Boletín 10/23

LOPD EN LA EMPRESA

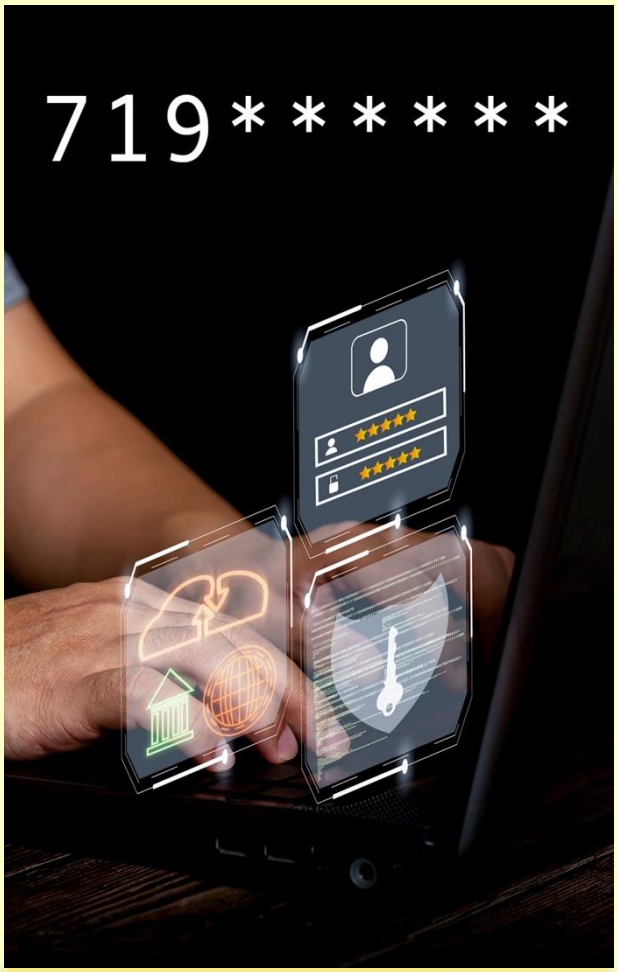
EL RGPD UE 2016/679 EN APLICACIÓN

Principio de integridad y confidencialidad de datos (II)

Contenido

Uno de los principios relativos al tratamiento es el principio de integridad y confidencialidad. Tanto el responsable del tratamiento como el encargado deben actuar garantizando una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito, aplicando las medidas de seguridad técnicas y organizativas más apropiadas.

La seudoanonimización de datos, es una medida que podemos aplicar para garantizar la confidencialidad de los datos. Un ejemplo lo encontramos en las orientaciones publicadas por la Agencia Española de Protección de datos (AEPD) para la publicación de datos personales por la Administraciones Públicas. Para garantizar la confidencialidad de los datos personales y minimizar el impacto en la privacidad de los ciudadanos la identificación incluirá como datos personales; el nombre, apellidos y la seudoanonimización del DNI con la publicación de las cuatro cifras aleatorias del documento oficial de identidad. Con relación a la aplicación de las cuatro cifras aleatorias la AEPD estableció unas orientaciones para ser cumplidas por todas las administraciones y evitar que la adopción de otras fórmulas de lugar a la publicación de cifras numéricas de los DNI, posibilitando con ello la recomposición íntegra de los documentos.



IMPORTANTE

Se deben aplicar medidas técnicas y organizativas apropiadas que garanticen una confidencialidad e integridad de los datos.

SANCIONES DE LA AEPD

La AEPD sanciona con 15.000 € a una empresa de seguridad por enviar correos electrónicos sin copia oculta

En la resolución de la AEPD https:// https://www.aepd.es/documento/ps-00452-2022.pdf, sanciona a una empresa de seguridad con 15.000 € por enviar correos electrónicos sin copia oculta al personal laboral de la empresa.

El reclamante, un trabajador de la empresa de seguridad, manifestó en su reclamación que se enviaron comunicaciones laborales al teléfono personal y al correo electrónico personal sin copia oculta. En este caso, la AEPD no sancionó a la empresa por el uso de la aplicación de mensajería de WhatsApp puesto que esta fue creada por el departamento de coordinación de la empresa y el teléfono fue facilitado de forma voluntaria por los trabajadores/as.

Por otro lado, sí que se sanciona el envío de comunicaciones laborales al correo electrónico sin utilizar la copia oculta. Supone una sanción puesto que se reveló la dirección de correo de la parte reclamante y del resto de destinatarios sin su consentimiento. **La empresa no contaba con ninguna legitimación para revelar la dirección del correo personal del reclamante. Este hecho supone una vulneración del principio de integridad y confidencialidad recogido en el art. 5.1 f del RGPD, por lo que se le sanciona con una multa de 15.000 €. Además, se le sancionó con 5.000 € por no aplicar las medidas de seguridad técnicas y organizativas para garantizar la confidencialidad de los datos.**

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

Nuestra LOPDGDD considera una infracción muy grave el tratamiento de los datos personales vulnerando los principios y garantías del Reglamento General de Protección de datos.

