PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

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

Boletín 05/24

EL RGPD UE 2016/679 EN APLICACIÓN

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

Contenido

La puesta en marcha de un canal de denuncias interno supone un tratamiento de datos personales que iremos abordando en boletines sucesivos. **Está regulado en nuestra LOPDGDD, además, se aprobó 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**.

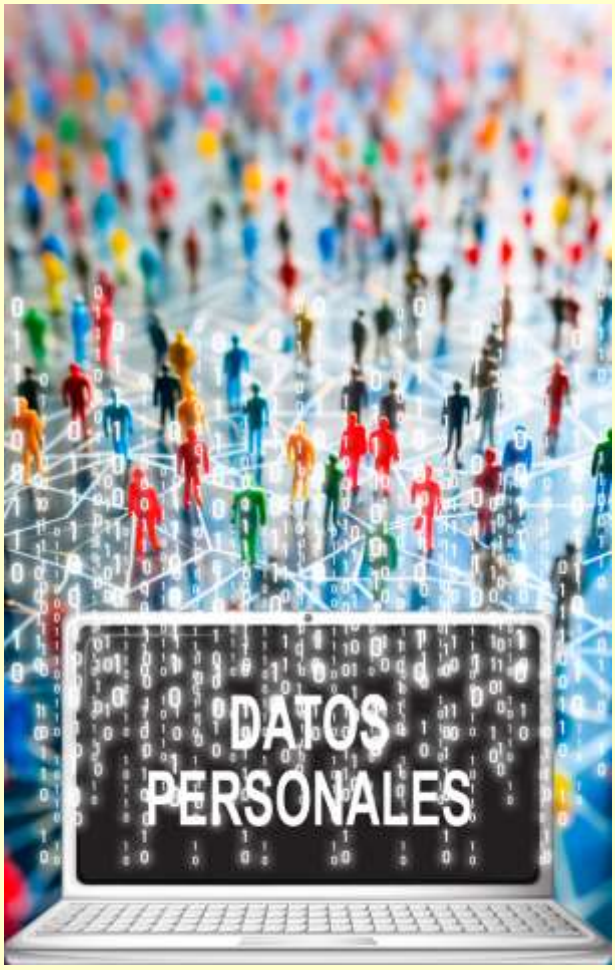
En esta norma encontramos los sujetos obligados a habilitar este canal de denuncias:

Entidades obligadas del sector privado

- Empresas que tengan contratados 50 o más trabajadores/as.
- Empresas del sector de servicios, productos y mercados financieros, prevención del blanqueo de capitales o de la financiación del terrorismo, seguridad del transporte y protección del medio ambiente.
- Los partidos políticos, los sindicatos, las organizaciones empresariales las fundaciones, que reciban o gestionen fondos públicos.

Entidades obligadas del sector público

Las entidades que integran el sector público están obligadas a disponer de este sistema de información interno. Entre otras, universidades públicas, corporaciones de derecho público y fundaciones del sector público.



IMPORTANTE

Los sujetos obligados han de tener implementado el canal de denuncias interno para evitar ser sancionados por incumplimiento de la Ley 2/2023

SANCIONES DE LA AEPD

Empresa tecnológica sancionada por no cumplimentar el contrato de acceso a datos con terceros

En la resolución de la AEPD https://www.aepd.es/documento/ps-00576-2021.pdf se sanciona a una empresa del sector tecnológico por no haber cumplimentado debidamente el contrato de encargado de tratamiento con su proveedor subcontratado de alojamiento en la nube.

La AEPD inició de oficio las actuaciones de investigación al recibir una notificación de una brecha de seguridad con respecto a un proveedor de servicios de hosting y almacenamiento en la nube. Los responsables del tratamiento fueron avisados por su encargado del tratamiento de la brecha de seguridad del proveedor de hosting.

La APED, solicitó a la empresa del sector tecnológico sancionada, que le facilitase el contrato de acceso a datos con el proveedor de servicios de hosting subcontratado. Puesto, que tal y como dispone el RGPD, el encargado que subcontrate el servicio prestado al responsable del tratamiento está obligado a cumplimentar un contrato de acceso a datos personales, conforme a lo dispuesto en el art. 28.3 del RGPD. La entidad sancionada no había cumplimentado el contrato en el momento de prestar el servicio a sus clientes.

Teniendo en cuenta como agravantes, que la entidad sancionada es encargada de tratamiento de numerosos responsables, la sanción ascendió a 60.000€

La imposibilidad de retirar el consentimiento una vez prestado sobre el uso de cookies que no sean técnicas supone una infracción de la LSSICE.

IMPORTANTE

Encargar el tratamiento de datos a un tercero sin la formalización de un contrato de acceso a datos es una infracción grave.

