Boletín 09 /23

LOPD EN LA EMPRESA

AUTOR: JULIO CÉSAR MIGUEL PÉREZ

Altabir
www.altabir.es
Consultoría de Empresas desde 1996

EL RGPD UE 2016/679 EN APLICACIÓN

Los principios relativos al tratamiento (I)

Contenido

En este boletín y sucesivos abordaremos cuáles son los principios relativos al tratamiento. Estos principios generales son de obligado cumplimiento para los responsables que lleven a cabo un tratamiento de datos personales y sus encargados de tratamiento.

¿Cuáles son los principios generales relativos al tratamiento recogidos en el artículo 5 del RGPD?

A. **Principio de licitud lealtad y transparencia**: Los datos personales tienen que ser tratados de manera, lícita leal y transparente en relación con el interesado.
B. **Principio de limitación de la finalidad**: Los datos personales se recogerán con fines determinados, explícitos y legítimos.
C. **Principio de minimización de datos**: Los datos serán adecuados, pertinentes y limitados a lo necesario.
D. **Principio de exactitud**: Serán exactos, y si fuera necesario, actualizados.
E. **Principio de limitación del plazo de conservación**: Se conservarán no más tiempo del necesario.
F. **Principio de integridad y confidencialidad**: Se tiene que garantizar una seguridad adecuada.

IMPORTANTE

El tratamiento de datos personales vulnerando cualquiera de los principios generales es una infracción muy grave.

SANCIONES DE LA AEPD

Sancionada una asesoría fiscal por falta de confidencialidad en el tratamiento de datos personales

En la resolución de la AEPD https://www.aepd.es/documento/ps-00475-2022.pdf, se sanciona con 3.000 € a una asesoría fiscal por falta de confidencialidad en el tratamiento de los datos personales.

Uno de los principios relativos al tratamiento que se recoge en el artículo 5 del RGPD es el principio de integridad y confidencialidad. Los datos tienen que ser tratados de forma que se garantice una seguridad adecuada de datos personales incluyendo la protección contra el tratamiento no autorizado o ilícito.

En este caso la reclamante solicitó a la asesoría fiscal un justificante de las gestiones y documentos presentados ante la Agencia Tributaria. El justificante entregado contenía un documento electrónico emitido por la Agencia Tributaria que hacía referencia a otro administrado, con el código seguro de verificación se pudo acceder a datos personales que no correspondían a la parte reclamante. Por esta causa, la AEPD sancionó a la reclamada con la cantidad de 2.000 €. **Además, en el momento de producirse la brecha, las medidas de seguridad de que disponía la parte reclamada eran insuficientes para garantizar la confidencialidad de los datos personales.** Se le sanciona con 1.000 € por la falta de medidas de seguridad apropiadas.

Las reclamaciones por la publicación de datos en Internet sin consentimiento, videovigilancia y otros trámites se realizan a través de la SEDE ELECTRÓNICA de la AEPD.

IMPORTANTE

El responsable y encargado del tratamiento deben aplicar las medidas de seguridad técnicas y organizativas apropiadas para garantizar la confidencialidad de los datos personales.

LA AEPD ACLARA

¿Cuáles son los malentendidos sobre el aprendizaje automático?

La Agencia Española de Protección de datos junto con el Supervisor Europeo de Protección de Datos (EDPS) publicaron un documento conjunto en el que se recogen los 10 malentendidos sobre el aprendizaje automático. **La Inteligencia artificial (IA) es un término general que engloba a la tecnologías que tienen como objetivo imitar las capacidades de razonamiento humano. La definición de aprendizaje automático**, en inglés ***Machine Learning*, es una rama específica de la IA aplicada a la resolución de problemas específicos y limitados.** Estos modelos de *Machine Learning (ML)* se entrenan utilizando conjunto de datos. Algunos de estos malentendidos son:

1. **Al desarrollar sistemas de aprendizaje automático, cuanto más datos y mayor sea la variedad, mejor.** No es así, ya que la realidad es que los conjuntos de datos de entrenamiento de *ML* deben seleccionarse con criterios de precisión y representatividad.
2. **Los interesados son capaces de anticipar las posibles salidas que los sistemas de *ML* pueden dar con sus datos.** No es cierto, la realidad es que los sistemas de *ML* son capaces de identificar patrones en los datos personales que van más allá de los planteados en el desarrollo del modelo, y que serían desconocido incluso por los individuos afectados.

