Boletín 09/19

LOPD EN LA EMPRESA

Altabir consulting

AUTOR: JULIO CÉSAR MIGUEL PÉREZ

WWW.ALTABIR.ES

EL RGPD UE 2016/679 EN APLICACIÓN

¿Cuándo y cómo notificar las brechas de seguridad? (II)

Lo primero que tenemos que plantearnos es si todos los incidentes que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación no autorizada a dichos datos, deben ser notificados a la autoridad de control competente.

El RGPD lo que dispone es que, siempre y cuando esos incidentes de seguridad supongan un riesgo para los derechos y las libertades de las personas físicas, se tienen que notificar, a más tardar en el plazo de 72hrs desde su conocimiento. Aunque parezca que las brechas de seguridad solamente afecten a grandes empresas, estas pueden ocurrir en cualquier entidad independientemente de su tamaño.

En la guía de la AEPD sobre gestión y notificación de brechas de seguridad, a modo orientativo, encontramos en su anexo III un modelo que puede servir de referencia para tomar la decisión de notificar a la autoridad de control. El cálculo del posible riesgo se obtiene de tres parámetros: volumen, tipología de datos e impacto. Cada uno de ellos está valorado con un rango. Así, por ejemplo, en el caso de que el riesgo de valor cuantitativo esté en un umbral superior a 20 (más o menos) y coincidan dos circunstancias cualitativas, habría que notificarla a la autoridad.

Contenido

IMPORTANTE

La comunicación se realizará presentando el formulario de notificación de incidentes de seguridad de datos personales. Se puede encontrar en la sede electrónica de la AEPD.

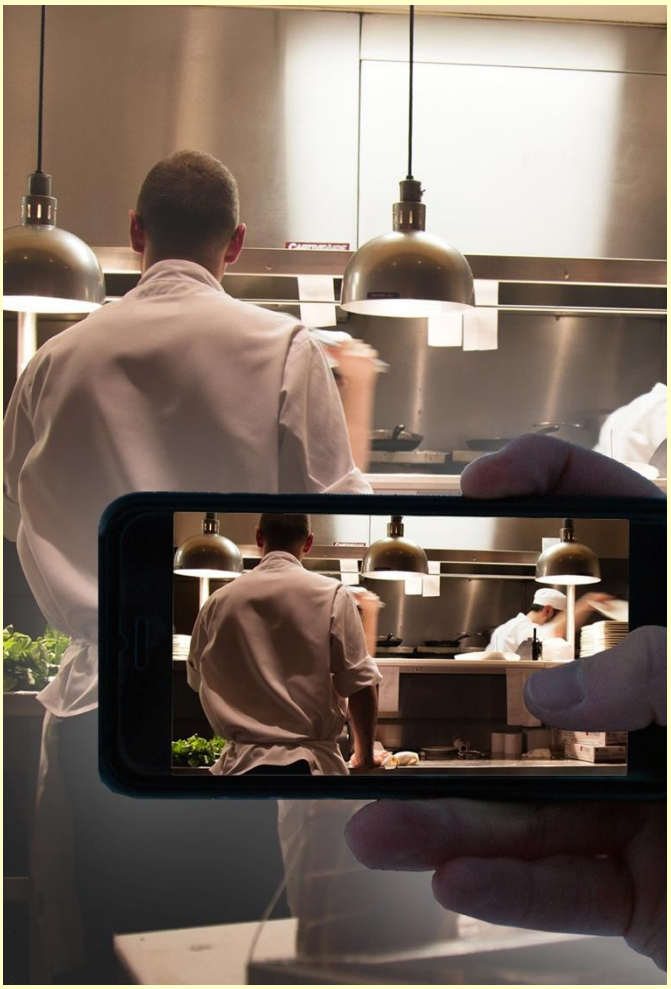
SANCIONES DE LA AEPD

Un restaurante multado por captación ilícita de imágenes de un trabajador y utilizarlas como base de sanción laboral

La AEPD impuso una multa administrativa de 12.000 euros por infringir el art. 5.1 a) del RGPD al tratar los datos del trabajador de forma ilícita.

La AEPD sanciona al RESTAURANTE LA OLIVA,https://www.aepd.es/resoluciones/PS-00401-2018_ORI.pdf por la captación de forma ilícita de las imágenes de uno sus trabajadores.

La reclamación presentada por el trabajador A.A.A. obedece al hecho de las grabaciones que le fueron realizadas en el interior y exterior del local para utilizarlas como prueba en la sanción disciplinaria que le fue impuesta por la empresa. El reclamante manifiesta que no fue avisado previamente de la instalación de las cámaras de vigilancia con la finalidad de control laboral y que tampoco había carteles informativos.



