Boletín 08/21

LOPD EN LA EMPRESA

Altabir consulting

AUTOR: JULIO CÉSAR MIGUEL PÉREZ

WWW.ALTABIR.ES

EL RGPD UE 2016/679 EN APLICACIÓN

La garantía de los derechos digitales (I)

El responsable del tratamiento de datos personales debe garantizar en todo momento los derechos y libertades en materia de protección de datos. **En nuestra ley orgánica (LOPDPGDD) se incluyó expresamente el título X "Garantía de los derechos digitales"**. En este título se pretende reconocer y garantizar un conjunto de derechos digitales de los ciudadanos conforme con los derechos reconocidos en la Constitución.

Como responsables de tratamiento de datos personales es importante conocer el listado de estos derechos digitales. La empresa debe incluir en sus procedimientos garantías suficientes que protejan los derechos de los interesados, empleados y usuarios de los cuales tratan sus datos personales.

Los derechos digitales que como empresa debemos garantizar son entre otros:

- Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.
- Derecho a la desconexión digital en el ámbito laboral.
- Derecho a la intimidad frente al uso de dispositivos de videovigilancia y grabación de sonidos en el lugar de trabajo.
- Derecho a la intimidad ante la utilización de sistemas de geolocalización.

Contenido

IMPORTANTE

Recientemente se ha aprobado la Carta de los derechos digitales (sin valor normativo).

SANCIONES DE LA AEPD

Una empresa hotelera sancionada con 7.000 euros por actuar sin contrato de encargado de tratamiento

Tratar los datos personales sin un contrato de encargado de tratamiento supone graves sanciones.

En la Resolución de la AEPD https://www.aepd.es/es/documento/ps-00151-2021.pdf, se sanciona a una empresa hotelera por haber realizado el tratamiento de datos personales de sus clientes sin conformar un contrato de acceso a datos.

La reclamada manifiesta ante la AEPD que sus datos aportados (DNI) al hacer la reserva se han utilizado para otros fines sin su consentimiento.

La AEPD en su proceso de investigación constata que la empresa hotelera sancionada no ha actuado diligentemente. En el caso concreto, cuando llegan huéspedes al alojamiento a una determinada franja horaria, éstos no son atendidos por el personal propio de la empresa hotelera, sino por el conserje de la comunidad de vecinos donde se encuentra el alojamiento alquilado. **No existe un contrato de acceso a datos con la comunidad para que puedan tratar los datos de los clientes. La sanción en este caso ascendió a 5.000 euros.**

Se investiga también la web de la reclamada constatando el incumplimiento de su política de cookies, ya que no se informa de ellas, ni tampoco se facilita un sistema granular para poder configurar las cookies. **La sanción por el incumplimiento de cookies ascendió a 2.000 euros.** Se impuso, además, una medida correctiva para que incluya un mecanismo que permita configurar las cookies correctamente.

IMPORTANTE
Deben incorporarse en la web mecanismos que imposibiliten la utilización de cookies no necesarias antes de dar el consentimiento y mecanismos que permitan su rechazo.

LA AEPD ACLARA

Informe desfavorable al proyecto de una entidad bancaria para la utilización del reconocimiento facial de sus clientes

La AEPD ha emitido recientemente un informe desfavorable al proyecto presentado por una entidad bancaria que pretendía la utilización de sistemas de reconocimiento facial en el momento del alta de clientes en la oficina o en el canal online. **La finalidad era la de llevar a cabo las verificaciones oportunas previstas en la Ley 10/02010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (Ley PBC/FT).**

La entidad bancaría alegaba en su proyecto como legitimación el consentimiento de los interesados. La AEPD, según se desprende del informe, no considera válida esta base jurídica. El consentimiento solicitado no cumpliría con los requisitos necesarios para su obtención, ya que no se puede garantizar que se haga de forma libre y voluntaria por el cliente. Se estaría condicionando la prestación de servicios al consentimiento.

Se alegaba también, por parte de la entidad bancaria, como alternativa al consentimiento, la utilización de un interés público esencial como base jurídica. La AEPD manifiesta en su informe que no es posible aplicar esta excepción. **Para poder utilizarlo tendría que existir una norma con rango de ley que especifique el interés público esencial y que respete en todo caso el principio de proporcionalidad.** La citada Ley de PBC/FT no ha previsto como el uso de datos biométricos como medida proporcional para la identificación de las personas físicas.

IMPORTANTE

Los datos biométricos son datos de categorías especiales de datos y por lo tanto requieren de mayores garantías de protección.

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 del empresariado. Asimismo, la guía también aborda temas que se plantean cada vez con mayor frecuencia, como la consulta por parte de la persona empleadora 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 la persona empleadora 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 la persona afectada 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 la persona empleadora 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

La formación y prevención: las mejores herramientas para evitar ciberataques (III)

En este apartado hemos desarrollado los principales tipos de ciberataques que puede sufrir una empresa.

Ahora llega el momento de protegerse y evitar ser víctimas de los ciberdelincuentes.

La concienciación y formación de todos los usuarios de dispositivos digitales es clave para conseguir que los ciberdelincuentes no consigan su propósito de robar la información de la empresa. El conocimiento de las situaciones a las que nos podemos enfrentar y cómo reaccionar a tiempo es una medida organizativa de prevención esencial que ninguna empresa debería de pasar por alto. Muchos de los ataques de *ransomware* se producen utilizando la ingeniería social. **La única forma de prevenirlo es conocer como funcionan y que hacer si sospechamos de conductas engañosas.**

Las medidas técnicas de prevención evitan la vulnerabilidad de nuestros sistemas. Debemos actuar con un diseño de red que segmente redes y evitar así la exposición de servicios internos al exterior. Otras medidas técnicas serían la actualización del software de los dispositivos, restringir el uso de aplicaciones o equipos no permitidos, realizar copias de seguridad con carácter periódico, desactivar los complementos o extensiones no utilizadas de los navegadores.

Una vigilancia periódica es decisiva para comprobar la eficacia de las medidas.

IMPORTANTE

La rápida actuación ante un ataque es fundamental para mitigar sus efectos. Cualquier incidencia sospechosa se debe poner en conocimiento del responsable TIC de la empresa.