Boletín 10/21

LOPD EN LA EMPRESA

EL RGPD UE 2016/679 EN APLICACIÓN

Derechos digitales en el ámbito laboral. Desconexión digital

En este apartado iremos desarrollando los derechos digitales del entorno laboral que debemos tener en cuenta como empresa.

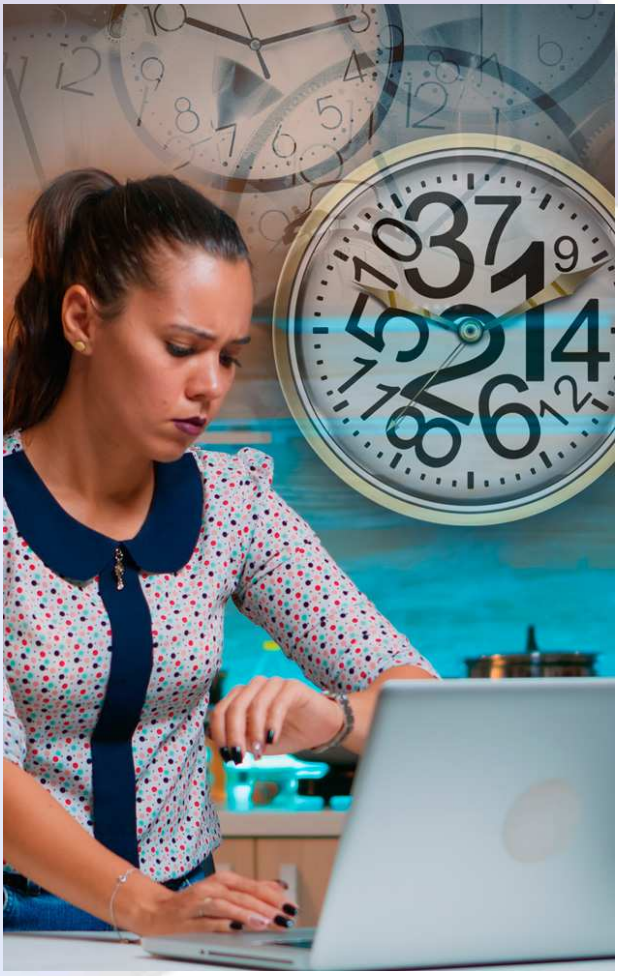
El derecho a la desconexión digital (art.88 LOPDPGDD) se ha convertido en uno de los derechos fundamentales a proteger como consecuencia del cambio en la forma de trabajar. La digitalización del entorno empresarial y el teletrabajo son dos de las razones por las cuáles estamos sujetos a una conexión total con los dispositivos digitales.

Los empleadores tienen que proporcionar el derecho a la desconexión digital para garantizar al personal laboral, fuera del horario laboral legal o convencionalmente establecido, el respeto de:

- El tiempo de descanso.
- Los permisos y vacaciones.
- Su intimidad personal y familiar.

Habrá que desarrollar políticas internas, en su caso, previa audiencia de los representantes de los trabajadores. En ellas se definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y sensibilización del personal sobre un uso razonable de las herramientas tecnológicas, evitando el riesgo conocido como fatiga informática.

Contenido



IMPORTANTE

El derecho a la desconexión digital se regula también en la Ley 10/2021, de 09 de julio, de trabajo a distancia.

SANCIONES DE LA AEPD

Sancionada con 10.000 euros una empresa de transporte por incumplimiento del principio de exactitud de datos

En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00151-2021.pdf, se sanciona a una empresa de paquetería por haber realizado el tratamiento de datos personales de forma inexacta.

La AEPD recibe una reclamación por parte de un ciudadano que considera que se han tratado sus datos personales de forma ilícita por parte de la empresa de paquetería. El reclamante realizó una solicitud de servicio a la empresa reclamada para que recogieran un paquete, para ello, puso como punto de recogida la dirección de su trabajo, aunque el pago y el correo lo hizo desde su correo personal.

La actuación fraudulenta, por parte de la empresa de transporte, tiene lugar, porque desde el departamento de administración consideraron que el servicio se había hecho por parte de su cliente (empresa donde trabaja el reclamante), al ver la dirección de recogida, y no por el particular (reclamante). **Por ello, envían una factura con los datos personales del reclamante al departamento de contabilidad de la empresa cliente.**

Se considera que la empresa de transporte ha infringido el principio de exactitud de los datos del art.5 del RGPD. **No se adoptaron medidas razonables para que se suprimieran o modificaran los datos personales inexactos. La multa ascendió a 10.000 euros.**

Actuar en contra de los principios relativos al tratamiento se considera una infracción muy grave.

IMPORTANTE

Las empresas deben realizar políticas de protección de datos que apliquen los principios relativos al tratamiento del RGPD.

LA AEPD ACLARA

Fichas prácticas de videovigilancia. Cámaras en comunidades de propietarios

En el apartado de áreas de actuación de la página de la AEPD nos encontramos en el apartado de Videovigilancia una serie de fichas informativas.