La AEPD inicia el procedimiento sancionador al RESTAURANTE LA OLIVA por la presunta infracción del art.5.1 a) del RGPD “los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado”. En la fase de alegaciones, el responsable indica que las videocámaras instaladas no funcionaban correctamente, ya que no tenían el software necesario, añadiendo que las imágenes habían sido tomadas con el móvil particular de otro empleado. La AEPD considera que el reclamado, al decidir sobre la finalidad y uso de las imágenes captadas con el dispositivo móvil, se convierte en responsable de las mismas, por lo que será objeto de aplicación del RGPD. El restaurante no informó al trabajador de la existencia de esas grabaciones, ni de su utilización para el control laboral.

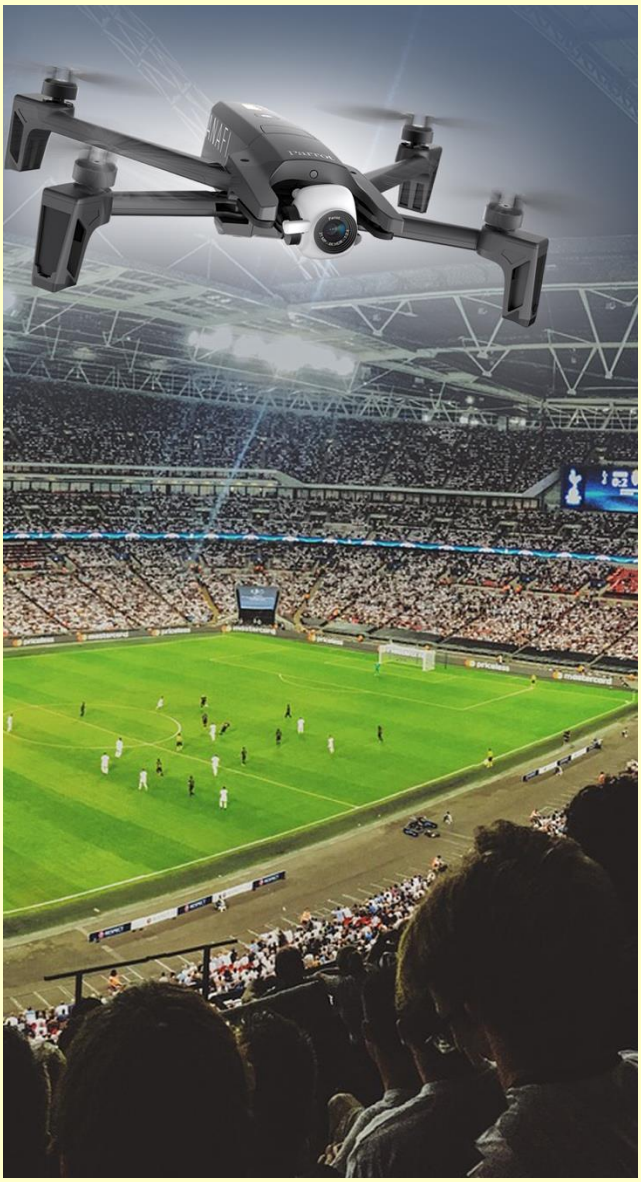
IMPORTANTE

El responsable debe facilitar al personal una información previa, expresa, clara y detalla del uso de los dispositivos tecnológicos con la finalidad de control laboral.

LA AEPD ACLARA

Qué implica la normativa de protección de datos a los operadores de drones.

La AEPD da respuesta en este informe https://www.aepd.es/media/informes/informe-juridico-rgpd-drones.pdf a la consulta planteada por una empresa de operadores de drones.



En este informe, lo primero que se analiza es la definición de dron. Con carácter genérico, se considera un vehículo aéreo de distintas categorías y capacidades variables que pueden incorporar, en su caso, sistemas de detección y equipos de radiofrecuencia. Según la AEPD lo relevante será el equipamiento de captación y el procesamiento de los datos personales de personas físicas lo que determine la aplicación de la legislación de protección de datos.

Los drones pueden realizar funciones de captación de imágenes para fines de videovigilancia, eventos deportivos, bodas, gestión de infraestructuras, etc. En todos estos supuestos se ha de cumplir con los principios esenciales de limitación de la finalidad, minimización de datos personales y licitud del tratamiento, es decir, que los datos sean recogidos de forma lícita atendiendo a toda la legislación y regulación propia relativa a los drones.

Los operadores de drones, en el ámbito de la normativa de protección de datos, operan como encargados del tratamiento, por lo que, además de cumplimentar un contrato de prestación de servicios, con sus propias características, deben regular el tratamiento de los datos personales con un contrato de acceso a datos.

