Boletín 05/21

LOPD EN LA EMPRESA

EL RGPD UE 2016/679 EN APLICACIÓN

La figura del Delegado de Protección de Datos

En estos tiempos en los que la utilización masiva de datos, y en especial, los datos personales, han cobrado un valor importante, se hace cada vez más necesario que las empresas y entidades tengan entre sus asesores a un Delegado de Protección de Datos.

Esta figura, conocida también como DPD/DPO, en algunos casos, será designada obligatoriamente tanto por el responsable como encargado de tratamiento. **¿Cuáles son estos supuestos?**

- Las autoridades y organismos públicos.
- Empresas que tratan datos personales con fines de observación sistemática y habitual a gran escala.
- Empresas que tratan datos de categorías especiales y datos relativos a condenas e infracciones penales a gran escala.

Además, nuestra Ley Orgánica en su art. 34 LOPDPGDD recoge una lista de sujetos obligados. Estos serían algunos de ellos: (ver lista completa en el artículo)

- Responsables de ficheros de blanqueo de capitales.
- Los centros docentes, Universidades públicas y privadas.
- Comercializadoras de servicios de energía.

Contenido

1. La figura del Delegado de Protección de Datos.
2. Sancionada una asesoría por la falta de medidas de seguridad técnicas y organizativas adecuadas.
3. Informe de la AEPD sobre el Derecho al Olvido en buscadores de Internet.
4. La AEPD publica una guía sobre protección de datos y relaciones laborales.
5. Fraude al Departamento de Recursos Humanos.

IMPORTANTE

La falta de designación de DPO/DPD es objeto de cuantiosas sanciones económicas por la AEPD.

SANCIONES DE LA AEPD

Sancionada una asesoría por la ausencia de medidas de seguridad técnicas y organizativas adecuadas

En la Resolución de la AEPD https://www.aepd.es/es/documento/ps-00483-2020.pdf, se sanciona a una asesoría por no haber implementado las medidas de seguridad adecuadas, para evitar incumplir el deber de confidencialidad.

La reclamante notifica a la AEPD, que la asesoría le remitió un correo electrónico con un documento que recoge los datos personales de otro cliente. Se le solicita al reclamado que en el plazo de un mes enviara a la AEPD la siguiente información:

- Copia de las comunicaciones de la decisión adoptada y acreditación de que ha recibido la comunicación.
- Informe sobre las causas que han motivado la incidencia.
- Informe sobre las medidas adoptadas para evitar que se produzcan incidencias similares.

No se recibió ninguna alegación, por lo que se acuerda iniciar el procedimiento sancionador a la asesoría por incumplir los siguientes artículos del RGPD:

a) **Art.5.1.f RGPD: el acceso a los datos de un tercero por inefectividad de las medidas de seguridad. Supone una falta de confidencialidad. Sanción 2.000 euros.**

b) **Art. 32.1RGPD: el reclamante no aplica diligentemente medidas de seguridad técnicas ni organizativas que garanticen una confidencialidad de los datos. Sanción 1.000 euros.**

El responsable debe garantizar una seguridad adecuada de los datos personales que eviten un acceso ilícito o no autorizado.

IMPORTANTE

Las brechas de seguridad originadas por la falta de medidas técnicas y organizativas adecuadas suponen una infracción grave.

LA AEPD ACLARA

Informe de la AEPD sobre el Derecho al Olvido en buscadores de Internet

La AEPD en el apartado de la web “informes y resoluciones” ha publicado recientemente un informe, **en el que da respuesta a la consulta planteada sobre la utilización de un dato personal diferente al nombre para ejercer el derecho al olvido en los buscadores de Internet.**

Para dar contestación a esta consulta, la AEPD aporta en su informe una interpretación conjunta de la normativa que regula el derecho al olvido, tanto el RGPD como la LOPDPGD, las Directrices dictadas por el CEPD, y la jurisprudencia del Tribunal Supremo y de Justicia emitida en estos casos.

Las conclusiones a la que llega la AEPD es que, por regla general, el Derecho al Olvido frente a buscadores abarcaría únicamente la búsqueda realizada a partir del nombre entendiendo este término como nombre y apellidos y con carácter excepcional se podrían admitir otros términos distintos al nombre, siempre y cuando éstos produzcan los mismos efectos de identificación y singularización de la persona que ejerce el derecho al olvido en los buscadores de Internet. Es decir, que ese dato, permita identificar inequívocamente a una persona frente a la generalidad.

La AEPD en su informe recoge resoluciones favorables al derecho al olvido a partir de una información distinta al nombre y apellidos. Es el caso, por ejemplo, de búsquedas realizadas a partir del diminutivo del nombre compuesto del afectado.

