PractiLetter
Protección de Datos

Defienda su empresa, proteja su información

Número 11 Diciembre 2010

Asesoriza
Publicaciones pensadas para la empresa

El importe de las sanciones de la LOPD

El Tribunal Supremo acaba de dictar una sentencia de las que dejan un regusto muy amargo. Ha confirmado una sanción de nada menos que 300.000 euros a una residencia de ancianos por haber dado los datos personales de algunos ancianos a la farmacia de al lado para que ésta pudiera suministrarles y cobrarles los medicamentos que necesitan y que no cubría la Seguridad Social, sin formalizar las correspondientes cláusulas de protección de datos. Un error formal, de acuerdo… ¿pero merece una sanción de ese importe cuando se trataba de facilitar el suministro de medicamentos y no de operaciones comerciales…?

*En el **Archivo Online** y con su contraseña, usted tiene acceso a las sentencias íntegras que aparecen en la sección de "Tribunales" (como ésta del Tribunal Supremo).*

***Laura Aramburu.** Editora*

Archivo online de documentos

Servicio gratuito exclusivo para Suscriptores

Obtenga y descargue desde su ordenador modelos de escritos y cartas, cláusulas, checklists, hojas de cálculo… de aplicación inmediata.

www.practiletter.com

Contraseña: cancelar

Derecho de cancelación: cómo tiene que responder su empresa ante cada solicitud

Al recabar los datos de una persona para incorporarlos a un fichero, su empresa debe informarle, entre otras cosas, de sus derechos relacionados con la privacidad. Uno de ellos es el derecho de cancelación, es decir, de la posible futura petición a su empresa de que suprima sus datos personales de los ficheros. Cuando alguien ejerce ese derecho, usted debe responder de forma adecuada y dentro de unos plazos determinados. Sepa cuándo puede cancelar los datos que le soliciten y cuándo no puede hacerlo aunque se lo pidan, y conozca bien todas las pautas para implantar en su empresa las normas adecuadas para responder a este derecho.

(sigue en la página 6)

Residuos informáticos: cómo deshacerse de ellos de forma segura

¿Qué hacen en su empresa cuando hay que desechar soportes informáticos? Un simple CD o un minúsculo pendrive pueden contener el equivalente a miles y miles de folios, almacenándose en ellos enormes cantidades de datos personales. Desprenderse de hardware que contenga información (disquetes, CDs, pendrives…) es una de las situaciones de mayor peligro para la confidencialidad y seguridad de los datos personales. Por eso su empresa necesita implantar un protocolo sencillo y a la vez muy riguroso para deshacerse de ellos.

(sigue en la página 3)

En este número:

Preguntas y Respuestas

¿Es un dato personal el pin de una tarjeta de crédito?

PREGUNTA: *En nuestra empresa los clientes pueden pagar con tarjeta de crédito, por lo que cada vez más deben marcar su código pin de identificación al efectuar el pago (en lugar de firmar el recibo), lo cual muchas veces ocurre a la vista de nuestros empleados. ¿Qué implicaciones tiene esto para nuestra empresa en cuanto a la protección de datos personales?*

RESPUESTA: El hecho de que los clientes deban teclear el código personal de sus tarjetas para que pueda producirse la transacción comercial no tiene ninguna relación con la aplicación de la normativa de protección de datos, puesto que su empresa no estaría realizando ningún tratamiento con esos datos (los pin), que solamente son tecleados por los clientes.

Caso distinto sería si su empresa creara un fichero con esos códigos y los sometiera a tratamiento, comunicación o cesión, pues en ese caso sí se trataría de un fichero de datos personales sujeto a la LOPD. Pero como no es el caso, la cuestión no guarda ninguna relación con la normativa de protección de datos personales.

¿Se deben hacer copias de seguridad de los ficheros no automatizados?

PREGUNTA: *Nuestra empresa tiene en marcha un completo protocolo de copias de seguridad y respaldo de todos los ficheros informatizados. ¿Hay que hacer algo parecido con los ficheros de papel?*

RESPUESTA: Desde el año 2007 –fecha en que se aprobó el Reglamento de Desarrollo de la LOPD (RD 1720/2007 de 21.12.07)- los ficheros manuales se encuentran también bajo el ámbito de aplicación de la LOPD y su normativa de desarrollo. Esto significa que se les aplican todas las previsiones establecidas en la normativa (por ejemplo, inscripción del fichero, atención de los derechos ARCO de los afectados, etc.) salvo, precisamente, la obligación de realizar copias de seguridad y respaldo.

La obligación de realizar estas copias no es aplicable a los ficheros no informatizados, sino que es una medida reservada a los ficheros automatizados, por su propia naturaleza electrónica y digital, en los que la realización de copias de seguridad se hace mediante un procedimiento informático (el backup).

La normativa española de protección de datos anterior a la Directiva europea del año 1995 y vigente hasta el 14 de enero de 2000, se refería a la regulación del tratamiento automatizado de los datos de carácter personal (Ley Orgánica 5/1992, de 29 de octubre), y no se aplicaba a tratamientos en soporte papel.

Sin embargo, la legislación europea posterior a la norma del año 1995 -y la legislación española desde la LOPD-, se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero, aunque de estos últimos no sea posible hacer copia de seguridad en formato digital.

PractiLetter Protección de Datos es una publicación de Asesoriza, división editorial de Global Publishers España, S.L.