IMPORTANTE

Se debe informar de la forma más apropiada posible y con carácter previo al uso de los drones. Indicando claramente quién es el responsable del tratamiento y las finalidades.

ACTUALIDAD LOPD

La AEPD publica el listado de tratamientos que no requieren de una EIPD

https://www.aepd.es/prensa/2019-09-04.html

(Madrid, 4 de septiembre de 2019). La Agencia Española de Protección de Datos (AEPD) ha publicado el listado de tratamientos de datos personales en los que no es obligatoria la realización de una evaluación de impacto, con el objetivo de facilitar a los responsables la identificación de este tipo de tratamientos. El Reglamento General de Protección de Datos (RGPD) recoge en su artículo 35.1 que las organizaciones que traten datos están obligadas a realizar una Evaluación de Impacto relativa a la Protección de Datos (EIPD) antes de efectuar dichos tratamientos cuando sea probable que, en función de su naturaleza, alcance, contexto o fines, entrañen un alto riesgo para los derechos y libertades de las personas.

Por otra parte, el apartado 5 del mismo artículo establece que las autoridades de control podrán publicar la lista de los tipos de tratamiento que no requieren una evaluación de impacto. Asimismo, y como contempla el RGPD, la Agencia ha comunicado al Comité Europeo de Protección de Datos (CEPD) el listado, que también se encuentra disponible en inglés. Esta lista, que no exime de cumplir el resto de obligaciones establecidas en la normativa de protección de datos, complementa a la publicada con anterioridad por la Agencia donde figuran aquellos tratamientos en los que sí es obligatorio llevar a cabo una EIPD.

La Agencia ha definido que no será necesario realizar una EIPD cuando se realicen tratamientos bajo directrices contenidas en circulares o decisiones emitidas previamente por las Autoridades de Control, en particular la AEPD, siempre y cuando el tratamiento no se haya modificado desde que fue autorizado.

Tampoco se requiere si el tratamiento se realiza cumpliendo con códigos de conducta aprobados por la Comisión Europea o las Autoridades de Control, siempre que ya se hubiera llevado a cabo una EIPD para validar dicho código de conducta e incluyera las salvaguardas definidas en la Evaluación de Impacto.

Dentro de los tratamientos que forman parte del listado también se encuentran, entre otros, aquellos que lleven a cabo los trabajadores autónomos que ejerzan de manera individual, en particular médicos, profesionales de la salud o abogados, sin perjuicio de que pueda requerirse cuando dichos tratamientos cumplan con dos o más criterios establecidos en la lista de tipos de tratamientos de datos que requieren EIPD; así como los obligatorios por ley y realizados con relación a la gestión interna del personal de las pymes con finalidad de contabilidad, gestión de recursos humanos y nóminas, seguridad social y salud laboral, pero nunca relativos a los datos de los clientes.

Puede ver más información en el siguiente enlace:

Listado completo de tratamientos

https://www.aepd.es/media/guias/ListasDPIA-35.5l.pdf

EL PROFESIONAL RESPONDE

Cuando nos llega una solicitud de un derecho. ¿Cómo hemos de responder?

Los derechos que puede ejercitar un afectado son los derechos de acceso, rectificación, supresión ("derecho al olvido"), oposición, portabilidad, limitación del tratamiento y derecho de oposición a las decisiones automatizadas (incluyendo la elaboración de perfiles). Cada uno de ellos puede ejercerse ante el responsable del tratamiento, delegado de protección de datos e incluso encargado del tratamiento, cuando así se haya previsto en el contrato de acceso a datos.

El plazo para resolver puede variar dependiendo del tipo de derecho solicitado, así, por ejemplo, el derecho de supresión se realizará sin dilación indebida, aunque, en cualquier caso, el plazo para responder será de un mes desde que se recibe la solicitud. Podríamos prorrogarlo dos meses más si fuera necesario, dependiendo de la complejidad del asunto y el número de solicitudes. En este caso, tendremos que informar al interesado de los motivos de la dilación dentro del plazo de un mes desde que recibimos la petición.

¿Qué ocurre si no es posible cursar el derecho solicitado? Tendremos que informar al interesado sin dilación indebida y, a más tardar, dentro del plazo de un mes de las razones por las cuáles no se puede dar respuesta a su derecho. Además, le informaremos de la posibilidad de presentar una reclamación a las autoridades de control.

IMPORTANTE

En todas las entidades debería existir un protocolo de actuación para dar respuesta a los derechos de los interesados para evitar graves sanciones por su incumplimiento.