LA AEPD ACLARA

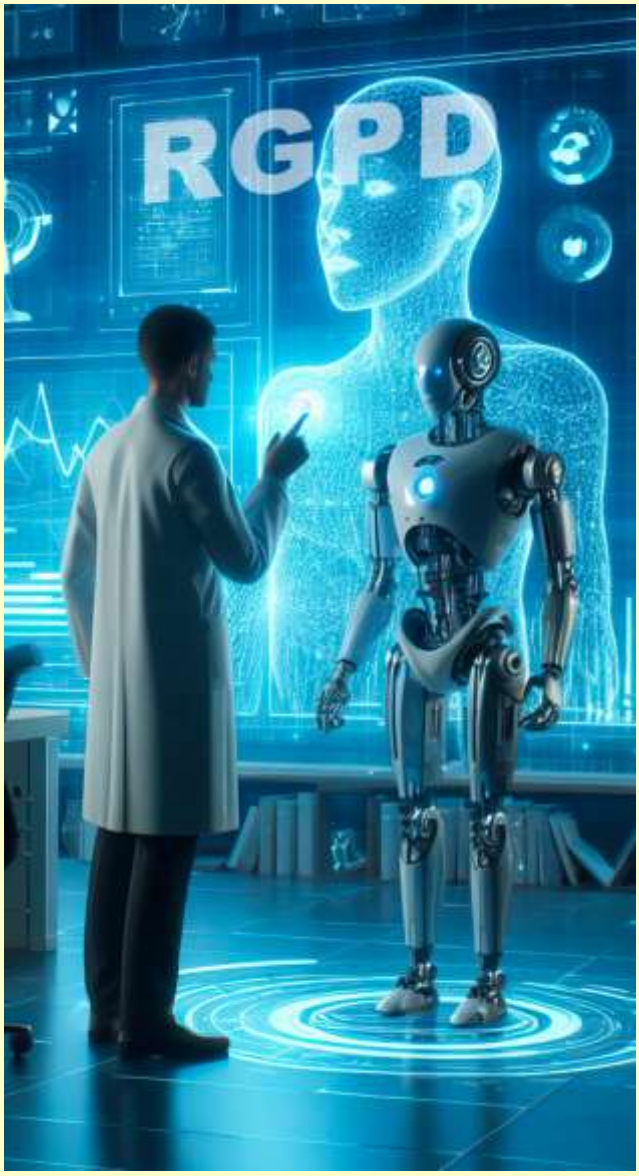
Transparencia en la Protección de Datos y la Inteligencia Artificial

En el apartado de Innovación y Tecnología de la AEPD podemos encontrar en su página web información relevante sobre los nuevos avances tecnológicos. En este sentido, en el escrito de la AEPD se hace referencia a la propuesta de Reglamento Europeo de Inteligencia Artificial (*Artificial Intelligence Ac)* en adelante *(AIA)* que ya ha sido aprobado por el Parlamento Europeo, cuyo ámbito material son los sistemas de IA.

Es importante diferenciar en este sentido, el concepto de transparencia en protección de datos y la transparencia de IA. Las principales diferencias están en el deber de informar:

- **Transparencia en Reglamento Europeo de Protección de datos (RGPD):** se aplica sobre los tratamientos de datos personales y los sujetos obligados al deber de informar que son los responsables del tratamiento. Los interesados deben recibir la información sobre el tratamiento de sus datos personales por parte del responsable.
- **Transparencia en Reglamento Europeo de Inteligencia Artificial *(AIA)*:** se aplica a los sistemas de IA y los sujetos obligados son los diseñadores, desarrolladores, proveedores y entidades que despliegan los sistemas de IA.

Al mismo tiempo, los desarrolladores están obligados a informar sobre el sistema de IA a las entidades que despliegan los sistemas de IA y a las personas físicas que se vean afectadas por ese sistema.



IMPORTANTE

La información disponible en el marco de transparencia de *AIA* ha de ser suficientemente completa para permitir a responsables y encargados cumplir con las obligaciones del RGPD.

ACTUALIDAD LOPD

Las autoridades de control de protección de datos publican unas orientaciones para tratamientos que incorporen tecnologías de seguimiento Wi-Fi

Fuente: AEPD

(7 de mayo de 2024). La Agencia Española de Protección de Datos, la Autoridad Catalana de Protección de Datos, la Autoridad Vasca de Protección de Datos y el Consejo de Transparencia y Protección de Datos de Andalucía han elaborado unas Orientaciones sobre tratamientos que incorporen tecnología de seguimiento Wi-Fi o Wi-Fi tracking en las que analizan las implicaciones de esta tecnología, identifican los principales riesgos y ofrecen una serie de recomendaciones para un uso responsable y compatible con la normativa de protección de datos.

El seguimiento Wi-Fi es una tecnología que permite **identificar y rastrear dispositivos móviles a través de las señales Wi-Fi** que estos emiten, detectando la presencia del dispositivo en una zona específica e identificando patrones de movimiento. Pueden encontrarse aplicaciones prácticas en centros comerciales, museos, centros de trabajo, áreas públicas, transportes o grandes eventos, empleándose para la estimación de aforos, el análisis de flujos de personas o la medición de tiempos de permanencia.

Las autoridades de protección de datos exponen que el uso de esta tecnología puede suponer un tratamiento de datos personales y, por tanto, deben someterse al conjunto de principios, derechos y obligaciones establecidos en el Reglamento General de Protección de Datos. Además, su uso plantea serios riesgos para la privacidad, ya que podría permitir el **seguimiento de los movimientos de las personas** sin que estas sean conscientes de ello y sin una base legal apropiada.