EDITORA: Laura Aramburu.
REDACCIÓN: Leticia Garín y Estela Martín.
CONSEJO EDITORIAL: Juan Carlos Aramburu, Jesús Efrén Díaz y Olga Jiménez.
Empresa Editora: Global Publishers España, S.L. Capitán Haya 35. 28020 Madrid. Telf: 914 170 615 Fax: 914 170 054. info@practiletter.com www.practiletter.com

Telf. Suscripciones: 914 170 615

Depósito Legal: M-50876-2009 Imprime: Gráficas Marcar

Seguridad informática

Residuos informáticos: cómo deshacerse de ellos en su empresa de forma segura

¿Qué se hace en su empresa cuando hay que desechar soportes informáticos? La pregunta es importante, pues desprenderse de hardware que contenga información (disquetes, CDs, pendrives…) es una de las situaciones de mayor peligro para la confidencialidad y seguridad de los datos personales. Por eso su empresa necesita un protocolo sencillo y a la vez muy riguroso para deshacerse de ellos.

Un simple CD o un minúsculo pendrive (memoria flash USB) pueden contener el equivalente a miles y miles de folios, almacenando en ellos enormes cantidades de datos personales e información confidencial. Deshacerse de ellos arrojándolos a la papelera o al cubo de basura puede poner en peligro toda la política de confidencialidad de su empresa. Siga los siguientes pasos para alejar de su empresa este riesgo.

• **DOS TIPOS DE HARDWARE.** Hay que diferenciar entre los restos informáticos de hardware que no contienen datos (teclado, ratón, lector de DVDs, etc.) y los residuos que sí los contienen o pueden contenerlos (CDs, DVDs, pendrives, discos duros internos o externos de un pc, portátil o servidor, etc.). Respecto a los que contienen datos de carácter personal es donde actúa la LOPD y en cuya destrucción deberá ser especialmente cuidadoso, para lo que puede seguir las pautas que siguen.

• **NUNCA A LA PAPELERA.** La regla general debe ser que nadie, bajo ningún concepto, se desprenda de ningún residuo o desecho informático depositándolo en la papelera o en la basura, ni siquiera inutilizándolo previamente.

• **DESTRUCTORA DE DOCUMENTACIÓN.** Si su empresa cuenta con una máquina destructora de documentación, asegúrese de si ésta, además de papel, también está preparada para la destrucción de CDs. Si aún no cuenta con una máquina de este tipo y se está planteando adquirir alguna, estudie la posibilidad de que sea capaz de destruir ambos formatos (papel y CDs).

• **EMPRESA DE DESTRUCCIÓN.** Plantéese contratar con una empresa especializada la destrucción de los residuos informáticos que se generen en su empresa. Estas empresas le proporcionarán un contenedor hermético en el que se van depositando los soportes de los que se quiere ir deshaciendo, que pasarán a recoger con la periodicidad que se acuerde, para posteriormente ser destruidos de forma segura. Su empresa puede decidir el nivel de seguridad que desee que se aplique a todo el proceso, y que deberá recogerse en un contrato.

CONSEJO: En el contrato de encargado de tratamiento (art. 12 de la LOPD) que firme con la empresa de destrucción y reciclaje mediante el que se comprometan a la completa destrucción de todo el material, conviene que establezca una penalización en caso de incumplimiento, que debería ser equivalente a las posibles sanciones que comporte la revelación o cesión inconsentida de datos personales.

• **REUTIZACIÓN.** Si los soportes van a ser reutilizados, deben entregarse al responsable de seguridad informática de la empresa para que sean

(sigue en la página siguiente)

Tres consejos extras sobre dispositivos informáticos

• Un **disco sin etiquetar** tiene muchas papeletas para acabar perdiéndose y terminar en la papelera. Por eso es importante que todos los dispositivos que se manejen en su empresa, estén correctamente identificados. En el caso de los CDs, es necesario utilizar un rotulador especial que permite escribir en su superficie.

• Hay que evitar usar pendrives para almacenar **datos confidenciales**. Si fuera necesario e inevitable hacerlo, debe borrarse su contenido inmediatamente cuando ya no sea necesario.

• Cuando se utilicen pendrives, y siempre que la situación en la que vayan a ser usados lo permita, es conveniente **cifrar los archivos** que se graben en ellos. Cifrar los datos hace que sólo puedan verse en el mismo ordenador en el que se grabaron (o en otro pero conociendo la clave), lo que asegura que nadie pueda acceder a ellos en caso de pérdida o robo.

(viene de la página anterior)

Residuos informáticos

formateados de nuevo, de forma que no se pueda recuperar ni acceder a la información que contenían antes. Si el nivel de seguridad que exigen los datos personales es alto, su empresa incluso puede plantearse la obligación de que los soportes que vayan a depositarse en el contenedor para su destrucción sean formateados previamente. De todas formas, tenga en cuenta que formatear un disco duro no garantiza que la información se borre, pues existen programas diseñados para recuperar la información de un disco formateado. Así que si la información es confidencial, se debe destruir el disco.

- **DOCUMENTO DE SEGURIDAD.** Incorpore su protocolo de destrucción de los desechos informáticos al documento de seguridad de su empresa. En el documento de seguridad, que debe estar siempre actualizado, se recogen las medidas de seguridad que deban aplicarse a los datos de carácter personal y a los sistemas de información de la empresa.

- **FORMACIÓN DE EMPLEADOS.** Informe a toda su plantilla del protocolo de destrucción de soportes informáticos que haya puesto en marcha su empresa y, si es necesario, realice periódicamente comunicaciones de recuerdo (circulares, recordatorios, etc.). Recuerde –y hágaselo saber así a su plantilla– que todo el personal que acceda a datos de carácter personal está obligado a conocer y observar las medidas, normas, procedimientos y reglas que establezca su empresa, así como al deber de secreto incluso después de finalizar su relación laboral con el titular del fichero o con su responsable.

