Boletín 11/21

LOPD EN LA EMPRESA

EL RGPD UE 2016/679 EN APLICACIÓN

Derechos digitales en el ámbito laboral. Videovigilancia

Los dispositivos de videovigilancia y grabación de sonidos podrán ser utilizados por los empleadores para ejercer las funciones de control del personal laboral. Este control laboral se legitima en el art. 20.3 del Estatuto de los trabajadores.

Las empresas tendrán que tener en cuenta los siguientes criterios para no causar perjuicios en los derechos de protección de datos personales de los empleados/as.

- Informar con carácter previo, de forma expresa, clara y concisa de la finalidad de la medida.
- No se instalarán los sistemas de grabación de sonidos y videovigilancia en los lugares de descanso, tales como vestuarios, aseos, comedores y análogos.
- La grabación de sonidos se admitirá solo cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad desarrollada en el centro de trabajo y siempre respetando el principio de proporcionalidad e intervención mínima.

La conservación de la imágenes y sonidos será como máximo un mes, salvo que sirvan para acreditar algún acto ilícito. En este caso se pondrán a disposición de la autoridad competente en el plazo máximo de 72 horas.

Contenido

1. Derechos digitales en el ámbito laboral. Videovigilancia.
2. Sanción de 2.000 € por incumplir con el deber de informar en una oferta de un puesto de trabajo.
3. EL delegado de protección de datos, papel fundamental en el nuevo modelo de responsabilidad activa.
4. Anonimización y seudonimización (II): la privacidad diferencial.
5. Navegar seguro y actualizar: dos medidas preventivas para prevenir los ataques de *ransomware*.

IMPORTANTE

Si se captase la comisión de un acto ilícito el deber de informar se entenderá cumplido con la existencia del cartel informativo.

SANCIONES DE LA AEPD

Sanción de 2.000 € por incumplir con el deber de informar en una oferta de un puesto de trabajo.

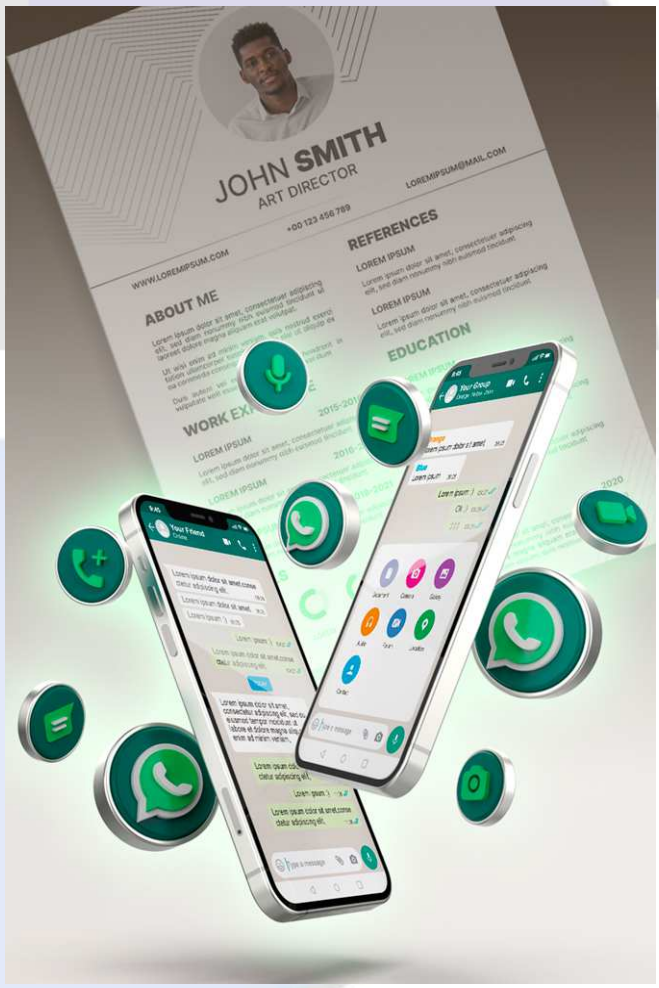
En la Resolución de la AEPD https://www.aepd.es/es/documento/ps-00237-2021.pdf, se sanciona a una empresa por no facilitar la información sobre protección de datos en la oferta de un puesto de trabajo.

El afectado envió un escrito de reclamación a la AEPD a través de su sede electrónica de reclamaciones ordinarias. En este escrito, manifestaba que contactó con la empresa a través del teléfono que constaba en el anuncio y envió su currículum vitae por la aplicación de mensajería de WhatsApp.