En concreto vamos a desarrollar la ficha de cámaras en comunidades de propietarios. **Cuando la Comunidad de Propietarios decide instalar un sistema de videovigilancia habrá de tener en cuenta los siguientes aspectos**:

1º Legitimación para la instalación. Esta deberá basarse en el acuerdo de la Junta de Propietarios (voto favorable de las tres quintas partes del total de los propietarios), tal y como se dispone en la LPH. **Se recomienda que en el acuerdo se indique el número de cámaras y características del sistema.**

2º Previamente a su puesta en funcionamiento se tendrá que elaborar un registro de actividades de tratamiento.

3º Derecho de información. Se tienen que instalar en los distintos accesos a la zona videovigilada, y en lugar visible, uno o varios carteles que informen que se accede a una zona videovigilada.

4º Instalación. **Las cámaras solamente podrán captar imágenes de las zonas comunes.** Las cámaras con zoom tendrán que tener instaladas máscaras de privacidad.

5º El acceso a las imágenes estará restringido a las personas designadas por la comunidad.

6º **Las imágenes se conservarán durante un plazo máximo de un mes.**

IMPORTANTE

El cartel debe indicar quien es el responsable de la instalación, ante quién ejercer los derechos y donde obtener información adicional.

ACTUALIDAD LOPD

Anonimización y seudonimización

Fuente: AEPD

La información anónima es un conjunto de datos que no guarda relación con una persona física identificada o identificable (Considerando 26 del RGPD), en tanto que la información seudonimizada es un conjunto de datos que no puede atribuirse a un interesado sin utilizar información adicional, requiere que dicha información adicional figure por separado y, además, esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable (Artículo 4.5).

Transformar un conjunto de datos personales en información anónima o seudonimizada exige realizar un tratamiento sobre dichos datos personales. El tratamiento de anonimización genera un único y nuevo conjunto de datos, mientras que el tratamiento de seudonimización genera dos nuevos conjuntos de datos: la información seudonimizada y la información adicional que permite revertir la anonimización.

El conjunto de datos anonimizados no está bajo el ámbito de aplicación del Reglamento General de Protección de Datos (RGPD) (Considerando 26) aunque pudiera estar bajo el ámbito de aplicación de otras normas (p. ej. de seguridad nacional, salud pública, infraestructuras críticas, etc.) En este caso debe tenerse en cuenta que:

- El tratamiento que generan los datos anonimizados sí es un tratamiento de datos personales, que puede considerarse compatible con el fin original del tratamiento de datos personales del que proceden los datos (Dictamen 05/2014 sobre técnicas de anonimización WP246 apartado 2.2.1. Legitimación del proceso de anonimización).
- El conjunto de datos anonimizados queda fuera del ámbito de aplicación del RGPD en la medida que es posible demostrar objetivamente que no existe capacidad material para asociar los datos anonimizados a una persona física determinada, directa o indirectamente, ya sea mediante el uso de otros conjuntos de datos, informaciones o medidas técnicas y materiales que pudieran existir a disposición de terceros.

En cuanto a los **sistemas internos de denuncias o *whistleblowing***, la Agencia considera que la información tanto a las personas denunciantes como a las potenciales personas denunciadas reviste un carácter primordial. La LOPDGDD admite sistemas de denuncias anónimas y, en caso de que la denuncia no sea anónima, la confidencialidad de la información de la persona denunciante debe quedar a salvo y no debe facilitarse su identificación a la persona denunciada.

Puede ver más información en el siguiente enlace

Innovación y Tecnología

EL PROFESIONAL RESPONDE

Copias de seguridad. Medida técnica de recuperación ante un ataque de *ransomware*

Cuando seamos víctimas de un ataque de *ransomware* que ponga en peligro la información de la empresa y la continuidad de la actividad profesional tenemos que estar preparados y actuar con la mayor diligencia posible.

La principal medida de seguridad que puede ofrecernos mejores garantías para recuperar la actividad de la empresa lo más rápidamente posible es realizar copias de seguridad o *backups.*

Las recomendaciones para ejecutarlas correctamente son:

- **Realizar tres copias de seguridad actualizadas y en distintos soportes.** Esto nos permitirá poder recuperar los datos y continuar con la actividad. Las copias pueden estar en un disco duro específico para copias, USB externo y servicio *cloud*.

- **Guardar las copias de seguridad en un lugar diferente al del servidor de ficheros, puesto que se puede ver afectado.** Lo recomendable es almacenarlos en discos físicos (DVD o *Blu-Ray*) o en soportes externos no conectados a nuestra red.

- **Comprobar regularmente que las copias de seguridad funcionan correctamente y los pasos para su recuperación están claros.**

- Cifrar los datos sensibles para que en caso de robo los ciberdelincuentes no puedan publicar la información**. La clave de cifrado no se debe guardar en el mismo dispositivo.**

IMPORTANTE

Las copias de seguridad en la nube se sincronizan de forma continua. Para evitar que el *ransomware* cifre y bloquee las copias de seguridad se tendría que desactivar la sincronización persistente

AUTOR: JULIO CÉSAR MIGUEL PÉREZ