Buenas prácticas

La entrega de nóminas, siempre en sobre cerrado

Por pequeña que sea su empresa y por seguro que parezca entregar la nómina en mano a cada trabajador, su empresa, como responsable del fichero de datos personales de los trabajadores, debe hacer la entrega de las nóminas siempre en sobre cerrado, aún cuando la entrega física la realice personal autorizado de la empresa.

La entrega del documento a la vista, aún en mano, no garantiza al cien por cien que no vaya a producirse pérdida o accesos no autorizados a los datos personales contenidos en el recibo de salarios por parte de terceras personas (que, además, podrían incluir datos personales de nivel alto, por ejemplo, el descuento salarial que se le aplica a un trabajador afiliado a un sindicato).

Nunca usar claves de acceso compartidas

Si entre los empleados hay confianza, y por facilitarse determinadas gestiones de su trabajo, pueden caer en la tentación de usar la misma clave de acceso a sus respectivos equipos informáticos o, si son distintas, comunicárselas unos a otros. Gran error. La normativa de protección de datos impone el uso de contraseñas que permitan la identificación de quien accede a los datos personales de forma inequívoca y personalizada, lo que sólo es posible si las contraseñas son personales y sólo las conoce cada usuario. Pero aunque la normativa es muy clara al respecto y su empresa tenga implantado un sistema de claves personalizadas, en el día a día entre empleados es posible que caigan en “malas prácticas” como revelarse las contraseñas o incluso dejarlas escritas en un post-it pegado a la pantalla por si alguien necesita acceder a su ordenador en su ausencia. Forme a sus empleados en la importancia de cumplir las normas que se implanten en la empresa en todo lo relacionado con la privacidad.

Formación específica para trabajadores extranjeros

Sus trabajadores deben ser sus mejores embajadores en el cumplimiento de las normas relacionadas con la privacidad y la protección de datos y su mejor escudo de defensa frente a posibles brechas de seguridad e incidencias. Está en juego la reputación de su empresa, la confianza de sus clientes y evitar sanciones por incumplimientos. Contar con una plantilla formada e implicada exige dedicación por parte de su empresa, especialmente en el caso de trabajadores extranjeros que no manejan a la perfección el español. Contemple la posibilidad de impartir esa formación en otros idiomas, o al menos los puntos clave de esa formación.

Opt-in / opt-out: cuál es cuál y cuándo aplicarlo

Cada tipo de destinatario de una comunicación comercial exige un tipo de consentimiento, que también varía en función del medio que se utilice para realizar la comunicación. Conozca cuál es cada tipo de consentimiento para saber cuándo aplicarlo.

En comunicación comercial, publicidad y marketing, opt-in y opt-out son dos términos que expresan con qué tipo de consentimiento se cuenta por parte del destinatario para poder enviarle publicidad. Así, en algunos casos se exige que se cuente con el consentimiento "opt-in" y en otros será suficiente con el "opt-out". El primero de ellos tiene además variantes:

- **OPT-IN.** Sólo se pueden enviar comunicaciones comerciales cuando se cuenta con el consentimiento previo e informado del destinatario, por lo que está prohibido todo tipo de comunicación comercial no consentida. Es decir, que la empresa que va a enviar publicidad debe contar con el consentimiento expreso e inequívoco del destinatario para poder hacerlo.

Ejemplo: una empresa coloca un formulario en su página web o blog para que los interesados en recibir sus promociones dejen su dirección de e-mail. Así, los que facilitan la dirección de e-mail están consintiendo recibir publicidad.

- **OPT-IN NOTIFICADO.** Una variante de este sistema sería el opt-in notificado (Notified Opt-in), por el cual cuando una persona deja sus datos personales para recibir publicidad (es decir, presta su consentimiento), recibe un mensaje de confirmación. Al mismo tiempo, se le daría en él la opción de solicitar su baja si ha cambiado de opinión o no ha sido él quien se ha dado de alta con sus datos.

Siguiendo con el ejemplo anterior, la persona que ha facilitado su dirección de e-mail rellenando el formulario de una web o blog recibiría inmediatamente un correo electrónico confirmándole su alta o preinscripción, agradeciéndole ésta y dándole la posibilidad de solicitar su baja en ese mismo momento a través de un link que se le facilita.

- **DOUBLE OPT-IN, consentimiento reforzado.** Es un sistema que se utiliza para enviar comunicaciones por e-mail por el cual una persona, para quedar inscrita en una lista de distribución, debe dar dos veces su consentimiento. Así, cuando se da de alta en algún servicio, recibirá inmediatamente un correo electrónico solicitándole que confirme su intención de suscribirse a través de un link. Si no lo hace, no queda dado de alta.

Este procedimiento no es legalmente obligatorio, pero sí es recomendable tanto desde un punto de vista de protección de datos personales como puramente de marketing. Así, aunque la lista que resulte de personas que hacen doble opt-in será probablemente más pequeña que la de las personas que dieron su consentimiento por opt-it (puesto que habrá un número de éstas que no confirmen), el double opt-in hace que la lista sea más cualificada (tendrá una tasa de apertura de los e-mails más alta, un índice de respuesta a las campañas también mayor, etc). El consentimiento, en cualquier caso, siempre puede ser revocado.

Siguiendo con el ejemplo, la persona que ha facilitado su dirección de e-mail recibiría inmediatamente un correo en el que le comunican que, para completar su alta, es necesario que confirme ésta haciendo clic en un link. Si no lo hace, no queda dado de alta y, si lo hace, recibe otro e-mail de confirmación.

- **OPT-OUT.** Permite el envío libre de comunicaciones comerciales siempre que se ofrezca al destinatario la posibilidad de solicitar la exclusión de la lista de envíos. Es decir, el destinatario recibe directamente una publicidad que él no ha solicitado, pero se le informa cómo puede darse de baja.