LA AEPD ACLARA

Proteger a las personas en el mundo digital: Comunicación de brechas de seguridad a los interesados (I)

La Agencia Española de Protección de datos ha publicado en su página web una infografía sobre la comunicación a los afectados de una brecha digital, tal y como dispone el art. 34 del RGPD. **En este documento de forma muy sencilla se van dando respuesta a las preguntas siguientes:**

¿Para qué? Para proteger a las personas ante las consecuencias de una brecha de datos personales.

¿Cuándo? Cuando se produzca un alto riesgo para los derechos y libertades de las personas.

¿A quién? A aquellas personas físicas que se encuentren en alto riesgo debido a la brecha.

¿Plazo? Sin dilación indebida. Antes de que las consecuencias puedan afectar a las personas y con tiempo para que se protejan.

¿Cómo? Con una comunicación dirigida a cada uno de los afectados. Por ejemplo, mediante un email, SMS, mensajería instantánea o correo postal. En el caso de que suponga un esfuerzo desproporcionado o se desconoce con precisión quien ha podido verse afectado, se puede realizar un comunicado público.

En la comunicación se deben evitar expresiones que distorsionen el mensaje, por ejemplo, "no corre riesgo". Además, no se deben omitir detalles relevantes para que las personas puedan valorar el riesgo de forma adecuada.

IMPORTANTE

No es una comunicación debida a los afectados cuando se comunica exclusivamente a la empresa cliente o un comunicado público injustificado sin contenido mínimo.

ACTUALIDAD LOPD

La Agencia lanza la herramienta ValidaCripto para evaluar los sistemas de cifrado

Fuente: AEPD

(5 de octubre de 2023). La Agencia Española de Protección de Datos (AEPD) ha lanzado la nueva herramienta ValidaCripto RGPD, que ayuda a evaluar los sistemas de cifrado para facilitar el cumplimiento de la normativa analizando cada uno de los elementos del proceso. Tras la publicación de las Orientaciones para la validación de sistemas criptográficos en la protección de datos junto a ISMS Forum y APEP el pasado mayo, y debido a la buena acogida nacional e internacional de la guía, la Agencia ha trasladado su metodología a una herramienta web ágil e intuitiva.

La herramienta gratuita se ejecuta localmente en el navegador, sin registrar ni transmitir ningún dato a la AEPD. Cuenta con un apartado de ayuda donde se explica su funcionamiento paso a paso, desde la selección del impacto del sistema de cifrado en el tratamiento, la categorización de los elementos más críticos, el repaso de los controles sugeridos y la generación de una documentación de seguimiento. Su objetivo es **ofrecer una solución eficaz** para verificar la idoneidad de los sistemas criptográficos implementados en los tratamientos de datos personales, seleccionando en la **lista de controles** propuestos aquellos que pudieran ser los más oportunos. Los datos pueden almacenarse y cargarse en un archivo local, bajo el control total del usuario, y permite generar informes.

La protección de los datos personales es un derecho fundamental que requiere medidas adecuadas para garantizar su seguridad. Una de estas medidas es el uso de sistemas criptográficos que permitan cifrar la información sensible, transformando la información en un conjunto de datos aparentemente ininteligible. Actualmente, **dos mil millones de personas** utilizan diariamente el cifrado para proteger sus comunicaciones (European Digital Rights 2023). El Reglamento General de Protección de Datos lo menciona como una medida que forma parte de las condiciones para la conformidad del tratamiento y como ayuda para **mitigar los riesgos ante una posible brecha de datos personales**.

Puede ver más información en el siguiente enlace:

Orientaciones para la validación de sistemas criptográficos en la protección de datos.

EL PROFESIONAL RESPONDE

Las copias de seguridad: medida imprescindible para proteger la información de la empresa

Uno de los activos más importantes de la empresa es la información y por ello debemos aplicar todas las medidas de seguridad técnicas y organizativas posibles para garantizar, la disponibilidad, integridad y confidencialidad de la información de la empresa.

Una de estas medidas son las copias de seguridad. Dependiendo del tamaño y necesidades de la empresa el procedimiento para realizar copias de seguridad puede ser distinto. El soporte dependerá del sistema de copia, de la fiabilidad que necesitemos y de la inversión a realizar.

En la implantación de un sistema de copias debemos tener en cuenta:

- El análisis de información sobre la que se va a realizar la copia, las configuraciones de dispositivos de red y los equipos de usuarios.
- Definir el número de versiones que vamos a almacenar de cada elemento guardado, y su periodo de conservación. Así, por ejemplo, si el volumen de información es bajo, se puede realizar una copia total diaria.
- Realizar pruebas de restauración periódicas.
- Disponer de una copia de seguridad fuera de la organización, para evitar la pérdida de información en caso de incendio, robo o inundación.
- Documentar el proceso de realización de copia y restauración.

IMPORTANTE

Si utilizamos proveedores de almacenamiento en la nube debemos seleccionar aquellos que nos garanticen una mayor seguridad en el almacenamiento y recuperación de la información.