Boletín 02/21

LOPD EN LA EMPRESA

Autor: Julio César Miguel Pérez

Balaguer & Gutiérrez
Correduría de Seguros
Consultoría de Protección de Datos

EL RGPD UE 2016/679 EN APLICACIÓN

La notificación y el registro de las brechas de seguridad

En el caso de que una empresa haya sufrido alguna de las diferentes tipologías de brechas de seguridad que indicábamos en el boletín pasado, tales como; brechas de confidencialidad, brechas de integridad y/o brechas de disponibilidad, ha de cumplir con las siguientes obligaciones recogidas en el RGPD. Es el responsable el que tiene que llevarlas a cabo, salvo que, en el contrato de acceso a datos se haya dispuesto que lo gestione el encargado de tratamiento.

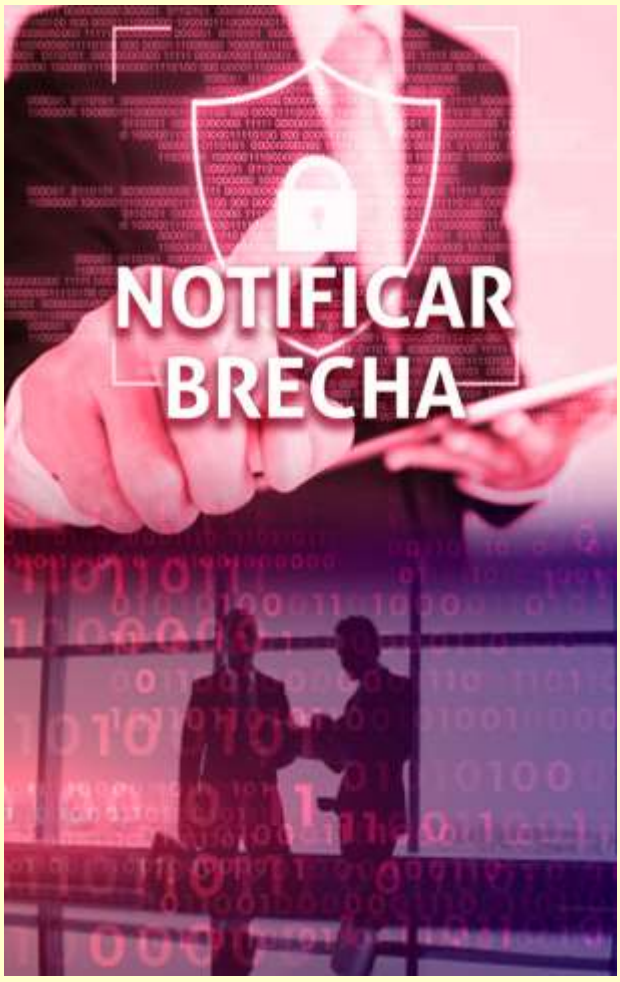
1º Se notificará a la autoridad competente, en el plazo de 72 horas desde su conocimiento, siempre y cuando suponga un riesgo para los derechos y libertades de los afectados.

2º Si no se notifica en el plazo de 72 horas, habría que indicar los motivos de la dilación. En el caso de que no pueda facilitar la información simultáneamente, ésta se entregará de forma gradual sin dilación indebida.

3º La notificación ha de tener un contenido mínimo, tal y como indica el art. 33.3 del RGPD;

Además de todas esas acciones, el RGPD hace referencia a la obligación que tiene el responsable de documentar cualquier brecha ocurrida en su empresa aunque no sea preciso notificarla a la autoridad competente.

Contenido



IMPORTANTE

El encargado de tratamiento está obligado a comunicar al responsable cualquier brecha de seguridad de la que tenga conocimiento.

SANCIONES DE LA AEPD

Comunidad de propietarios sancionada por notificar deudas en el tablón de anuncios.

En el procedimiento sancionador https://www.aepd.es/es/documento/ps-00143-2020.pdf una comunidad de propietarios recibe una sanción de apercibimiento por notificar indebidamente las deudas a un propietario.

El reclamante manifiesta que sus datos de carácter personal y económicos han sido expuesto ante terceros, puesto que la notificación se realizó en el tablón de anuncios.

Ante la AEPD llegan las alegaciones de la comunidad de propietarios, la cual manifiesta, qué además de la publicación en el tablón correspondiente se realizó mediante burofax no siendo recogido por el deudor.

La AEPD estima que la comunidad no actuó correctamente, por un motivo de falta de cumplimiento de plazos, ya que el cartel anunciando la convocatoria que contenían la deuda y los datos personales se hizo antes de que transcurriera el plazo para recoger la notificación.

La sanción que se le pide a la comunidad es de apercibimiento, lo que implica, que en el plazo de un mes tiene que acreditar ante la AEPD el cumplimiento de que procede con todas las medidas necesarias para que el reclamado actúe de conformidad con los principios del art.5.1. f del RGPD; principio de integridad y confidencialidad.

Este tipo de sanciones hacen ver de la necesidad que tiene los responsables de tener un protocolo adecuado en protección de datos.

Principio de confidencialidad: garantizar al interesado la intimidad de sus datos frente a terceros.

IMPORTANTE

Los requerimientos que la AEPD solicita al responsable en las sanciones de apercibimiento deben realizarse en el plazo máximo de un mes.

LA AEPD ACLARA

¿Cuándo es posible la grabación de imágenes en el ámbito educativo?