Legislación aplicable:

- Art. 7 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Art. 4.1 y 4.2 LOPD, y arts. 8 y 10 RLOPD, sobre calidad de datos.
- Art. 6 LOPD y arts. 12 a 17 RLOPD, sobre consentimiento.
- Art. 15 RLOPD, sobre solicitud del consentimiento en el marco de una relación contractual para fines no relacionados directamente con la misma.

Derecho de cancelación: cómo tiene que responder su empresa ante cada solicitud

Al recabar los datos de una persona para incorporarlos a un fichero, su empresa debe informarle, entre otras cosas, de sus derechos relacionados con la privacidad. Uno de ellos es el derecho de cancelación, es decir, de la posible futura petición a su empresa de que suprima sus datos personales de los ficheros. Sepa cuándo puede cancelar los datos en caso de que se lo soliciten y cuándo no debe hacerlo aunque se lo pidan, y cómo implantar un buen protocolo para responder a este derecho.

La normativa de protección de datos de carácter personal reconoce a los interesados, como titulares de sus datos, una serie de derechos que se conocen como "derechos ARCO" (Acceso, Rectificación, Cancelación y Oposición), que les otorgan un poder de control sobre aquellos datos que se encuentren sometidos a tratamiento, comunicación o cesión por parte de organismos públicos o entidades privadas.

Uno de ellos es el **derecho de cancelación**, que ofrece al ciudadano la posibilidad de solicitar la supresión de aquellos datos que resulten inadecuados o excesivos, y cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

Conviene que su empresa tenga bien definido un **protocolo interno de actuación** en su organización ante una solicitud del ejercicio del derecho de cancelación, para que el procedimiento sea ágil y efectivo, se cumplan los plazos de respuesta que impone la normativa y no se invierta en ello más tiempo del necesario. De esa forma, su empresa se asegura de cumplir con su obligación sin arriesgarse a ser sancionada. Las siguientes claves le ayudarán a elaborarlo:

1 Quien puede solicitarlo. El ejercicio del derecho de cancelación es "personalísimo", por lo que sólo puede ejercitarlo el titular de los datos. Pueden darse las siguientes situaciones:

- Que se efectúe directamente por el **propio interesado**. En este caso, debe acreditar su identidad mediante copia del DNI, pasaporte u otro documento de carácter equivalente que lo identifique. También es válida la firma electrónica. **¡Atención!:** Si la persona se encuentra en situación de incapacidad o es menor de edad, de forma que no puede ejercer de forma personal este derecho, podrá realizarlo su representante legal, siempre que éste acredite su condición.
- Que se lleve a cabo por un **representante legal** expresamente designado por el interesado para el ejercicio del derecho de cancelación. La identidad del representante deberá constar claramente acreditada, a través de copia del DNI, pasaporte u otro documento equivalente que lo identifique. **¡Atención!:** Este representante deberá disponer

Consejos para su prot

- ✔ Conviene que **designe a una persona como responsable**. Se trata de la persona a la que su empresa, como responsable del fichero, asigna formalmente la función de coordinar y controlar las medidas de seguridad aplicables a sus ficheros, y que tendría también la función de dar respuesta a las peticiones de derechos ARCO. Además de asegurar el conocimiento y aplicación de la legislación sobre protección de datos, garantizará una actuación más diligente.
- ✔ Para evitar posibles reclamaciones de la AEPD por vencimiento de plazo, es conveniente que en el protocolo interno de respuesta que usted establezca en su empresa se fije un **plazo menor para responder** (por ejemplo, responder en cinco días, en lugar de los diez con los que cuenta legalmente), de forma que su empresa tenga margen para posibles incidencias.
- ✔ Si su empresa no ha respondido al interesado respecto a la cancelación de sus datos personales dentro del plazo que tiene para ello, es preferible que lo haga superado ese plazo antes que no hacerlo. Si esa persona acude a la AEPD y, durante la tramitación del procedimiento contra su empresa, su empresa atiende el derecho, entonces la AEPD podría limitarse a estimar la reclamación por motivos formales e indicar que su empresa atendió finalmente dicho derecho, aun **fuera de plazo**, por lo que probablemente no le dirijirán

de un apoderamiento especial para ejercitar el derecho de cancelación en nombre del representado, por lo que no es válido un apoderamiento general.

- Cancelación de los datos de una **persona fallecida**. La normativa de protección de datos no se aplica a fallecidos, pero sus familiares podrán solicitar la cancelación de sus datos justificando tanto el fallecimiento como la relación con el fallecido que les permite solicitar la cancelación.

2 Procedimiento de solicitud. El ejercicio del derecho de cancelación deberá efectuarse mediante una comunicación (preferentemente por escrito, aunque la ley no obliga expresamente a ello), que deberá tener el siguiente contenido:

- Nombre y apellidos del interesado, junto con el mecanismo adecuado para acreditar su identidad (DNI, pasaporte, etc.).
- Dirección a efectos de notificaciones, fecha y firma.
- Documentos que acrediten el interés legítimo del afectado para solicitar la cancelación de sus datos.
- Petición en que se concreta la solicitud (es decir, aquellos datos a los que se refiere el interesado).

¡Atención! A fin de no desvirtuar el derecho que asiste al interesado, no es necesario que especifique en su solicitud los ficheros en los que se encuentran o pudiesen encontrarse contenidos los datos personales que pretende cancelar ya que, en la mayoría de los casos, esto será desconocido para el afectado.

El procedimiento para atender las solicitudes de cancelación deberá ser **sencillo y gratuito** (es decir, que la empresa no puede establecer un procedimiento que suponga un ingreso o una compensación económica para la entidad ante la que se ejercita el derecho). Tampoco se permite que su empresa exija la utilización de medios que impliquen un coste excesivo al interesado, como cartas certificadas, burofaxes, requerimientos notariales o servicios de telecomunicaciones que impliquen una tarificación adicional. El envío mediante correo ordinario (que tiene un coste, aunque reducido) se considera válido, por ser el timbre postal un precio público.