IMPORTANTE

La admisión de variantes distintas al nombre es excepcional, lo relevante es como se conoce a la persona a nivel general.

ACTUALIDAD LOPD

La AEPD publica una guía sobre protección de datos y relaciones laborales

Fuente: AEPD

((Madrid, 18 de mayo de 2021). La Agencia Española de Protección de Datos (AEPD) ha publicado hoy la guía 'Protección de datos y relaciones laborales' con el objetivo de ofrecer una **herramienta práctica de ayuda** a las organizaciones públicas y privadas para un adecuado cumplimiento de la legislación. Esta guía ha sido elaborada por la Agencia con la participación tanto del Ministerio del Trabajo y Economía Social como de la patronal y organizaciones sindicales.

La aplicación del Reglamento General de Protección y la Ley Orgánica de Protección de Datos y garantía de los derechos digitales (LOPDGDD) ha supuesto una serie de cambios tanto en lo relativo a los derechos de las personas trabajadoras como en la recogida y el uso de sus datos por parte de los empresarios. Asimismo, la guía también aborda temas que se plantean cada vez con mayor frecuencia, como la consulta por parte del empleador de las redes sociales de la persona trabajadora, los sistemas internos de denuncias (*whistleblowing*), el registro de la jornada laboral, la protección de los datos de las víctimas de acoso en el trabajo o de las mujeres supervivientes a la violencia de género o el uso de la tecnología wearable como elemento de control.

El documento comienza recogiendo las **bases que legitiman el tratamiento** de datos personales, la información que es necesario facilitar y los derechos de protección de datos aplicados al entorno laboral. Aborda también el **principio de minimización**, ya que la ejecución del contrato de trabajo no implica que el empleador pueda conocer cualquier tipo de dato personal de las personas trabajadoras. Además de los **deberes de secreto y seguridad** (que los datos personales sólo sean conocidos por el afectado y por aquellos usuarios de la organización con competencias para usar, consultar o modificar esos datos), el documento también recoge los límites al tratamiento de datos en los procesos de selección y contratación de personal.

En el apartado de **selección de personal y redes sociales**, la Agencia detalla que las personas no están obligadas a permitir que el empleador indague en sus perfiles de redes sociales, ni durante el proceso de selección ni durante la ejecución del contrato. Aunque el perfil en las redes sociales de una persona candidata a un empleo sea de acceso público, el empleador no puede efectuar un tratamiento de los datos obtenidos por esa vía si no cuenta para ello con una base jurídica válida y para ello será necesario informar de ello a la persona trabajadora y demostrar que dicho tratamiento es necesario y pertinente para desempeñar el trabajo. Por otro lado, la Agencia aclara que la empresa no está legitimada para solicitar 'amistad' a las personas candidatas para que éstas proporcionen acceso a los contenidos de sus perfiles.

Puede ver más información en el siguiente enlace

La protección de datos en las relaciones laborales

EL PROFESIONAL RESPONDE

Fraude al Departamento de Recursos Humanos

Todas las empresas con independencia de su tamaño pueden tener el riesgo de ser víctimas de un ciberataque.

En este caso, vamos a analizar el supuesto de fraude al departamento de RRHH. Es importante conocer cómo operan los ciberdelincuentes para poder prevenir este tipo de ataques, y en su caso, cuando" ya sea tarde" actuar con la mayor diligencia posible.

Las técnicas utilizadas son similares al fraude del CEO, aunque en esta ocasión la identidad suplantada no es la del CEO, sino la de un empleado de la empresa.

En la comunicación, el ciberdelincuente se hace pasar por un empleado de la empresa y le pide al departamento de RRHH que le ingrese la nómina en un nuevo número de cuenta. Para ello se ha tenido que realizar un estudio previo de la empresa víctima, identificando al personal de la empresa y sus cuentas de correo electrónico.

¿Qué podemos hacer para identificar el ataque y prevenirlo? En este caso, cuando la solicitud que recibe el departamento de RRHH esté relacionada con el cambio del número de cuenta bancaria de un empleado, se debe verificar esta solicitud mediante otro medio de comunicación, por ejemplo, a través de una llamada telefónica o presencialmente.

Cuando se sufre de este tipo de ataques se debe denunciar ante las Fuerzas y Cuerpos de Seguridad del Estado y contactar con el banco lo antes posible.

IMPORTANTE

En este tipo de ataques se utiliza la técnica de email spoofing: envío de correos falsificados suplantando la identidad de la persona que realiza el envío de email.