Boletín 01/11

LOPD EN LA EMPRESA

comSeveral
TIEMPO COSTE CALIDAD

LA LOPD EN EL DÍA A DÍA

¿Deben estar todos los datos personales bajo llave?

El artículo 107 del RD1720/2007 establece que:

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura.

Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

Es decir, que **todos los archivadores, carpetas, documentos**, etc. que contengan datos personales **deberán estar almacenados en armarios** (u otro mobiliario) **que dispongan de cerradura** y deberán estar cerrados cuando no sea necesario acceder a ellos.

Excepción:

Cuando los **armarios no dispongan** de dichas **cerraduras**, se podrán almacenar soporten con datos personales siempre que **se adopten otras medidas** que impidan el acceso a los soportes por parte de personas no autorizadas.

Ejemplos de medidas alternativas:

- Que los soportes estén en un recinto cerrado con llave y se cierre cuando no se esté accediendo a dichos soportes.
- Que los soportes estén vigilados en todo momento por personal autorizado, no dejando sola a ninguna persona no autorizada.

Contenido

IMPORTANTE

Los armarios, cajoneras y demás dispositivos que se utilizan para almacenar los soportes deberán estar descritos en el documento de seguridad, así como la relación de personal que tiene acceso a los mismos.

SANCIONES DE LA AEPD

Sanción por enviar SMS sin cumplir los requisitos legales

En el procedimiento sancionador PS/00278/2010 de la AEPD podemos ver la importancia que tiene la inclusión de las cláusulas pertinentes en cada comunicación electrónica que se envía con fines publicitarios.

"Antes de realizar una campaña de marketing hay que revisar las implicaciones legales."

Según los hechos, una ciudadana que recibió un SMS de la empresa JET MULTIMEDIA ESPAÑA S.A. (JET) que decía: *"Publi: El telefono ####### ha sido seleccionado para poder ganar 3000 euros. Si quieres conseguirlos envia la palabra ORO al ### -1,5e/sms"* denunció el hecho ante la AEPD por considerarlo un envío comercial no solicitado.

La AEPD después de investigar el caso, **sancionó a JET con 600,00€** por una infracción de la LSSI:

d) El envío de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente cuando en dichos envíos no se cumplan los requisitos establecidos en el artículo 21 y no constituya infracción grave".

"En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija."

El requisito que faltaba en dicho mensaje es que no ofrecía al destinatario del mismo un procedimiento sencillo y gratuito para que pueda oponerse al tratamiento de sus datos con fines promocionales.

IMPORTANTE

Antes de mandar cualquier comunicación comercial a los clientes, debemos estar seguros que se cumplen los requisitos legales que exige el envío que se realiza.

Previo al inicio de cualquier campaña de marketing hay que analizar las implicaciones legales que tiene y los posibles inconvenientes que pueden surgir.

LA AEPD ACLARA

Conservación de las historias clínicas

El informe 0443/2010 de la AEPD aclara la forma y plazos de conservación de las historias clínicas de pacientes por parte de los centros sanitarios.

De dicho informe jurídico se extrae lo siguiente:

- **Cada centro archivará las historias clínicas de sus pacientes**, cualquiera que sea el soporte papel, audiovisual, informático o de otro tipo en el que consten, de manera que queden garantizadas su seguridad, su correcta conservación y la recuperación de la información.

- **La Ley permite la conservación de la historia clínica en un soporte distinto del original**, siempre que quede preservada su autenticidad, seguridad e integridad.

- Dicha historia debe **conservarse durante un mínimo de cinco años** desde el último episodio asistencial.

- Hay que tener en cuenta la finalidad de la historia clínica: es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente, con lo cual, **aparte del plazo mínimo, será preciso considerar la relevancia y trascendencia de cada episodio** de asistencia **sobre futuros episodios** que pudieran tener lugar.

- Cuando sea necesario el **consentimiento, corresponderá al centro sanitario la prueba de su obtención.**

A TENER EN CUENTA

Aunque el **plazo mínimo** de conservación de la historia clínica **es de 5 años de forma general**, este **plazo depende de la comunidad** autónoma en la que esté ubicado el centro sanitario, **llegando a ser de hasta 20 años** en algunas de las comunidades autónomas.

ACTUALIDAD LOPD

Estudio sobre la seguridad de la información y la e-confianza en los hogares españoles

Fuente: www.inteco.es

Puede descargarse este estudio desde:

http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Estudios_e_Informes_1/Estudio_hogares_3T2010

EL PROFESIONAL RESPONDE

¿Quién debe ser el Responsable de Seguridad?

Cuando se implanta la LOPD en una entidad que trata ficheros de nivel medio y/o alto y llega la hora de definir al Responsable de Seguridad, suelen surgir dudas sobre la persona más adecuada para desempeñar dicho cargo.

¿Personal técnico ó jurídico?

Aunque la primera impresión es escoger personal técnico, hemos de recordar que la implantación de las medidas de seguridad técnicas es tan sólo una de las obligaciones que exige el cumplimiento de la LOPD, pero el resto de las obligaciones (información, consentimiento, contratos, etc.). son legales.

Lo ideal es que sea personal con **conocimientos jurídicos en protección de datos**, y asesorado si es necesario, por el personal técnico para la implantación correcta de las medidas de seguridad que exige la LOPD.

"Elegir bien al Responsable de Seguridad es fundamental para la aplicación y control de las medidas de seguridad"

¿Trabajador ó mando intermedio?

El correcto cumplimiento de la LOPD exige que se modifiquen, a veces, ciertos aspectos de la operativa diaria (guardar bajo llave la documentación, nombre de usuario y contraseña, etc.).

Si la persona que tiene que hacer cumplir dichas medidas no cuenta con mando suficiente para poder "persuadir" a aquellos que no quieren aplicarlas ó está en un nivel inferior a ellas, va a ser muy, pero que muy difícil que la entidad cumpla con las medidas que impone la Ley.

El perfil ideal para esto es el de mando intermedio ó directivo.