Boletín 02/12

LOPD EN LA EMPRESA

comSeveral
TIEMPO COSTE CALIDAD

LA LOPD EN EL DÍA A DÍA

Cómo proteger el acceso a los datos en formato automatizado (parte II)

Contenido

(Continuación)

Proteger el acceso a los recursos del servidor

- Los recursos (carpetas compartidas, aplicación de gestión, etc.) del servidor donde se ubiquen datos personales no deben tener, por defecto, el acceso permitido a nadie. Posteriormente se irá concediendo acceso a los usuarios autorizados que se den de alta.

Proteger el acceso a las aplicaciones

- Para poder acceder cualquiera de las aplicaciones que utilice la organización en las cuales se traten datos personales, se debe introducir el nombre de usuario la contraseña asociada al mismo.

Proteger el acceso a los puestos de trabajo

- Se debe limitar el acceso al sistema operativo de los puestos de trabajo a los usuarios debidamente autorizados. No se debe poder acceder a ningún sistema sin introducir el correspondiente nombre de usuario y contraseña de acceso o cualquier otro método alternativo que garantice que la persona que está accediendo está autorizada a hacerlo.

A TENER EN CUENTA

No vale solo con tener documentados los procedimientos en el Documento de Seguridad. Han de cumplirse dichos procedimientos.

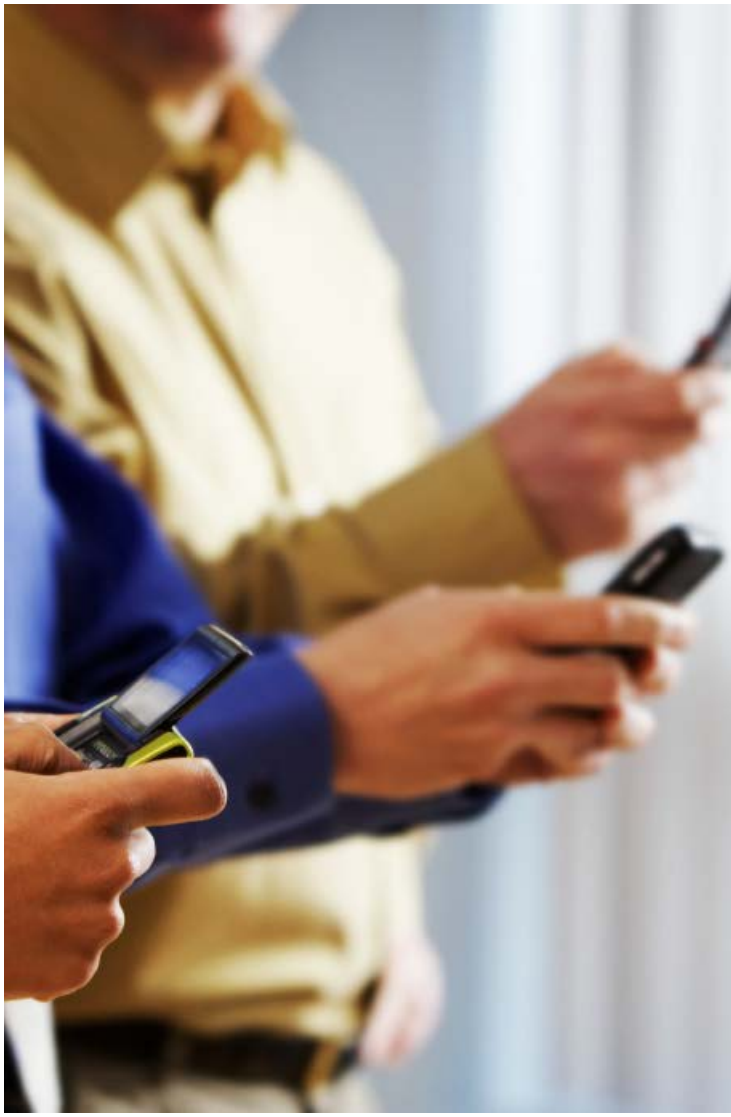
SANCIONES DE LA AEPD

Sanción por no atender revocación de consentimiento

La organización debe establecer procedimientos para el ejercicio de los derechos de los titulares.

En el procedimiento sancionador **PS/00307/2011** de la AEPD podemos ver la sanción que puede sufrir una entidad por **no hacer caso a una revocación del consentimiento prestado para recibir SMS.**

Con fecha 11 de agosto de 2010 tiene entrada en la AEPD un escrito de D. A.A.A., en el que declara que tras haber sido usuario de GAY CONTACTOS (www.gay-contactos) ha estado recibiendo SMS sin autorización. A pesar de haber solicitado reiteradamente no recibir mensajes ha continuado recibiéndolos.



Durante la actuación inspectora de la AEPD ha quedado **acreditado** que el **usuario intentó por varios medios oponerse a la recepción de SMS**, siendo infructuosos sus esfuerzos, pese a la recepción de mensaje confirmando su baja.

A este respecto, en cuanto a las alegaciones relativas a la carencia de requisitos formales en las solicitud de cancelación realizada por el denunciante, concretamente a la no acreditación de la identidad, hay que señalar que la regulación que cita la entidad denunciada es para lo referente a la normativa de protección de datos de carácter personal, y en el presente caso, estamos ante un **incumplimiento de los derechos** de los usuarios de servicios de telecomunicaciones que tutela la LSSI.