¡Atención!: No obstante, aunque el afectado no haya empleado el procedimiento establecido por la organización, se deberá atender su solicitud siempre que haya utilizado un medio que permita acreditar el envío y la recepción, y que la solicitud tenga el contenido mínimo (nombre y apellidos, dirección a efecto de notificaciones, etc.).

CONSEJO: Su empresa podría dar la posibilidad de que los interesados realicen la solicitud ante los servicios de atención al público y reclamaciones que ya existan en su empresa. En ese caso, la identidad del interesado quedaría acreditada simplemente empleando los mismos mecanismos internos establecidos para la identificación de clientes a través de dichos servicios; por ejemplo, muchas empresas que tienen habilitado este sistema facilitan un "código de referencia" (aunque sea telefónicamente) como justificante de que se ha ejercitado el derecho.

(sigue en la página siguiente)

rotocolo de actuación

ningún requerimiento adicional y se procederá al archivo de las actuaciones.

✔ En la gestión de las solicitudes que reciba su empresa, asegúrese de que quede constancia de las respuestas, puesto que sobre su empresa recae la **carga de la prueba**. Así, además de conservar las solicitudes, conserve la respuesta enviada y el certificado de acuse de recibo.

✔ La LOPD protege solamente los derechos de las personas físicas, lo que significa que el derecho de cancelación sólo puede ser ejercido respecto de datos de éstas, y no de **personas jurídicas**. Esto significa que si en su empresa se recibe una solicitud de cancelación en nombre y representación de una persona jurídica (por ejemplo, una sociedad mercantil), su empresa no tiene obligación de responder.

✔ Sea **extremadamente cuidadoso** con el bloqueo o la destrucción de los datos personales de la persona que ha ejercido su derecho de cancelación, instaurando los medios técnicos y humanos para impedir que vuelvan a ser objeto de tratamiento. Cuando alguien ha ejercido sus derechos ARCO, especialmente el de cancelación, es probable que se muestre especialmente intransigente si se produce un error que le lleva, por ejemplo, a recibir publicidad de su empresa. Si denunciara a su empresa ante la AEPD, incurriría en una infracción grave, sancionable con hasta 300.506,05 euros.

(viene de la página anterior)

Derecho de cancelación

3 Posibles actuaciones a adoptar ante la solicitud. Tanto si su empresa dispone de datos del interesado como si no, y tanto si puede cancelarlos como no, su empresa deberá responder al interesado. La respuesta puede ser alguna de las siguientes:

- Si su empresa **no tiene datos** suyos, deberá comunicárselo, declarando improcedente su solicitud.
- Si la solicitud que ha recibido **no reúne los requisitos formales** necesarios, deberá responder al interesado solicitando que los subsane.
- Si la solicitud ha sido **efectuada correctamente**, cumpliendo los requisitos formales necesarios, deberá resolver sobre la solicitud de cancelación, en un sentido positivo o negativo.

Por tanto, la solicitud de cancelación que cumpla los requisitos formales podrá ser:

a) CONCEDIDA, es decir, estimada. En este caso, su empresa debe identificar y bloquear los datos concretos objeto de la reclamación, a fin de impedir su tratamiento, comunicación o cesión posterior a partir de ese momento. Este bloqueo implica que los datos cancelados se conservan reservados a disposición únicamente de las administraciones públicas, jueces y tribunales para atender posibles responsabilidades nacidas tanto del tratamiento de los datos como de la relación que tenga su empresa con la persona que ejerza el derecho (por ejemplo, si se trata de un trabajador, de un cliente, etc.) y sólo durante el plazo de prescripción de esas responsabilidades (que es variable). Transcurridos dichos plazos, deberán ser suprimidos definitivamente, es decir, destruídos o borrados sin posibilidad posterior de recuperación. Sólo podrán conservarse de forma "disociada", imposibilitando totalmente la identificación del interesado (por ejemplo, con fines estadísticos).

¡Atención!: Si su empresa comunicó previamente a otra entidad los datos que ahora va a cancelar, deberá informar a ésta de la cancelación en un plazo máximo de diez días hábiles, para que ella proceda, a su vez y en ese mismo plazo desde la recepción de la notificación, a efectuar la cancelación correspondiente en sus ficheros.

b) DENEGADA, bien porque dichos datos deban ser conservados "operativos" durante los plazos previstos en las disposiciones legales aplicables o durante las relaciones contractuales vigentes entre su empresa y el interesado. Dichas relaciones justifican el tratamiento hasta la extinción de las mismas. Es decir, que su empresa también deberá denegar motivadamente la solicitud de cancelación cuando así lo disponga una ley o una norma de derecho comunitario de aplicación directa (en ambos casos, siempre que esas normas lo indiquen de forma explícita), o cuando éstas impidan revelar a los propios afectados el tratamiento o cesión de los datos (es decir, que se derive de la interpretación de cualquiera de ellas la imposibilidad de efectuar la cancelación solicitada). Es decir, que si existe una normativa (por ejemplo, tributaria o laboral) que impide que se puedan cancelar los datos o que permita u obligue a conservarlos, puede denegarse la cancelación de los mismos, haciéndoselo saber al reclamante.

La solicitud de cancelación puede no referirse a la **totalidad de los datos** que posea su empresa de esa persona, sino sólo respecto de **algunos**. Pero incluso aunque la persona solicite la cancelación de todos sus datos, quizá su empresa no pueda acceder a ella en su totalidad (por ejemplo, en cumplimiento de las disposiciones legales aplicables a la relación contractual vigente entre su empresa y el interesado), en cuyo caso deberá cancelar los datos que correspondan y dejar los demás sin bloquear.

