PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

www.prodasur.es
prodasur@prodasur.es
952 60 37 70

Boletín 06/24

EL RGPD UE 2016/679 EN APLICACIÓN

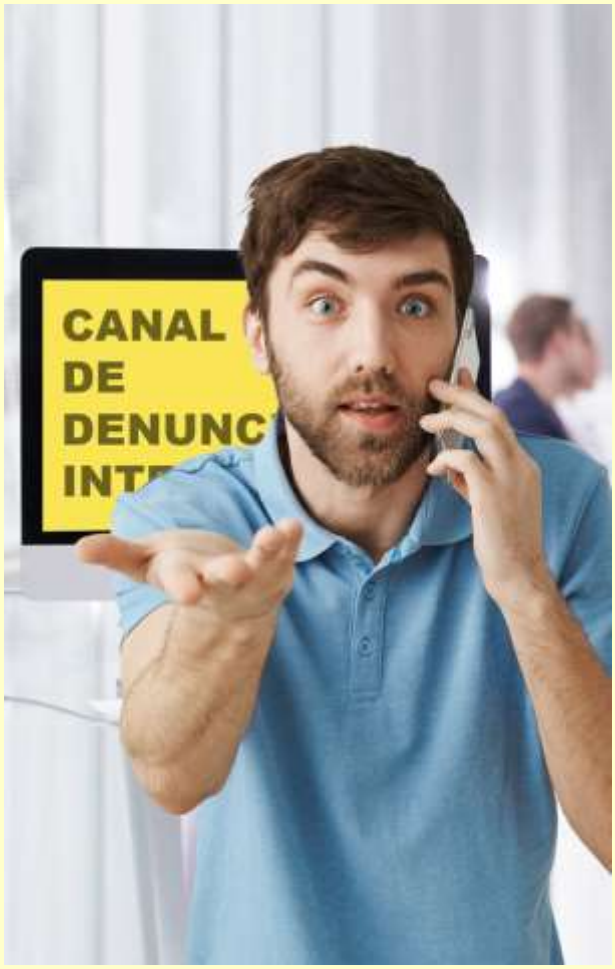
Tratamiento de datos en los sistemas de denuncias interno (II)

En la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de la lucha contra la corrupción hace referencia al procedimiento de gestión de las denuncias.

¿Cuáles son los requisitos para implementar un canal de denuncias?

1. Se tiene que identificar claramente la existencia del canal de denuncias e informar a todo el personal laboral.
2. **Las comunicaciones podrán realizarse por escrito (correo postal o electrónico), verbales (por teléfono o mensajería) o inclusive presencialmente.**
3. Enviar acuse de recibo al informante, en el plazo de siete días naturales siguientes a su recepción.
4. **Garantizar la anonimidad de los informantes cuando opten por realizar una denuncia anónima.**
5. Informar de la existencia del canal externo de información de la Autoridad Independiente de Protección del Informante (A.A.I)
6. Disponer de una política interna de protección de los informantes, de un procedimiento para gestión de denuncias y un libro registro de denuncias.

Contenido



IMPORTANTE
El tercero externo que gestione el sistema de denuncias tendrá la consideración de encargado del tratamiento y por lo tanto habrá que formalizar el contrato de acceso a datos.

SANCIONES DE LA AEPD

Sancionada una clínica dental por no atender debidamente una brecha de seguridad de datos personales

En la resolución de la AEPD https://www.aepd.es/documento/ps-00078-2024.pdf se sanciona a una clínica dental por no atender a tiempo una brecha de seguridad de datos personales.

La entidad sancionada comunicó a la División de Innovación Tecnológica de la AEPD una brecha de seguridad de datos personales, siendo ésta realizada en una fecha muy posterior al plazo legal que marca la norma de 72hrs. Se comunicó la detección de un *Malware* en el ordenador servidor de la clínica, que impedía el acceso al sistema informático utilizado para la recopilación de datos. La brecha afectó a la disponibilidad y confidencialidad de los datos personales entre los que se incluían datos de salud e historiales clínicos de los pacientes.

La AEPD en su labor de investigación solicitó a la sancionada el registro documentado de la brecha de seguridad, el registro de actividades de tratamiento, la comunicación a los afectados y justificación del motivo de retraso de la notificación de la brecha. Además, le solicitó el análisis de riesgos, la posible Evaluación de impacto y las medidas de seguridad implementadas antes y después de la brecha.

La sanción ascendió a 20.000€ por falta de diligencia en la notificación y no haber aplicado las medidas adecuadas para mitigar los riesgos.

La falta de adopción de las medidas técnicas y organizativas que garanticen un nivel de seguridad adecuado al riesgo es una infracción grave.

IMPORTANTE

La notificación de una brecha de seguridad de datos personales debe hacerse de forma inmediata y a más tardar en las 72hrs después de conocer el incidente.

