LOPD EN LA EMPRESA

comSeveral
TIEMPO COSTE CALIDAD

LA LOPD EN EL DÍA A DÍA

El deber de secreto y los trabajadores

La LOPD dice en su artículo 10:

El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al 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.

Es decir, todas las personas que intervienen en el tratamiento de los datos de carácter personal (en la recogida, en el almacenamiento, en la utilización, etc.) están obligadas por ley al secreto profesional respecto de los mismos.

También están obligadas a guardarlos y custodiarlos adecuadamente, de forma que no tenga acceso a dichos datos alguien no autorizado.

Para dar a conocer esto a todos los trabajadores involucrados, además de formarlos y concienciarlos, es conveniente darles a firmar un compromiso de confidencialidad y deber de secreto, a través del cual se comprometen a no revelar ningún dato incluso después de finalizada la relación laboral, de forma que podamos acreditar que le hemos informado adecuadamente.

Contenido

Debemos formar a los trabajadores que tratan los datos personales.

IMPORTANTE

Aunque un trabajador vulnere el deber de secreto y revele datos a terceras personas, **la sancionada por la AEPD será la entidad** responsable del fichero, no el trabajador en cuestión.

Por eso es tan importante para la entidad el formar adecuadamente a los trabajadores que tratan los datos.

SANCIONES DE LA AEPD

Fax enviado al trabajo con datos personales

El procedimiento sancionador de la AEPD PS/00575/2009, iniciado a instancias de una denuncia presentada por un particular a la entidad GENERAL ELECTRIC MONEY BANK SA pone de manifiesto la **necesidad que tienen las organizaciones de adecuar sus procedimientos de contacto con los clientes** de forma que se cumpla en todo momento la normativa y se protejan los datos de dichos individuos.

En este caso, el hecho es que la denunciante suscribió un crédito con la mencionada entidad.

Al resultarse impagadas algunas de las cuotas de dicho crédito, **la entidad envió un fax al trabajo del denunciante** exponiendo el hecho de que existían cuotas impagadas e instando a su regularización (fax que evidentemente estuvo a disposición del resto del personal que trabajaba en las instalaciones).

La entidad no ha podido acreditar que existía consentimiento de la denunciante para enviar dicha información al fax de su trabajo.

El resultado: una sanción de 3.000€ por infringir el artículo 10 de la LOPD (grave), relativo al secreto profesional y al deber de guardar dichos datos al haber posibilitado y facilitado que otras personas tuviesen acceso a datos personales de aquélla sin su consentimiento.

Hemos de tener en cuenta que se ha aplicado el artículo 45.4, rebajando la cuantía de la sanción de entre 60.101,21 y 300.506,05 euros a 2.000€.

"Siempre que se efectúe, o pueda efectuar una comunicación de datos, debe obtenerse el consentimiento del titular de dichos datos y guardar acreditación de que se ha obtenido."

CONCLUSIÓN

En este procedimiento hemos visto la necesidad que tiene en toda entidad el **adecuar los procedimientos de contacto con sus clientes** de forma se no se vulnere la LOPD.

También hemos visto la importancia de **poder acreditar que hemos obtenido el consentimiento** del titular para el tratamiento de los datos, en especial cuando dicho tratamiento sea "delicado" (posible cesión de datos, uso distinto que prestar un servicio directo al titular, etc.).

LA AEPD ACLARA

Delegados de Prevención

El informe 0355/2010 de la AEPD da respuesta a la consulta planteada: si los delegados de prevención pueden acceder a los datos de salud de los empleados públicos contenidos en los partes de accidentes de trabajo y en la relación de accidentes de trabajo sin baja médica, de acuerdo con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), y a su Reglamento de desarrollo.

