Boletín 01/17

LOPD EN LA EMPRESA

AUTOR: JULIO CÉSAR MIGUEL PÉREZ

inz Aragón

LA LOPD EN EL DÍA A DÍA

¿Cuál es el contenido de una solicitud de derechos ARCO?

Cualquier empresa o entidad que trate datos de carácter personal, deberá conceder al interesado un **medio sencillo y gratuito para el ejercicio de los derechos** de acceso, rectificación, cancelación y oposición (ARCO).
El ejercicio de estos derechos será gratuito para el interesado.

El escrito para solicitar un derecho deberá contener lo siguiente:

a) **Nombre y apellidos** del interesado.

b) **Fotocopia del DNI/NIF del interesado,** y en su caso, de la persona que lo representa así como el documento que acredita tal representación.

c) **Petición en que se concreta la solicitud.**

d) **Dirección a efectos de notificaciones**, fecha y firma del solicitante.

e) **Documentos acreditativos** de la petición que formula, en su caso.

No se considerará conforme el envío de **cartas certificadas**, la utilización de servicios de **telecomunicaciones de tarificación adicional**, y cualquier medio que implique un **coste excesivo** para el interesado.

Contenido

IMPORTANTE

En caso de infracción de la LOPD por una entidad, además de la sanción impuesta por la AEPD, el titular afectado puede exigir también una indemnización

SANCIONES DE LA AEPD

Sanción por control laboral sin comunicación previa a los trabajadores

Antes de realizar cualquier control laboral por el empresario y nunca después, es necesario informar debidamente al trabajador

En el PS/00275/2016 de la AEPD vemos la sanción impuesta a una U.T.E. madrileña a instancias de la UNION GENERAL DE TRABAJADORES **por controlar a sus trabajadores sin informarles previamente.**

En 2015, el sindicato UGT denuncia ante la AEPD a la citada U.T.E. por **proporcionar** a sus trabajadores para el desempeño de su trabajo, **unos dispositivos móviles (PDAs) con línea telefónica y GPS que controla su actividad,** sin haber informado previamente ni a empleados ni tampoco al Comité de empresa.

Este servicio de GPS tiene entre sus fines permitir **el fichaje del personal**, al inicio y al final de la jornada laboral, lo que **indica al empleador la posición exacta del dispositivo, y por tanto del trabajador** a través de las coordenadas (siempre que esté encendido).

En su defensa la UTE declaró que **Sí había entregado tanto a cada trabajador, como al Comité de empresa, documento informativo sobre el tratamiento de dichos datos de geolocalización** de los trabajadores. Sin embargo, **la inspección de la AEPD comprobó** que dicha información al Comité de empresa **se facilitó 2 años después de la recogida de los datos** al comienzo de la actividad que tuvo lugar en el año 2013.

Resultado: multa de 900 € a la U.T.E. MADRID SUR por infracción del art 5 de la LOPD, tipificada como leve en el art 44.2.c) de la misma por no informar en el momento debido.

IMPORTANTE

Los datos de geolocalización se consideran datos de carácter personal, pues permiten fácilmente la identificación del usuario del terminal

LA AEPD ACLARA

Conciliación LOPD y Ley de Transparencia

En el Informe 0178/2014 de la AEPD se plantea la cuestión sobre **cómo interaccionan la LOPD y la Ley de transparencia 19/2013**, y si es posible publicar a través de internet, los datos personales de los beneficiarios con discapacidad de ayudas o subvenciones.

A esta consulta, la AEPD resuelve:

- El objeto de la Ley 19/2013 es **aumentar la transparencia de la actividad pública de la Administración y garantizar el derecho de acceso a la información** sobre su actividad.
- El artículo 5.4 de la Ley 19/2013 señala **que la información que puede ser objeto de transparencia, será publicada en las sedes electrónicas o páginas web** de forma clara, estructurada y entendible.
- Sobre el otorgamiento de subvenciones públicas, es **la propia Ley quien ordena la publicación de cualquier información relativa a actos de gestión administrativa con repercusión económica o presupuestaria (subvenciones, etc.).**
- **Si la información contuviera datos especialmente protegidos** (discapacidad o salud), la publicidad podrá realizarse únicamente:
  - **previa disociación de los datos**
  - **si se cuenta con el consentimiento expreso** y previo del interesado
  - Si la cesión **se encuentra amparada por una norma con rango de Ley**

Fuera de estos tres casos, no sería posible la publicación en internet de datos de beneficiarios de ayudas o subvenciones públicas que tuvieran algún tipo de discapacidad.

