Boletín 02/13

LOPD EN LA EMPRESA

AUTOR: JULIO CÉSAR MIGUEL PÉREZ

LA LOPD EN EL DÍA A DÍA

Mucho cuidado con los programas para compartir ficheros (eMule, Ares, etc.)

Mucha gente tiene **instalado en el ordenador programas P2P** como eMule, Ares, Torrent, etc., sin darse cuenta que están **expuestos a un gran riesgo**, ya que dichos programas se basan en compartir ficheros de una carpeta. Carpeta en la que, accidentalmente podemos colocar cosas que no deben compartirse...

Para muestra, un ejemplo: «En septiembre de 2010 recibí un mensaje de una persona advirtiéndome de que **mi DNI estaba en Emule**. Mi pareja de entonces recordó que fue él quien **lo subió sin mala intención, al escanearme el DNI** por un tema laboral y que, al parecer, **quedó grabado en la zona de descargas de Emule**». De esta forma comienza la palentina S. A. T. Y., de 30 años su angustioso relato por una situación que, lejos de solucionarse, cada día que pasa se complica más a tenor de las denuncias y requisitorias judiciales que le van llegando **reclamándole importantes cantidades de dinero**.

Y es que, utilizando la imagen escaneada de su DNI **han abierto cuentas a su nombre** en distintas entidades financieras, así como **varios créditos** que ahora le reclaman.

Fuente: Diario Palentino.es (15/02/2013).
Para ver la noticia completa pulse aquí.

Contenido

A TENER EN CUENTA

Si accidentalmente compartimos, por ejemplo, la base de datos de clientes, nos enfrentamos a una sanción de hasta 600.000€.

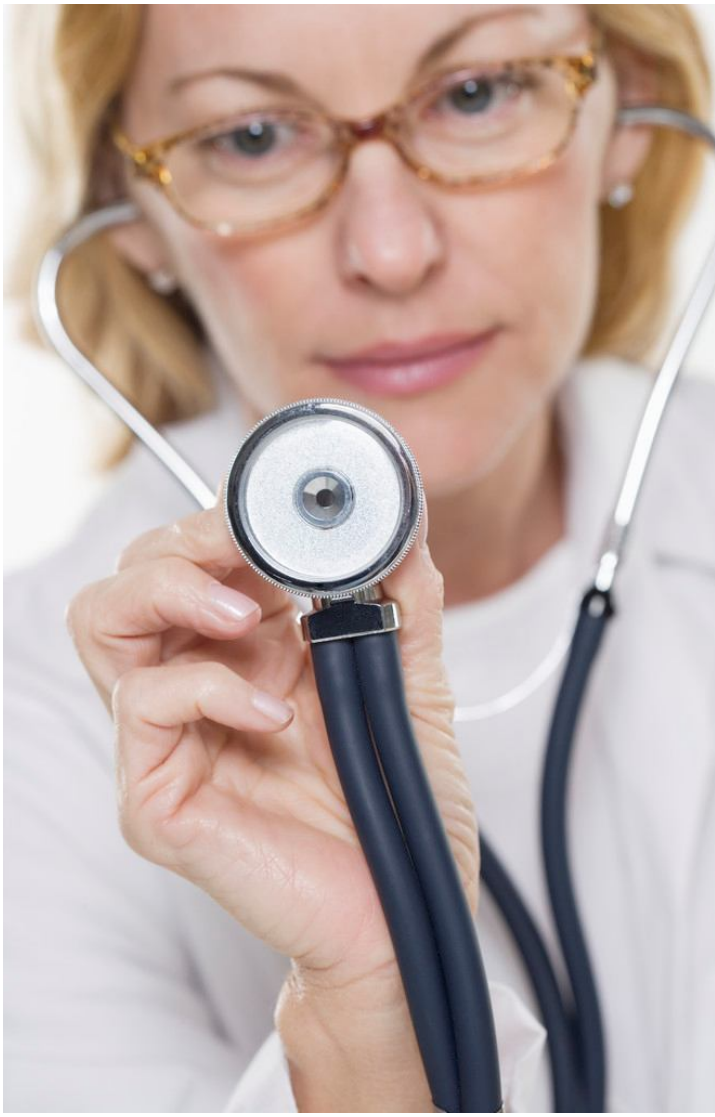
SANCIONES DE LA AEPD

Sanción por ceder datos de colegiado

En la resolución R/03127/2012 de la AEPD se puede ver la **sanción que puede sufrir un colegio profesional por ceder datos personales de un miembro sin recabar su consentimiento.**

Antes de ceder datos personales hay que asegurarse de contar con el consentimiento del titular de los datos.

Con fecha 14/07/2011, tuvo entrada en la AEPD un escrito de DÑA. A.A.A. (en lo sucesivo la denunciante) en el que denuncia que sus datos bancarios han sido facilitados por la entidad COLEGIO OFICIAL DE MÉDICOS DE ALICANTE (en lo sucesivo COLEGIO DE MEDICOS) a la compañía aseguradora AmTrust Europe Limites y a la entidad SEGUROS MEDICOS COLEGIALES ALICANTE, CORREDURIA DE SEGUROS, S.L. (en lo sucesivo SEMECO), que se encarga de la gestión de los seguros médicos.