A tenor de dicho informe jurídico se deben tener en cuenta lo siguiente:

- Tanto la relación de accidentes de trabajo como la información sobre los daños en la salud que aparezcan en los partes de accidentes de trabajo de los trabajadores que determinen una ausencia al trabajo superior a un día, podrá facilitarse a los delegados de prevención **de forma disociada**. Es decir, sin hacer referencia a qué trabajador corresponden dichos datos.

- Que los datos suministrados sean **adecuados, pertinentes y no excesivos** para esa finalidad.

- Que no se utilicen para **ninguna otra finalidad**.

- Los delegados de prevención deberán **guardar secreto** respecto de la información así obtenida (artículo 10 de la LOPD).

A TENER EN CUENTA

Siempre que se traten datos especialmente protegidos, las medidas de seguridad han de extremarse.

Siempre que sea posible, han de disociarse dichos datos, de forma que no exista referencia directa al titular de los mismos.

ACTUALIDAD LOPD

Deficiencias en el cumplimiento de la LOPD en hospitales

Fuente: www.agpd.es

Informe de cumplimiento de la LOPD en Hospitales
Alcance y metodolgía

Datos por titularidad del centro

Desglose de los centros que han sido requeridos para realizar el informe de cumplimiento en función de la titularidad, así como el número de centros, por titularidad, que han atendido dicho requerimiento y el resultado numérico de centros que presentan deficiencias en el cumplimiento de la LOPD.

	Requeridos	No contestan	Contestan	Envío de recomendaciones	Requerimiento medidas correctoras
Privados	313	20	294	251	43
Públicos	292	23	268	109	159
Total	**605**	**43**	**562**	**360**	**202**

Informe de cumplimiento de la LOPD en Hospitales
Implantación de medidas de seguridad

Preguntas	C. Públicos	C. Privados
Documento de seguridad	El 83% dispone de él	El 98% dispone de él
Mecanismos que dificulten la apertura de los dispositivos de almacenamiento	El 35% carece de ellos	El 89,4% dispone de ellos
Medidas para evitar la sustracción, pérdida o acceso indebido	El 30% carece de ellas	El 15% carece de ellas
Conservación de un registro con todos los accesos a la información	El 37,4 no lo conserva	El 85,6% lo guarda
Conservación del registro de accesos por un periodo mínimo de dos años	El 42% no lo conserva	El 21% no lo conserva
Auditan que el personal autorizado utiliza los datos para la finalidad que justificó el acceso	El 75% no lo hace	El 35% no lo hace
Auditoría bienal de seguridad	El 66% no lo hace	Lo realiza el 88%
Se ha informado al personal de limpieza sobre la necesidad de garantizar la confidencialidad	El 74% lo ha hecho	El 94% lo hace

EL PROFESIONAL RESPONDE

¿Qué plazo tengo para ejercer los derechos ARCO?

Muchas empresas no tienen claro los plazos de tiempo que tienen para ejercer los derechos de acceso, rectificación, cancelación y oposición de los ciudadanos.

R: El plazo depende del derecho que se quiere ejercer.

Para el **derecho de acceso, la empresa dispone de 30 días** para estimar la solicitud y luego 10 días para efectuar la contestación efectiva.

Se debe contestar un derecho de acceso incluso si no se posee ningún dato del interesado.

Los derechos de **rectificación y cancelación** deben hacerse efectivos y contestarse en un plazo máximo de **10 días** desde su recepción.

Si se ha producido una **cesión de datos, debe extenderse la petición** efectuada a todas las entidades cesionarias de dichos datos para que también se haga efectivo en las mismas.

El derecho de **oposición** debe hacerse efectivo y contestarse también en un máximo de **10 días**.

Para poder ejercer cualquier derecho, el titular debe aportar:

- **Fotocopia del DNI** ó documento equivalente.
- **Petición** en que se concreta la solicitud.
- **Dirección** a efectos de notifica-ciones, fecha y firma.
- **Documentos acreditativos** de la petición que formula, en su caso.

"Hay que contestar todas las solicitudes recibidas en tiempo y forma."