En todo caso, ante una respuesta denegatoria (total o parcial), su empresa deberá informar al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos (AEPD) (art. 18 de la LOPD).

¡Atención!: Su empresa deberá siempre poder acreditar que ha cumplido su obligación de dar respuesta adecuadamente a la solicitud de cancelación de datos personales, ya que será su empresa quien tenga que demostrarlo ante la AEPD.

Puede descargarse en el **Archivo Online de Documentos** dos modelos de escritos de respuesta: un modelo concediendo la solicitud de cancelación y otro denegándola.

4 En qué plazo debe responder. Su empresa tiene un plazo máximo de diez días para responder al solicitante –sea cual sea el sentido de la respuesta– que empiezan a contar desde el momento de la recepción de la solicitud. En ese plazo deben computarse sólo los días hábiles (es decir, descontando los festivos). **¡Aten-**

(sigue en la página siguiente)

(viene de la página anterior)

Derecho de cancelación

ción!: El plazo de diez días es el que tiene su empresa para responder, aunque el afectado reciba la respuesta más allá de esos días.

Es muy importante responder dentro del plazo, pues si el solicitante no recibe respuesta puede dirigirse a la AEPD y presentar una "reclamación de tutela por denegación del derecho de cancelación".

5 Cómo debe responder. Su empresa debe responder por escrito a la dirección postal o, en su defecto, electrónica que facilitó el interesado en la solicitud o que conste en el documento oficial identificativo, utilizando un medio que permita acreditar el envío y la recepción. Esto último es muy importante, pues si finalmente la persona que le solicita información reclama a la AEPD, será su empresa quien deba acreditar que efectivamente atendió la solicitud. Su respuesta debe ir firmada por una persona con facultades de representación suficientes y en vigor.

6 Cómo puede reaccionar el solicitante. Si su empresa no responde al interesado dentro del plazo máximo de diez días hábiles, o se le ha denegado la cancelación de sus datos y el interesado no está de acuerdo, o bien considera que su empresa no le ha contestado satisfactoriamente, puede solicitar ante la AEPD la tutela por denegación del derecho de cancelación. La AEPD, tras estudiar el asunto, puede dar la razón a su empresa (desestimando la reclamación dirigida contra ésta con el archivo del expediente) o bien reconocerla al ciudadano (estimándola), instando en ese caso a su empresa a responder adecuadamente en el plazo de diez días, pudiendo incurrir en una infracción de no hacerlo.

Contra la resolución emitida por parte de la AEPD, tanto su empresa como el afectado podrán interponer recurso contencioso-administrativo ante la Audiencia Nacional.

También pudiera ocurrir que durante la tramitación del procedimiento ante la AEPD la persona que ha reclamado contra su empresa desista en su reclamación, en cuyo caso, si no se han personado otros afectados, la AEPD, a la vista de las circunstancias concurrentes, y siempre que no tenga obligación de actuar de oficio en garantía de los derecho en juego, aceptaría el desistimiento y se terminaría el procedimiento contra su empresa.

Stéfanos Altidis Cabrejas,
Abogado especialista en protección de datos personales

Infracciones y sanciones

Se considerará infracción **leve** de la LOPD que su empresa no atienda, por motivos formales, la solicitud de cancelación cuando legalmente proceda; infracción **grave** el no llevar a cabo las cancelaciones de datos de carácter personal que legalmente se establezcan; e infracción **muy grave** la desatención u obstaculización sistemática por parte de su empresa del ejercicio del derecho de cancelación.

En el primer caso, la multa podría estar comprendida, entre 601,01 y 60.101,21 euros; entre 60.101,21 y 300.506,05 euros en el segundo, situándose, en el tercer supuesto, entre 300.506,05 y 601.012,10 euros.

Cancelación "de oficio"

La normativa exige que la cancelación se produzca "de oficio" por parte de su empresa (es decir, sin que se lo haya solicitado previamente el interesado) cuando:

- Los datos del afectado sean **inexactos** (en todo o en parte) o incompletos, debiendo ser sustituidos por los que sean correctos y se adecuen a la situación real del afectado (por ejemplo, su empresa deberá cancelar los datos cuando tenga conocimiento de la defunción del sujeto). Debe llevarse a cabo en un plazo de diez días hábiles desde que se tuviese conocimiento de la inexactitud, teniendo en cuenta en cualquier caso la obligación de mantener operativos los datos durante los plazos previstos en las disposiciones legales aplicables.

- Cuando los datos **dejen de ser necesarios o pertinentes** para la finalidad para la que hubiesen sido recabados o registrados. En este caso, los datos se pueden conservar bloqueados mientras le puedan ser exigidas responsabilidades derivadas de relaciones u obligaciones jurídicas, de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado. Finalizados estos plazos, los datos deben suprimirse.

Solicitar la baja no es lo mismo que solicitar la cancelación

El hecho de que un cliente solicite darse de baja en la prestación de servicios (sean de pago o gratuitos) que facilita una empresa no significa que esa persona esté solicitando la cancelación de sus datos personales que obren en poder de éste. Otra cosa sería que, a la vez que solicita su baja en el servicio, solicite también la cancelación de sus datos siguiendo el procedimiento adecuado para ello.