En su escrito de denuncia añade que, a comienzos de 2011, procedió a la devolución de un recibo cargado en su cuenta bancaria de la entidad CAM de la compañía AmTrust Europe Limites, emitido y tramitado a través de SEMECO y correspondiente a un seguro complementario de responsabilidad civil, que no deseaba seguir manteniendo. Sin embargo, el 17/05/2011 **recibe otro cargo en su cuenta de Barckays; cuenta que no había proporcionado a SEMECO**.

Durante el procedimiento de inspección, La entidad **COLEGIO DE MEDICOS reconoció que facilitó a la entidad SEMECO la cuenta bancaria** designada por la denunciante para la domiciliación de la cuota colegial, abierta por la misma en la entidad Barclays Bank, S.A., que había sido aportada por la misma al COLEGIO DE MEDICOS para la domiciliación de la cuota colegial.

Resultado: Sanción de 6.000€ a la entidad COLEGIO DE MEDICOS y sanción de 10.000€ a la entidad SEMECO, por vulneración de los artículos 11 y 6.1 de la LOPD, respectivamente.

IMPORTANTE

La cesión no consentida de datos personales es una de las prácticas que la LOPD pretende erradicar, y por tanto, la que tiene consecuencias más graves.

LA AEPD ACLARA

Tarjetas identificativas de los trabajadores

El informe jurídico 0028/2011 de la AEPD resuelve la consulta planteada sobre si resulta adecuado a la Ley Orgánica 15/1999 (LOPD), la **inclusión del nº de D.N.I. y la fotografía, además del nombre y los dos apellidos, en las tarjetas identificativas que los trabajadores** deben llevar en lugar visible mientras prestan servicios en la empresa.

De dicho informe jurídico se extrae lo siguiente:

a) **La inclusión del dato de D.N.I. en las tarjetas identificativas del personal no vulnera el principio de proporcionalidad**, al no resultar dicho tratamiento excesivo para la finalidad de identificación del personal.

b) Respecto al tratamiento de la **imagen de los trabajadores** y la legitimidad para su realización, se señala por la Agencia que "Igual argumentación cabe aplicarse a la inclusión en las tarjetas identificativas de la fotografía del trabajador, **no pudiendo al misma considerarse excesiva** a los efectos previstos en el artículo 4.1 de la LOPD".

c) Por otra parte, la finalidad que justifica la inclusión de los datos del DNI y la fotografía de los trabajadores en sus tarjetas es garantizar su identificabilidad en el desempeño de sus funciones, por lo que el tratamiento de los datos **no precisa recabar el consentimiento de los afectados**, sin prejuicio del deber de informar a los mismos según el art. 5 de la LOPD.

Por tanto, sí, **sería conforme a la LOPD la inclusión de tales datos en las tarjetas identificativas**, no considerándose un tratamiento de datos excesivo por la finalidad de cumple de identificación del personal.

Tampoco será necesario el consentimiento por parte del trabajador para tratar dichos datos en base a la relación laboral que les une.

No obstante, **sí deberán ser informados** en los términos del art. 5 de la LOPD.

A TENER EN CUENTA

Cualquier exposición de datos personales constituye una cesión que debe ser consentida por el titular o estar amparada en alguna de las excepciones previstas por la LOPD.

ACTUALIDAD LOPD

El director de la AEPD destaca que la protección de datos contribuye a generar confianza en las nuevas tecnologías

Fuente: www.agpd.es

Nota de prensa

Durante la inauguración de la Jornada '20 años de protección de datos en España'

El director de la AEPD destaca que la protección de datos contribuye a generar confianza en las nuevas tecnologías

- **El director de la AEPD ha señalado que la legislación española de protección de datos representa "un referente internacional que está siendo tomado como modelo en varios países latinoamericanos"**
- **El ministro de Justicia, Alberto Ruiz-Gallardón, ha subrayado que este derecho fundamental es "una materia de especial trascendencia" porque contribuye a la dignidad de la persona**
- **El secretario de Estado de Telecomunicaciones y Sociedad de la Información, Víctor Calvo-Sotelo, ha recordado que los ciudadanos tienen derecho a saber qué pasa con sus datos**
- **La celebración de esta jornada coincide con el Día Europeo de Protección de Datos**

Puede acceder desde este enlace:

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2013/notas_prensa/common/130128_NP_20_aniversario.pdf

EL PROFESIONAL RESPONDE

“Tengo una clínica y manejamos informes médicos en Word. ¿Cómo puedo registrar los accesos a los informes?”

Los informes médicos incluyen datos personales de nivel alto. Para cumplir la LOPD se ha de **implementar un registro de accesos** con las siguientes características:

a) De **cada intento de acceso** se guardarán, como mínimo la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

b) En caso de ser autorizado, se deberá guardar información que permita identificar el **registro accedido**.

c) Los **mecanismos** que permiten el registro de accesos estarán bajo el control directo del **responsable de seguridad** competente sin que deban permitir la desactivación ni la manipulación de los mismos.

d) El período mínimo de **conservación** de los datos registrados será de **dos años**.

e) El responsable de seguridad se encargará de **revisar al menos una vez al mes la información de control registrada** y **elaborará un informe** de las revisiones realizadas y los problemas detectados.

¿Y cómo se puede hacer todo esto?

La mejor opción para poder realizar esto es implantar un **software de gestión documental** que valide el acceso de cada usuario a los informes y registre cada uno de los accesos, tal y como nos exige la normativa.

A TENER EN CUENTA

Las medidas de seguridad han de implantarse de forma efectiva. No vale solo con tenerlas descritas en el Documento de Seguridad.