LA AEPD ACLARA

Inteligencia Artificial. Sistemas, tratamiento, medios y finalidad

En el apartado de Innovación y Tecnología de la página de la AEPD encontramos información relevante sobre el uso de sistemas de Inteligencia Artificial (IA) por los responsables de tratamiento de datos personales.

La utilización de los sistemas de Inteligencia Artificial (IA) no siempre van a suponer que sus resultados impliquen una decisión automatizada. Los responsables del tratamiento son lo que finalmente decidirán si esos resultados son automatizados o bien, se incluye una supervisión humana que tome la decisión final.

La AEPD plantea un ejemplo de utilización de sistemas de IA para la captación de nuevo personal de la empresa. En este tratamiento habrá varias operaciones para conseguir el resultado final, que es el reclutamiento, en el que se apliquen sistemas de IA como medios o herramientas, pero no como finalidad última. Así, por ejemplo, el procedimiento para guiar a los candidatos a completar el formulario de solicitud para incluir sus CV podría implementarse mediante un *chatbot* (IA). En el caso de que existiera un alto número de participación de candidatos, el responsable puede decidir utilizar un sistema de IA para la selección automática de los CV más interesantes, de acuerdo con un criterio establecido por el responsable. Sera éste quién determine si la selección será supervisada por un humano o no.

IMPORTANTE

En la toma de decisiones individuales automatizadas, se debe garantizar al interesado obtener intervención humana por parte del responsable, expresar su punto de vista e impugnar la decisión.

ACTUALIDAD LOPD

Worldcoin se compromete a paralizar su actividad en España

Fuente: AEPD

(4 de junio de 2024). La Agencia Española de Protección de Datos (AEPD) ordenó el pasado marzo una medida cautelar para que *Tools for Humanity Corporation* cesase en la recogida y tratamiento de datos personales que estaba realizando en España en el marco de su proyecto *Worldcoin*.

Mientras tanto, las investigaciones de la *Bayerisches Landesamt für Datenschutzaufsicht (BayLDA*), la autoridad de protección de datos de Baviera (Alemania), donde la empresa tiene su establecimiento principal en Europa, están avanzando y se espera que concluyan pronto con una decisión final alineada con todas las autoridades de supervisión europeas interesadas. En este contexto, la compañía se ha comprometido de forma jurídicamente vinculante a no reanudar su actividad en España hasta final de año o hasta que la *BayLDA* adopte una resolución definitiva en relación con el tratamiento de datos realizado por la compañía.

Este compromiso legalmente vinculante adoptado por la empresa no afecta a las competencias de la *BayLDA* o de la AEPD para adoptar medidas de supervisión adicionales en caso de incumplimiento de estas obligaciones.

La medida cautelar, establecida en el artículo 66.1 del Reglamento General de Protección de Datos (RGPD) para proteger los derechos y las libertades de interesados, fue avalada por la Audiencia Nacional al considerar que prevalecía "la salvaguarda del interés general que consiste en la protección del derecho a la protección de datos personales de los interesados frente al interés particular de la empresa".

Con posterioridad a la medida provisional impuesta por la Agencia, Tools for Humanity Corporation anunció cambios en su funcionamiento, como la introducción de controles para verificar la edad o la posibilidad de eliminar el código del iris. La Agencia está colaborando con la autoridad de protección de datos de Baviera, al ser esta la autoridad principal en cuanto al tratamiento de datos, siendo la AEPD autoridad interesada, tal y como establece el RGPD.

Puede ver más información en el siguiente enlace:

Medida cautelar que impide a *Worldcoin* seguir tratando datos personales en España

EL PROFESIONAL RESPONDE

¿Cuáles son los principales incidentes de ciberseguridad? (II)

Es importante conocer cuáles son los principales incidentes de ciberseguridad para poder afrontarlos y aplicar las medidas de seguridad técnicas y organizativas adecuadas para minimizar los riesgos.

Estos son algunos de los principales incidentes de ciberseguridad:

- **Infecciones por código malicioso**: sobre todo a través de correo electrónico, páginas web comprometidas, SMS o redes sociales.
- **Intrusión y vulnerabilidades**: Explotación de vulnerabilidades conocidas, compromiso de cuentas y aplicaciones y suplantación de identidad.
- **Ataques *DoS* y fallos de disponibilidad**: Denegación de servicio afectando recursos como redes, servidores y equipos.
- **Compromiso de la información**: cuando se produce un acceso no autorizado o se ha producido una modificación por cifrado de *ransomware.*
- **Fraude y *phishing***: a través de la suplantación de entidades legítimas para beneficio económico.
- **Escaneo de redes (*scanning*)** para investigar sobre tecnologías y sistemas utilizadas por la empresa.
- **Análisis de paquetes (*sniffing*)** analizar el tráfico de red permitiendo un monitoreo de redes en tiempo real.

IMPORTANTE

La inversión en ciberseguridad resulta crucial para la prevención y minimización de los riesgos ocasionados por los incidentes de ciberseguridad.