Tribunales

DESCARGA DE SENTENCIAS: En el Archivo Online de Documentos podrá acceder con su contraseña de acceso a las sentencias íntegras que se mencionan en esta sección.

www.practiletter.com

Tribunal Supremo

300.000 euros a una residencia por entregar datos de ancianos a la farmacia para comprar medicamentos

El Tribunal Supremo ha confirmado la sanción de 300.506,05 euros que la AEPD había impuesto a una residencia de ancianos -y que ya había ratificado la Audiencia Nacional- por haber facilitado a una farmacia cercana un listado con datos personales de algunos residentes para que ésta pudiera ir cargando en sus cuentas los medicamentos que los ancianos iban necesitando.

Los hechos suponen por parte de la residencia de ancianos una **infracción muy grave** por haber cedido datos de los afectados a terceras personas sin el consentimiento de éstas (art. 11.1 de la LOPD). Por parte de la farmacia también suponen una **infracción de carácter grave**, por haber tratado esos mismos datos personales sin el consentimiento de los afectados (art. 6 de la LOPD), por lo que la Audiencia también ratifica la sanción de 60.101,21 euros a la farmacia que impuso la AEPD.

La inspección de la AEPD se desencadenó cuando los familiares de tres ancianos internos en la residencia presentaron tres denuncias idénticas ante la AEPD contra la farmacia por estar cargando importes correspondientes a medicamentos en sus respectivas cuentas bancarias. La farmacia explicó entonces que correspondían a pedidos de medicamentos que hacía directamente la residencia de ancianos para atender a las necesidades de éstos.

Los residentes de la residencia facilitaban a ésta sus datos personales como parte de la relación contractual que les une, de forma que la residencia contaba con el consentimiento de éstos para tratar esos datos. Algunos de los medicamentos que precisaban los internos estaban cubiertos por la Seguridad Social, pero no todos, de forma que la residencia entregó a la farmacia un listado con los nombres y apellidos, sus DNI y los números de cuenta bancaria de algunos residentes para que pudieran cobrarles directamente los medicamentos y productos de parafarmacia que no cubría la Seguridad Social, dado que los ancianos no contaban con dinero en metálico. Sin embargo, el contrato que había firmado la residencia con cada uno de los ancianos no contemplaba la cesión de los datos personales a un tercero, lo que está en el origen de las infracciones.

"*Esta Sala no está en condiciones de determinar cómo se debe proceder al suministro de medicamentos a las personas más o menos imposibilitadas que se encuentran en una residencia, pues es una cuestión ligada a la organización empresarial*" -expone el Tribunal Supremo en su sentencia-, "pero lo que sí se puede afirmar es que el mecanismo ideado produce claras infracciones de los derechos a la protección de datos de las personas ingresadas", por lo que ratifica las sanciones, tanto a la residencia como a la farmacia (sent. del TS de 8.10.10).

¡ATENCIÓN!: ¿En qué falló la residencia de ancianos? En no haber informado a los residentes (o a sus familiares) en el contrato de prestación de servicios que firmaron de que, dentro de la asistencia integral que prestaban a los internos, era necesaria la cesión de datos personales a la farmacia para que ésta pudiera atender y cobrar cada pedido. Igualmente debía haber firmado un contrato de encargado de tratamiento con la oficina de farmacia que legalizara el acceso de ésta al fichero de datos personales del que era responsable la residencia.

¿Y en qué falló la farmacia? En la resolución de la AEPD, ésta argumentó al imponer a la farmacia la sanción de 60.101,21 euros que "no tuvo ninguna diligencia, ni siquiera la de realizar una mera consulta a la residencia sobre si contaba con el consentimiento informado para ceder los datos". Así pues, el error de la farmacia fue aceptar sin más los datos personales que le confió la residencia para poder realizar la transacción.

➡ Esta sentencia viene a recordar la rigurosidad de la AEPD –ratificada por el Tribunal Supremo-, cuando pudiera pensarse que al tratarse de facilitar el suministro de medicamentos de interés vital para los ancianos no se aplicaría el mismo criterio que si se tratase de operaciones comerciales.

Las empresas ante la AEPD

(viene de la página 12)

consentimiento previo del destinatario para el envío de mensajes SMS o correos electrónicos salvo que exista una relación contractual entre quien envía el mensaje y quien lo recibe y, además, cuando el sujeto que lo recibe no manifieste su oposición a recibir mensajes comerciales (art. 21.1 de la Ley 34/2002 de Servicios de la Sociedad de la Información y Comercio Electrónico –LSSI-). La condición de cliente existía en este caso, pero también que ese cliente había manifestado expresamente su voluntad contraria a recibir mensajes comerciales, una voluntad que la operadora de telefonía no respetó.

Asimismo, la resolución de la AEPD recuerda también que el envío de comunicaciones comerciales no solicitadas puede considerarse una infracción leve o grave en función del número de envíos que se realicen y en qué plazo de tiempo. Así, más de tres comunicaciones a un mismo destinatario en el plazo de un año ya se consideraría un envío masivo, una infracción calificada como grave que se aplicaría en este caso, puesto que el destinatario recibió 13 mensajes en unos pocos meses.

Por ello, la Agencia impone a la operadora una multa de 30.000 euros como autora de una infracción grave por el envío masivo de comunicaciones comerciales no solicitadas -arts. 38.3 y 38.4 de la LSSI- (PS/00211/2010 de la AEPD de 16 de septiembre de 2010).

Multa de 180.000 euros por no haber comprobado la identidad de un supuesto cliente y terminar incluyéndolo en un fichero de morosos

Un particular denunció ante la AEPD a una empresa de televisión por satélite y a su distribuidora porque, según él, nunca suscribió sus servicios y le terminaron incluyendo en un fichero de morosos por una supuesta deuda de 405 euros.