Junto a la reclamación aporta la captura de pantalla de móvil con la conversación a través de WhatsApp. En este sentido, la AEPD recomienda, que para que la reclamación se resuelva de forma exitosa y reducir los plazos de tiempo, se aporten todos aquellos documentos que sirvan para probar los hechos reclamados.

En ningún momento el afectado fue informado sobre el tratamiento de sus datos personales incumpliendo el art.13 del RGPD. En este artículo, se indican todos los aspectos relativos al tratamiento de datos personales que han de conocer los interesados en el momento de la recogida de sus datos. El responsable del tratamiento debe facilitar esa información de una forma clara y sencilla para que el interesado conozca la identidad del responsable, los datos del DPD en su caso, los fines del tratamiento y la base jurídica entre otros aspectos.

La LOPDGDD indica que puede cumplirse el deber de información facilitando al interesado la información básica e indicando donde solicitar más información.



IMPORTANTE

Cuando el responsable trate por primera vez los datos personales del interesado tiene que poner a su disposición toda la información en materia de protección de datos.

LA AEPD ACLARA

EL delegado de protección de datos, papel fundamental en el nuevo modelo de responsabilidad activa.

En el informe 0018/2021 publicado por la AEPD analiza la importancia del delegado de protección de datos en el nuevo modelo de responsabilidad activa.

La mayor novedad que presentaba el Reglamento (UE) 2016/679 era la evolución del modelo basado en el control de cumplimiento a otro que determina el principio de responsabilidad activa. Este principio exige al responsable y encargado del tratamiento una previa valoración del riesgo que se puede generar en el tratamiento de los datos de carácter personal y adoptar de este modo las medidas que procedan.

Además, es el responsable del tratamiento a quién le corresponde determinar la base jurídica que puede amparar un tratamiento. **Es en este nuevo modelo de responsabilidad activa, donde la figura del delegado de protección de datos resulta determinante como apoyo para el responsable y encargado del tratamiento.**

Para ello, se indica en el informe que, tanto el responsable como el encargado, tienen que garantizar que el DPD participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales. **Se enumeran también cuáles son las funciones del delegado de protección de datos contenidas en el art. 39 del RGPD. Entre otras, tendrá que informar y asesorar al responsable, encargado y a sus empleados de las obligaciones que les incumbe en materia de protección de datos.**

IMPORTANTE
La designación de delegado de protección de datos en algunos casos tiene carácter obligatorio, el incumplimiento de su nombramiento supone una sanción grave.

ACTUALIDAD LOPD

Anonimización y seudonimización (II): la privacidad diferencial

Fuente: AEPD

El valor estratégico de los datos personales para empresas y organizaciones es evidente. Sin embargo, es igualmente innegable el riesgo que el tratamiento masivo de datos personales supone para los derechos y libertades de los individuos y para nuestro modelo de sociedad. Por ello, es preciso adoptar las garantías necesarias para que los tratamientos realizados por los distintos responsables no supongan una injerencia en la privacidad de las personas. En la búsqueda de un equilibrio entre la explotación legítima de la información y el respeto a los derechos individuales, surgen estrategias encaminadas a preservar la utilidad de los datos al tiempo que se respeta su privacidad. Una de estas estrategias es la **privacidad diferencial**.

La oficina del Censo de los Estados Unidos, para garantizar la precisión de sus estadísticas, impedir que la información personal se revele incluso a través de las mismas, y así aumentar la confianza de los ciudadanos en la seguridad de los datos que proporcionan, aplica privacidad diferencial.

La privacidad diferencial puede encuadrarse dentro de una de las técnicas de mejora de la privacidad, o PET (Privacy Enhancing Technologies), dirigidas a establecer garantías de protección de datos desde el diseño mediante la implementación práctica de estrategias de abstracción de la información. Tal y como lo describe su creadora, Cynthia Dwork, la privacidad diferencial permite garantizar, mediante la incorporación de ruido aleatorio a la información original, que en el resultado del proceso de análisis de los datos a los que se ha aplicado esta técnica no hay pérdida en la utilidad de los resultados obtenidos. Tiene su fundamento en la Ley de los Grandes Números, un principio estadístico que establece que cuando el tamaño de la muestra crece, los valores promedios que se derivan de la misma se aproximan al valor medio real de la información. De esa forma, la adición a todos los datos de un ruido aleatorio permite compensar estos efectos y producir un valor "esencialmente equivalente".

