack Pro, el Spam Exterminator y el Spamkiller.

¿QUÉ MEDIDAS HA ADOPTADO CONTRA EL SPAM LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS?

En la medida en que el spam es un fenómeno transnacional, la Agencia de Protección de datos ha iniciado relaciones

con otras autoridades de control que se enmarcan en la vocación de cooperación internacional que informa la actividad de la Agencia, y que se plasman, entre otras, en las siguientes acciones:

- Representación española en el Grupo Europeo de Autoridades de control de Protección de Datos, conocido como Grupo del artículo 29.

- Representación española en la Presidencia de la Red Iberoamericana de Protección de Datos.

- Participación en numerosos foros internacionales, como los Talleres de la OCDE de Lucha Contra el «spam», o el Grupo CNSA («Contact Network Of spam Authorities») de la Comisión Europea.

- Participación en la creación e impulso de la iniciativa denominada London Action Plan, surgida bajo los auspicios de la OCDE el 1 de octubre de 2004.

- Participación en la Iniciativa «Zombie drone».

- Colaboración de las autoridades de control de Alemania y Reino Unido en casos concretos.

- Relación bilateral con la Federal Trade Commission (FTC) que se ha plasmado en la firma de un acuerdo de colaboración.

- La promoción de la celebración del Tercer Encuentro Iberoamericano de Protección de Datos en Colombia, suscribiendo la llamada Declaración de Cartagena de Indias.

La colaboración internacional en esta materia permitirá establecer un marco homogéneo que resulta imprescindible para combatir el spam, dado el ámbito transnacional del propio fenómeno, pero, es preciso, además, propiciar e

impulsar iniciativas de autorregulación sectorial que complementen y faciliten la aplicación del marco regulatorio sobre la materia.

¿QUÉ RÉGIMEN SE ESTABLECE PARA LAS COMUNICACIONES COMERCIALES NO ELECTRÓNICAS?

Las comunicaciones comerciales no siempre revisten la característica que la Ley de comercio electrónico define como vía electrónica, puesto que la publicidad no sólo se trasmite a través de correos electrónicos u otro medio electrónico equivalente (sms, mms) sino que diariamente las empresas ofrecen sus productos a través de llamadas comerciales no deseadas. A este respecto, según la definición de servicios de la sociedad de la información quedan excluidos de la misma los servicios de telefonía vocal, fax o télex. Por tanto, no se podrán considerar ni las llamadas comerciales ni los faxes promocionales comunicaciones comerciales vía electrónica.

¿QUÉ RÉGIMEN SE ESTABLECE PARA EL TELEMARKETING Y EL MARKETING INTERACTIVO?

El llamado telemarketing es una actividad que, junto al marketing interactivo, ha tenido un enorme crecimiento en los últimos años. La legislación comunitaria exige el consentimiento previo para utilizar los sistemas de llamada automática sin intervención humana (aparatos de llamada automática) y el fax con fines de venta directa respecto de sus abonados.

En cambio, cuando los medios utilizados no sean los mencionados, se ofrece la posibilidad a los Estados miembros de la Unión de determinar el sistema correspondiente, es decir, podrán optar, o bien por el sistema del consentimiento previo o por el sistema de oposición. El legislador español ha transpuesto esta regulación en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, determinando que los abonados a los servicios de comunicaciones

electrónicas tendrán el derecho a no recibir llamadas automáticas sin intervención humana o mensajes de fax, con fines de venta directa sin haber prestado su consentimiento previo e informado para ello. En el mismo sentido se pronuncia el Real Decreto 424/2005, al establecer que las llamadas no solicitadas por los abonados con fines de venta directa que se efectúen mediante sistemas de llamada automática, a través de servicios de comunicaciones electrónicas, sin intervención humana (aparatos de llamada automática) o facsímil (fax), sólo podrán realizarse a aquellos que hayan dado su consentimiento previo, expreso e informado. El incumplimiento de dicha obligación de obtener el consentimiento previo, expreso e informado será sancionado de acuerdo con lo establecido en la Ley de servicios de la sociedad de la información.