Como **pruebas** aportó un contrato que recibió a su nombre con todos sus datos, incluso los bancarios de domiciliación de recibos, firmado con una rúbrica que él no reconoce como suya; la carta en la que le comunican la resolución del contrato por no haber pagado y le solicitaban su pago; una carta de una empresa de cobro de deudas instándole a pagar, y otra carta comunicándole su inclusión en un fichero de morosos. También aportó la carta que él escribió a la empresa tras recibir el contrato diciendo que él no había contratado esos servicios y facilitando la copia de su DNI y la última carta que les escribió pidiendo que cancelaran sus datos. En definitiva, y al denunciar los hechos ante la AEPD, alegaba que los datos personales que manejó la operadora de televisión y que se incluyeron en el fichero de morosos eran veraces, pero que ni él contrató esos servicios ni la firma del contrato era suya.

En sus alegaciones ante la AEPD, la empresa demostró que el contrato se firmó en persona por alguien que se encontraba en el domicilio del denunciante y que facilitó todos sus datos a un trabajador de la empresa distribuidora de los servicios (por lo que aventuran que lo debía haber hecho con el consentimiento de éste) y también quedó demostrado que desde ese domicilio se había hecho uso del servicio, e incluso se habían comprado partidos de fútbol desde la terminal.

La AEPD tiene claro que se cometieron **tres infracciones graves de la LOPD**, que parten del hecho de que no se tomaron las debidas cautelas ni se instauraron los procedimientos adecuados para poder comprobar la autenticidad del contrato y la identidad del contratante, de forma que no se verificó su consentimiento para el tratamiento de sus datos que implicaba el alta en el servicio.

Así, la AEPD impone tanto a la operadora de televisión digital como a la distribuidora del servicio una multa de 60.101,21 euros a cada una de ellas por el tratamiento inconsentido de los datos personales del denunciante (art. 6 de la LOPD) y, además, otra multa de otros 60.101,21 euros a la operadora de televisión por una infracción del principio de calidad de los datos en relación a la inclusión de los datos del denunciante en el fichero de morosos -art. 4.3 en relación con el 29.4 de la LOPD- (PS/00098/2010 de la AEPD de 14 de septiembre de 2010).

Las empresas ante la AEPD

La Agencia Española de Protección de Datos (AEPD) es el "guardián" de la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD). Entre sus funciones está velar por su cumplimiento, lo que se traduce en atender las denuncias e investigar y, llegado el caso, sancionar (con multas de entre 601 y 601.012 euros) a todas las empresas que considere que han incumplido la normativa. Éste es un resumen de algunas de sus últimas resoluciones.

Un error atribuible a la "mecánica bancaria" no infringe la LOPD

Un particular que tenía suscrita una póliza con una entidad de asistencia sanitaria privada para él y su familia recibió un cargo de la aseguradora por importe de seis euros en una entidad bancaria en la que tenía una cuenta, pero que no era en la que tenía domiciliados los recibos. El asegurado no entendía cómo podía haber ocurrido, así que acudió en busca de una explicación tanto a la entidad de asistencia sanitaria como al banco en el que recibió el cargo, aclaración que no supieron darle, y este último anuló el cargo. Ante la falta de explicaciones, denunció los hechos ante la AEPD.

Tras la investigación, la AEPD descubrió lo que había ocurrido: la entidad sanitaria emitió por error el cargo de seis euros al banco en el que finalmente se le cargó, pero que no era en el que el titular había domiciliado los pagos. Sin embargo, casualmente, el titular también tenía cuenta en ese otro banco, por lo que se hizo el cargo. Se trató así, según la AEPD, de una "simple anomalía de mecánica bancaria" y no de ninguna infracción de la normativa de protección de datos.

La AEPD, por lo tanto, **archiva el procedimiento** sancionador, puesto que considera que los errores bancarios quedan excluidos del ámbito de la LOPD y todas las entidades involucradas cumplían perfectamente sus obligaciones en materia de privacidad y protección de datos personales. Sin embargo, matiza que "cuestión distinta será la vulneración o no de la normativa bancaria", pero recuerda que ellos no se encargan de velar por su cumplimiento (PS/00296/2010 de la AEPD de 22 de septiembre de 2010).

30.000 euros de sanción por enviar a un cliente promociones pese a haber pedido éste que no lo hicieran

Un cliente de una empresa de telefonía móvil adquirió un terminal con tarjeta prepago. Al firmar el contrato, marcó con una señal X las casillas en las que indicaba que no deseaba recibir publicidad de la entidad, ni que se cedieran sus datos a otras empresas del grupo, ni tampoco que se trataran sus datos con fines comerciales. Pese a ello, al día siguiente recibió el primer mensaje SMS de texto en su móvil con una oferta para hacer una recarga de saldo, y recibió 12 más en los tres meses siguientes con variadas ofertas del mismo tipo.

El cliente entendió que no habían hecho caso a su voluntad de no recibir publicidad y lo denunció ante la AEPD. Durante la investigación se puso de manifiesto que la compañía contaba con un sistema propio por el que se excluían de las campañas promocionales a quienes no querían recibir publicidad, que formaban parte de un fichero "Robinson" que había creado la empresa. Sin embargo, el argumento que daba la empresa para que ese cliente concreto hubiera recibido esos mensajes es que éstos "*no eran comunicaciones comerciales en sentido estricto*", sino "*informaciones a los clientes de prepago sobre los beneficios que les podía reportar hacer una recarga*". Según la compañía, los servicios de modalidad prepago requieren que los titulares realicen recargas periódicas para poder mantener la línea telefónica, y esto hacía que los mensajes no pudieran ser considerados como mera publicidad, sino que quedaban amparados por la legalidad.

La AEPD no comparte en absoluto ese argumentos, pues considera que se ha producido una verdadera "**comunicación comercial**", definida como toda forma de comunicación dirigida a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional.

Además, la AEPD recuerda que es necesario el

(sigue en la página anterior)