En concreto, **ni se ofrecía un medio de oposición en cada comunicación comercial, ni se hizo caso al denunciante** cuando manifestó esta oposición por otros medios

Resultado: Sanción de 30.001 € por una infracción del artículo 21 de la LSSI, tipificada como grave.

IMPORTANTE

En cada comunicación comercial electrónica que se envíe a un destinatario debe indicarse el procedimiento para que pueda oponerse a seguir recibiendo dichas comunicaciones.

LA AEPD ACLARA

Plazo de conservación de datos personales

El informe 0408/2010 de la AEPD resuelve la consulta planteada sobre el **plazo legalmente establecido para poder proceder a la destrucción de la documentación** obrante en sus ficheros.

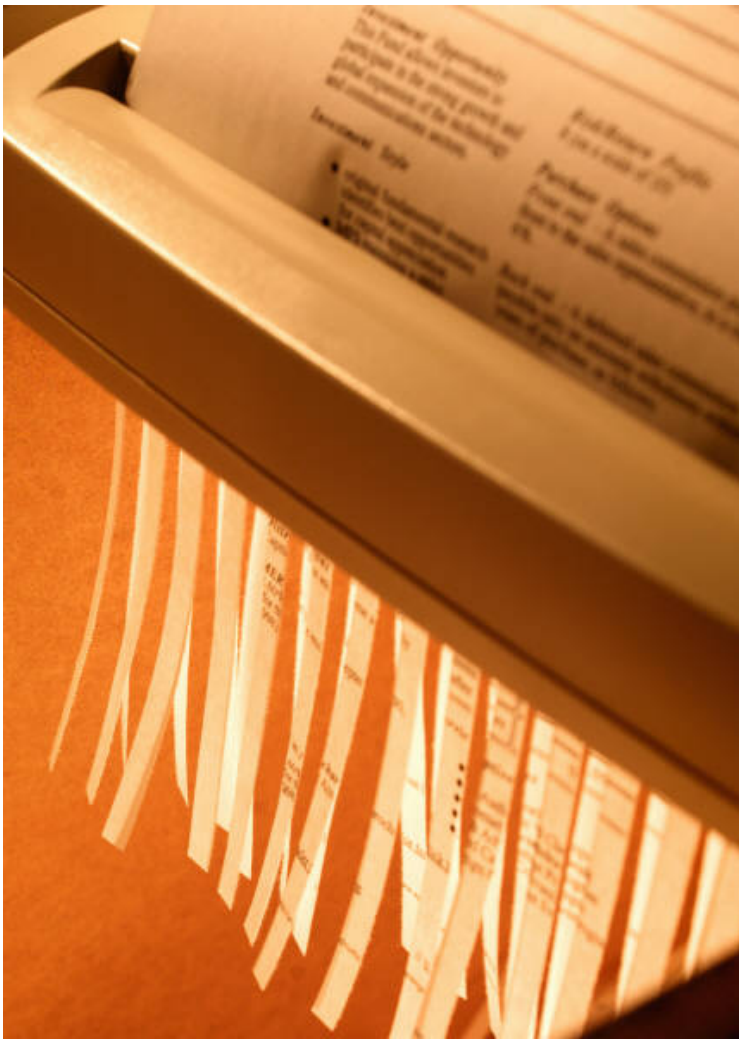
De dicho informe jurídico se extrae lo siguiente:

a) Resulta **imposible establecer una enumeración taxativa de los periodos en que el dato habrá de permanecer bloqueado**, está deberán fundamentarse en lo dispuesto "en las disposiciones aplicables" o a la "atención de las responsabilidades nacidas del tratamiento".

b) Los datos deberán, pues, **cancelarse una vez hayan dejado de ser necesarios para la finalidad para la que se recabaron**.

c) **Primero** deberán mantenerse **bloqueados** al menos durante el tiempo necesario para la prescripción de las acciones que pudieran derivarse de la relación jurídica que vincula a las dos partes, así como los derivados de la normativa tributaria, el plazo de prescripción de 3 años de la Ley Orgánica de Protección de Datos, o los establecidos en otras normas con rango de Ley que resulten de aplicación al caso.

d) **Por último**, una vez hayan transcurrido dichos plazos, se deberán **suprimir** los datos.



A TENER EN CUENTA

No hay una regla fija para la eliminación de datos personales.

ACTUALIDAD LOPD

Nueva web de la Agencia Española de Protección de Datos

Fuente: www.agpd.es

EL PROFESIONAL RESPONDE

¿Es lo mismo un parte de baja que un parte de accidente laboral de cara al nivel de seguridad a aplicar?

El parte de baja laboral que entrega un trabajador a la empresa no ha de contener más datos que la fecha y la situación de baja por enfermedad, pero sin dar datos concretos de la enfermedad que ha provocado la mencionada baja.

En este caso, podemos aplicar la excepción del art. 81.6 de RD1720/2007, que establece:

"También podrán aplicarme medidas de seguridad de nivel básico a los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad, o a la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos".

Con lo cual, es posible aplicar **medidas de seguridad de nivel básico a dichos partes de baja** laboral.

En cambio, un **parte de accidente laboral** contiene más datos de los estrictamente mencionados antes (en concreto, contiene el accidente sufrido y las lesiones ocasionadas) que hacen que no sea posible acogerse a la excepción señalada en el párrafo anterior, siendo necesario **aplicar medidas de seguridad de nivel alto** a dichos datos.

A TENER EN CUENTA

Es muy importante segregar correctamente los ficheros para aplicar el nivel de seguridad que corresponde según los datos que contienen.