IMPORTANTE

Los datos de carácter personal referentes a la salud, solo podrán ser recabados, tratados y cedidos, cuando así lo disponga una Ley o el interesado consienta expresamente

ACTUALIDAD LOPD

La AEPD elabora un decálogo con consejos prácticos de privacidad y seguridad en dispositivos conectados

Fuente: www.agpd.es

La AEPD elabora un decálogo con consejos prácticos de privacidad y seguridad en dispositivos conectados

La Agencia Española de Protección de Datos ha elaborado un listado de claves imprescindibles a tener en cuenta en los dispositivos con conexión a internet.

(Madrid, 15 de diciembre de 2016). Uno de los ejes principales de actuación de la Agencia Española de Protección de Datos (AEPD) es apostar de forma decidida por la prevención para que los ciudadanos sean más conscientes de los derechos que les asisten y cómo ejercerlos. La Agencia ha elaborado un listado de 10 claves imprescindibles en materia de privacidad y seguridad a tener en cuenta en los dispositivos conectados.

1. **Tu cuerpo dice más de lo que crees.** La tecnología 'vestible' (pulseras, relojes, podómetros, etc.) incorpora sensores que registran y pueden transferir información sobre hábitos y costumbres del usuario, tanto al fabricante como a terceros. Si los utilizas para monitorizar tu actividad física, es recomendable comprobar quién está recogiendo los datos que aportas, para qué los va a utilizar y si los va a ceder a otros. Si vas a subir estos datos a una red social intenta dar la menor información personal posible al registrarte y elimina o limita el acceso a tu ubicación siempre que puedas, ya que a partir de este dato se puede inferir mucha más información sobre ti de la que imaginas.

2. **Una ventana indiscreta.** Buena parte de los dispositivos incorporan cámaras que aportan funcionalidades añadidas. Desconéctala o tápala con una cinta adhesiva si no la estás utilizando para evitar que un extraño pueda verte si se hace con el control del dispositivo sin que te des cuenta. Por otro lado, en el caso de un dron, además de la normativa aeronáutica, ten en cuenta que si difundes por internet imágenes en las que se pueda identificar a las personas que aparecen en ellas, necesitarás tener su permiso o consentimiento.

3. **Dispositivos vulnerables.** Bloquea la pantalla de inicio y utiliza un código de desbloqueo lo más largo posible. Además, actualiza el software de tus dispositivos siempre que sea posible para evitar que sean vulnerables ante un posible hackeo y valora instalar algún programa que te proteja ante el software malicioso. Desactiva el bluetooth si no vas a utilizarlo y la conexión automática a wifis abiertas, ya que pueden ser una puerta de entrada para posible ataques.

4. **Protege tus datos ante pérdidas o robos.** Localiza en las opciones de configuración del terminal la forma en la que podrías acceder a distancia a su contenido para eliminarlo y piensa si te interesa utilizar una aplicación para realizar el borrado remoto. Valora si además quieres bloquear algunas aplicaciones que contengan información sensible y, en cualquier caso, realiza copias de seguridad con frecuencia.

Puede ver más información en el siguiente enlace:

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2016/notas_prensa/news/2016_12_15-ides-idphp.php

EL PROFESIONAL RESPONDE

¿Es posible grabar imágenes de alumnos durante el horario de clases?

Debido a la conflictividad alcanzada hoy día en algunos centros docentes, se llega al punto de plantearse por parte de éstos la posibilidad de **instalar videocámaras** no sólo en sus patios, pasillos y zonas de recreo, sino también **dentro de las propias aulas durante el desarrollo de las horas lectivas**.

La cuestión es si conforme a la LOPD, es posible **captar imágenes en un entorno escolar cuando la finalidad es controlar hurtos, acoso escolar o agresiones físicas o verbales a los profesores y compañeros en horario escolar.**

-La instalación de videocámaras en patios, zonas públicas o de acceso a un colegio está permitida y sujeta al ámbito de aplicación de la LOPD y la Instrucción 1/2006, **pues su legitimación se ampara en el art. 2 de la instrucción 1/2006** en relación con el 6.1 de la LOPD y la Ley 23/1992, de 30 de julio, de Seguridad Privada.

-Sin embargo, cuando se plantea si **es posible grabar dentro de las aulas,** la legitimación que existía para el supuesto anterior, no es válida, pues considera la AEPD que su finalidad no es mantener la seguridad del centro sino otra, y por tanto será **necesario el consentimiento de los profesores, alumnos, padres o representantes legales** (si fueran menores de 14 años), **para poder realizar dichas grabaciones**, pues en caso contrario, la grabación sería ilegítima.

IMPORTANTE

Para poder instalar cámaras de vigilancia dentro de las aulas con fines distintos de la seguridad, será imprescindible el consentimiento de los afectados o de sus padres.