En esta sección del boletín haremos referencia a las consultas que la AEPD ha ido resolviendo a través de la publicación de sus guías sectoriales.https://www.tudecideseninternet.es/aepd/images/guias/GuiaCentros/GuiaCentrosEducativos.pdf

En este caso, se trata de dar respuesta a la legitimación del tratamiento de la grabación de imágenes de alumnos/as y profesores/as en los centros educativos.

Habría que distinguir entre la toma de imágenes como parte de la función educativa, en estos casos, estaría legitimado en el cumplimiento de la normativa propia y no precisaría de consentimiento.

Así, por ejemplo, tal y como indica la guía, los profesores en el desarrollo de la programación y enseñanza de las áreas, materias y módulos, puede precisar la realización de ejercicios que impliquen la grabación de imágenes, las cuáles solamente han de estar disponibles para las partes interesadas, es decir, alumnos/as, padres o tutores y el personal docente correspondiente. **En ningún caso, se podría difundir de forma de forma abierta en internet, sin el consentimiento de los interesados.**

Por otro lado, también es posible la toma de imágenes del alumnado en determinados eventos desarrollados en el entorno escolar con la única finalidad de que los padres puedan acceder a ella. Este acceso debería llevarse a cabo en un entorno seguro, que exigiera la previa identificación y autenticación de los interesados involucrados.

IMPORTANTE

Supone una vulneración del deber de confidencialidad la divulgación de las imágenes obtenidas a través de la intranet facilitada por el centro educativo.

ACTUALIDAD LOPD

La AEPD lanza un Pacto Digital con el respaldo de las principales organizaciones empresariales, fundaciones y asociaciones

Fuente: AEPD

(Madrid, 21 de enero de 2021). La Agencia Española de Protección de Datos ha lanzado el Pacto Digital para la Protección de las Personas, una iniciativa que forma parte del Marco de Responsabilidad Social y Sostenibilidad de la Agencia y que promueve un gran acuerdo por la convivencia en el ámbito digital. Su objetivo es tanto fomentar el compromiso con la privacidad en los modelos de negocio de empresas y organizaciones, compatibilizando el derecho a la protección de datos con la innovación, la ética y la competitividad empresarial, como concienciar a los ciudadanos, y en especial a los menores, de las consecuencias de difundir contenidos sensibles en Internet.

El desarrollo del proyecto ha contado con la colaboración de las principales organizaciones empresariales, fundaciones, asociaciones de medios de comunicación y grupos audiovisuales, que lo han ratificado adhiriéndose al Pacto. A través de esta adhesión, las entidades se han comprometido a implantar los principios y recomendaciones recogidas en el mismo, así como a difundir entre sus usuarios, clientes y empleados el Canal prioritario para solicitar la eliminación urgente de contenidos sexuales y violentos difundidos sin consentimiento en internet, y otros recursos y herramientas de la AEPD para ayudar a la concienciación sobre el valor de la privacidad y la importancia del tratamiento de los datos personales.

El **Pacto Digital para la Protección de las Personas** promueve la privacidad como un activo para organizaciones. Con él la Agencia pretende concienciar de que junto a un derecho puede existir también una obligación. Para ello, es necesario que todos los actores implicados en el ámbito digital, los ciudadanos y las organizaciones, sean conscientes de las consecuencias que puede suponer en la vida de la persona afectada la difusión de contenidos especialmente sensibles y también las responsabilidades en que pueden incurrir aquellos que los difunden (civiles, penales y administrativas).

Entre los principios del Pacto también se encuentra impulsar la transparencia para que los ciudadanos conozcan qué datos se están recabando y para qué se emplean, promover la igualdad de género y la protección de la infancia y las personas en situación de vulnerabilidad, o promover la innovación garantizando que las nuevas tecnologías eviten perpetuar sesgos o aumentar las desigualdades existentes, evitando la discriminación algorítmica por razón de raza, procedencia, creencia, religión o sexo, entre otras.

Puede ver más información en el siguiente enlace

Pacto Digital para la Protección de las Personas

EL PROFESIONAL RESPONDE

Las fases principales de un ataque de ingeniería social

La mayoría de los ataques de ingeniería social que pude sufrir una empresa tiene la misma operativa. **Conocer sus fases nos ayuda a prevenirlo puesto que lo vamos a poder identificar a tiempo para actuar con diligencia.**

El ciclo de vida de este tipo de ataque consiste en tres fases:

1ª Fase de reconocimiento: Esta fase conocida también como footprinting consiste en recabar toda la información posible de las potenciales victimas del fraude, por ejemplo, números de teléfono, nombres de dominio, correo electrónico, etc...

2ª Fase de manipulación: La manipulación psicológica es clave en este tipo de fraudes. Así por ejemplo hacer creer que existe una determinada urgencia en una operación muy importante que ha costado mucho conseguir, actuar rápidamente para no perder un servicio. Lo que trata el ciberdelincuente es establecer una relación de confianza utilizando nombres de dominios falsos o suplantando la identidad de una persona u organización conocidas.

3ª Fase final del ataque: Una vez obtenido el objetivo el ciberdelincuente tratará que el fraude no sea descubierto, puesto que así la extorsión puede continuar durante más tiempo y el impacto será mayor para la empresa.

IMPORTANTE

La formación y el conocimiento en el funcionamiento de los distintos tipos de ataque son herramientas fundamentales para su prevención.