Por otra parte, respecto a las llamadas no solicitadas con medios distintos a las llamadas automáticas sin intervención humana o fax, en ningún momento se hace mención a este supuesto en la Ley General de Telecomunicaciones. Es decir, la normativa española no se pronuncia respecto a qué criterio se debe seguir para realizar este tipo de llamadas comerciales no solicitadas. Para salvar esta laguna, el Real Decreto 424/2005, de 15 abril, dispone que las llamadas no solicitadas a los abonados con fines de venta directa que se efectúen mediante sistemas distintos a la llamada automática y al fax podrán efectuarse, salvo las dirigidas a aquellos que hayan manifestado su deseo de no recibir dichas llamadas. No obstante, para realizar las llamadas a las que este se refiere a quienes hubiesen decidido no figurar en las guías de comunicaciones electrónicas disponibles al público o a los que hubiesen ejercido su derecho a que los datos que aparecen en ellas no sean utilizados con fines de publicidad o prospección comercial, será preciso contar con el consentimiento expreso de aquéllos.

En todo caso, los abonados deberán ser informados al menos un mes antes de que sus datos se incorporen a las guías. Si es la primera vez que se les incluye en una de estas guías, deberán prestar su consentimiento expreso –contestando a la solicitud recibida–, mientras que para las siguientes ediciones será suficiente su no oposición expresa cuando se le notifique. También podrá el abonado solicitar figurar en la guía pero que sus datos no se utilicen con fines publicitarios, así como que no consten algunos de sus datos tales como el domicilio.

12. Anexo I - Anexo II

ANEXO I

NORMATIVA EN MATERIA DE PROTECCIÓN DE DATOS

- Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal
- Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos (modificado por Real Decreto 156/1996, de 2 de febrero)
- Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992
- Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
- Ley 59/2003, de 19 de diciembre, de firma electrónica.

ANEXO II

ESQUEMAS

¿CUÁLES SON LOS NIVELES DE SEGURIDAD EXIGIDOS EN LOS FICHEROS?

NIVELES DE SEGURIDAD EN FUNCIÓN DE LOS DATOS QUE CONTENGA:

Básico = Para cualquier dato de carácter personal no especificados para el nivel medio o alto. Podríamos distinguir, dentro de éste nivel, un nivel **Básico Superior** que estaría referido a todo conjunto de datos que, relacionados entre sí, permitan obtener una evaluación de la personalidad del individuo y por ello se les exige la auditoria obligatoria.

Medio = Para datos Relativos a comisión de sanciones administrativas o penales, Hacienda Pública, servicios financieros, servicios de información sobre solvencia patrimonial o de crédito.

Alto = Respecto a datos sobre ideología, religión, creéncias, origen racial, salud, vida sexual.

MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO

CLAVES	DESCRIPCIÓN BÁSICA
TIPO DE DATOS	· Nombre · Apellidos · Direcciones de contacto (tanto físicas como electrónicas) · Teléfono (tanto fijo como móvil) · Nº cuenta corriente · Otros
MEDIDAS DE SEGURIDAD OBLIGATORIAS	· Documento de seguridad · Régimen de funciones y obligaciones del personal · Registro de incidencias · Identificación y autenticación de usuarios · Control de acceso · Gestión de soportes · Copias de respaldo y recuperación

MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO SUPERIOR

CLAVES	DESCRIPCIÓN BÁSICA
TIPO DE DATOS	· Conjunto de datos que cruzándose permitan obtener una evaluación de la personalidad del individuo
MEDIDAS DE SEGURIDAD OBLIGATORIAS	· Medidas de seguridad de nivel básico · Auditoría bianual

12. Anexo I - Anexo II

MEDIDAS DE SEGURIDAD DE NIVEL MEDIO

CLAVES	DESCRIPCIÓN BÁSICA
TIPO DE DATOS	· Comisión infracciones penales · Comisión infracciones administrativas · Información de Hacienda Pública · Información de servicios financieros
MEDIDAS DE SEGURIDAD OBLIGATORIAS	· Medidas de seguridad de nivel básico · Responsable de Seguridad · Auditoría bianual · Medidas adicionales de Identificación de usuarios · Control de acceso físico · Medidas adicionales de gestión de soportes · Registro de incidencias · Pruebas sin datos reales

MEDIDAS DE SEGURIDAD DE NIVEL ALTO

CLAVES	DESCRIPCIÓN BÁSICA
TIPO DE DATOS	· Ideología · Religión · Creencias Origen racial · Salud · Hábitos de vida sexual · Afiliación sindical
MEDIDAS DE SEGURIDAD OBLIGATORIAS	· Medidas de seguridad de nivel básico y medio · Seguridad en la distribución de soportes · Registro de accesos · Medidas adicionales de copias de respaldo · Cifrado de telecomunicaciones