IMPORTANTE

El responsable del tratamiento y destinatarios de los datos deben cumplir con los principios de responsabilidad proactiva, seguridad y limitación de propósitos entre otros.

ACTUALIDAD LOPD

La AEPD apoya el Plan Digital Familiar de la Asociación Española de Pediatría

Fuente: AEPD

(14 de septiembre de 2023). La Agencia Española de Protección de Datos (AEPD) apoya el Plan Digital Familiar de la Asociación Española de Pediatría (AEP), una plataforma con información útil sobre el uso adecuado de internet por parte de los menores para familias y pediatras. Incluye, además, un documento que las familias podrán personalizar y adaptar a sus circunstancias particulares con recomendaciones avaladas por la evidencia científica en función de la edad de sus hijos y otras generales para todos los miembros.

"Lo primero que debemos tener claro es que las tecnologías han venido para quedarse y forman parte de nuestra vida. Los niños y adolescentes son especialmente vulnerables a sus riesgos al estar en desarrollo" apunta la **doctora María Salmerón**, coordinadora del grupo de trabajo de Salud Digital del Comité de Promoción de la Salud de la AEP.

"Lo que sí debemos tener en cuenta es que es difícil que los niños, de forma autónoma, hagan un buen uso de la tecnología. Por eso, es importante que nosotros, como padres, eduquemos a través del ejemplo, les supervisemos, estemos disponibles para ellos y establezcamos límites; en definitiva, que les ayudemos a gestionar su uso", añade la experta.:

Cómo se establece un plan

El Plan Digital de la AEP se materializa en un documento que las familias pueden adaptar a sus circunstancias particulares. Así, ofrece la opción de elegir entre una serie de propuestas basadas en recomendaciones científicas; unas en función de la edad y otras generales para todos los miembros. Tras la selección, se puede descargar un documento personalizado para aplicarlo en el hogar.

Puede ver más información en el siguiente enlace:

Plan Digital Familiar AEP

EL PROFESIONAL RESPONDE

¿Cuáles son los puntos mínimos que debe contener una política de control de acceso? (II)

El control de acceso a la información en la empresa resulta imprescindible para evitar fraudes y accesos ilícitos a la información y a los datos personales. Los puntos mínimos que debe contener una política de control de acceso son, entre otros:

1. **Definir la clasificación de la información:** puede ser confidencial; restringida; de uso interno o pública.
2. Determinar el perfil de usuarios y grupos de la empresa que pueden tener acceso a la información.
3. **Establecer los permisos que un grupo tiene sobre determinada información.**
4. Elaborar procedimientos para solicitar accesos extraordinarios a la información por aquellos perfiles que en un principio no estaban autorizados.
5. **Definir una periodicidad para realizar las revisiones de los permisos facilitados.**
6. Genera procedimientos para revocar la asignación de alguna persona a determinados grupos. Por ejemplo, cuando un trabajador/a se ausenta de la oficina durante un tiempo determinado.

No todas las personas necesitan acceder a toda la información para realizar correctamente sus funciones dentro de la empresa. Establecer estos puntos mínimos de control ayudará a la empresa a proteger la información y evitar problemas de fuga, acceso ilícitos o indisponibilidad de la información de la empresa.

IMPORTANTE

El control de acceso a la información de la empresa es una de las medidas organizativas que los responsables y encargados de tratamiento pueden incorporar en las medidas de seguridad.