Por ello, las autoridades consideran que, dados los factores y elementos de riesgo inherentes, en general, se cumplen las condiciones para que antes de llevar a cabo el tratamiento sea obligatorio realizar una **Evaluación de Impacto en la Protección de Datos** (EIPD). De hecho, teniendo en cuenta los factores de riesgo, recomiendan realizarla incluso cuando el responsable del tratamiento pueda no tener clara su obligatoriedad. Además, para utilizar estas tecnologías es necesario intensificar el cumplimiento del **principio de transparencia** a través de una información clara y accesible, como paneles visibles con información, señalización pública, alertas de voz o campañas de información, entre otros.

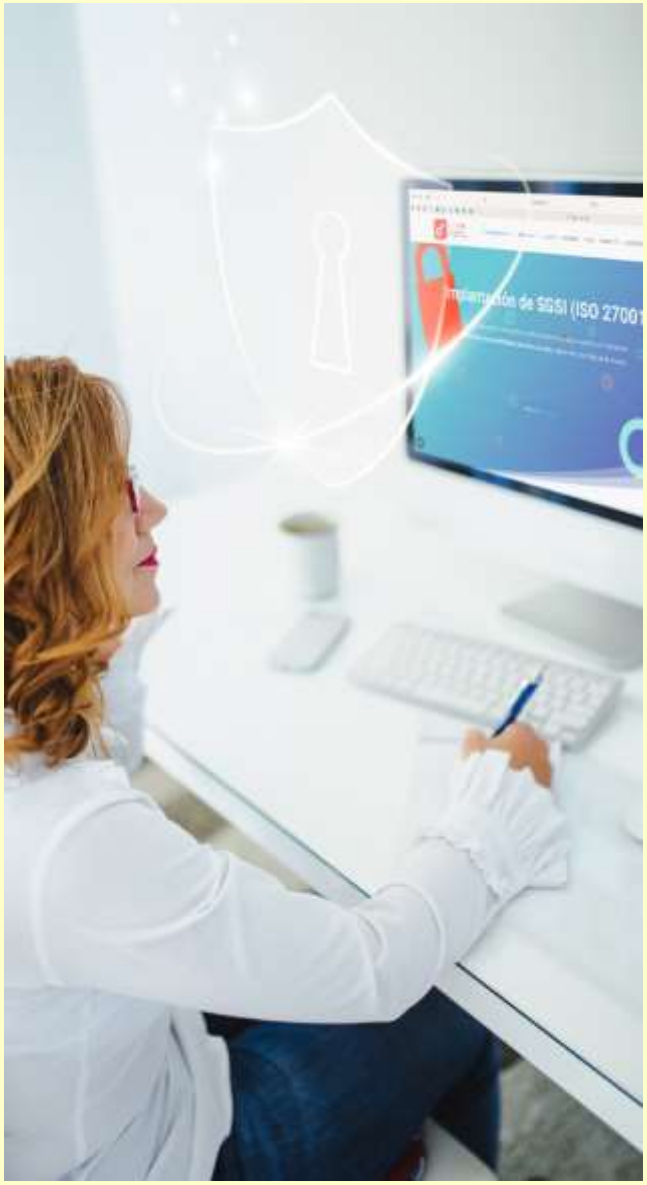
Puede ver más información en el siguiente enlace:

TECNOLOGÍAS DE SEGUIMIENTO WI-FI: orientaciones para responsables del tratamiento

EL PROFESIONAL RESPONDE

¿Cómo podemos proteger a la empresa de incidentes de ciberseguridad? (I)

La ciberseguridad es un aspecto crucial en el mundo empresarial actual. Proteger a la empresa de incidentes de ciberseguridad es una tarea que requiere una estrategia sólida y medidas preventivas efectivas. **Entre ellas, con carácter general podemos implementar las siguientes medidas de seguridad técnicas y organizativas:**



- **Concienciación y formación**: todos los empleados/as deben estar bien informados sobre las amenazas de ciberseguridad y cómo prevenirlas.
- **Actualizaciones regulares:** Mantener todos los sistemas y software actualizados con los últimos parches de seguridad para evitar accesos ilícitos.
- **Copias de seguridad**: Realizar copias de seguridad regulares de la información, en servidores propios o proveedores de copias en la nube.
- **Autenticación de dos factores**: método de seguridad que utiliza dos elementos diferentes para verificar la identidad de un usuario antes de otorgarle acceso a un sistema o servicio.

Proteger a nuestra empresa de incidentes de ciberseguridad es una tarea continua que requiere un enfoque proactivo. Hay que mantenerse informado y actualizado sobre las últimas amenazas, de esta forma se fortalecerá la defensa contra los incidentes de ciberseguridad.

IMPORTANTE

La concienciación y formación del personal laboral es una medida de seguridad organizativa que ayuda a las empresas a reforzar al eslabón más débil en la cadena de la ciberseguridad.