El concepto "esencialmente equivalente" no significa que el resultado obtenido sea idéntico, sino que se refiere a que el resultado concreto a partir del análisis que se deriva del conjunto original de datos, y el resultado del conjunto al que se ha aplicado privacidad diferencial son, funcionalmente, equivalentes. Esta circunstancia permite incorporar la "negación plausible" de que los datos de un sujeto concreto estén en el conjunto de datos objeto de análisis. Para ello, el patrón de ruido incorporado a los datos ha de estar adaptado al tratamiento y los márgenes de exactitud que es necesario obtener.

Puede ver más información en el siguiente enlace

Innovación y tecnología

EL PROFESIONAL RESPONDE

Navegar seguro y actualizar: dos medidas preventivas para prevenir los ataques de *ransomvare*

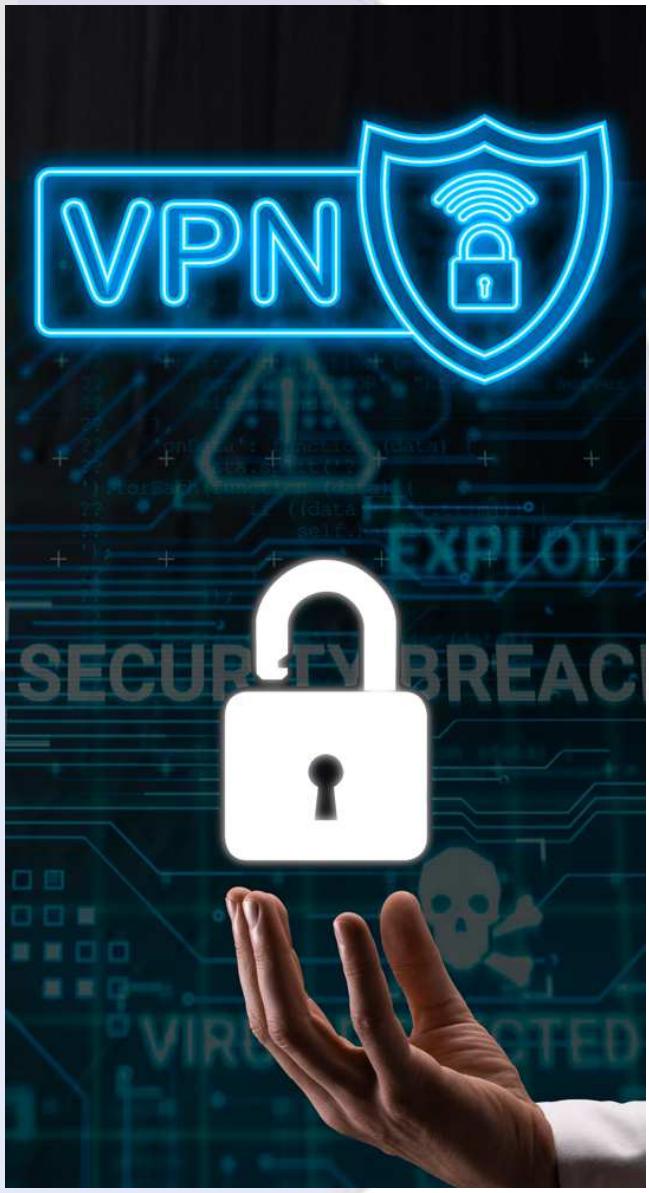
Seguimos hablando de medidas de protección y de prevención frente a los ataques de los ciberdelincuentes.

Una navegación segura te permitirá proteger de forma óptima toda la información de tu empresa. La digitalización del entorno empresarial y laboral ha supuesto la necesidad de acceder en remoto a los documentos de la intranet o equipo corporativo. Se recomienda para ello, la utilización de redes privadas virtuales (*Virtual Private Network VPN*) cuando sea posible. En estas redes, el tráfico viaja cifrado y, por eso, los ciberatacantes no son capaces de visualizar el contenido.

Se debe evitar acceder a sitios web de contenido dudoso. Hay páginas que aparentan ser legítimas y, en cambio, pueden esconder *exploit kits* que detectan vulnerabilidades del navegador web para instalar *ransomware* en el dispositivo.

La actualización de los navegadores web, del sistema operativo y del software resultan imprescindibles para hacer frente a los ciberdelincuentes. Cuanto más actualizados estén los sistemas que se utilizan en la empresa, conseguiremos mitigar las vulnerabilidades haciendo más difícil que puedan infectarte.

Los sistemas operativos, aplicaciones y dispositivos deberían tener habilitada la instalación de actualizaciones de forma automática.



IMPORTANTE

Para la selección de una *VPN* la empresa tiene que revisar sus necesidades, decidir para que servicios se permitirá y los requisitos de seguridad.

AUTOR: JULIO CÉSAR MIGUEL PÉREZ