

EL RGPD UE 2016/679 EN APLICACIÓN

Responsabilidad proactiva y buen gobierno del dato personal en las organizaciones

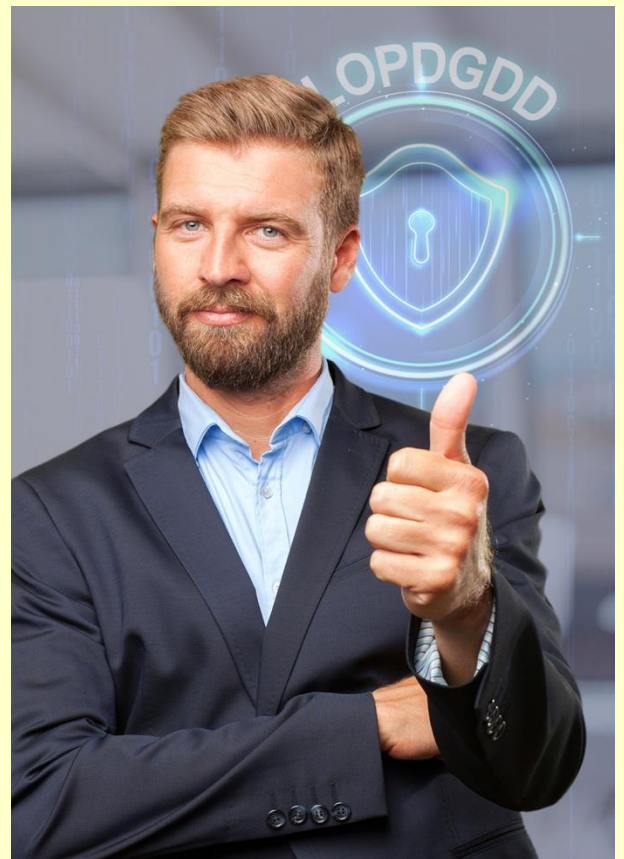
El Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), establecen un conjunto de principios generales que—como hemos visto en boletines anteriores—deben guiar cualquier tratamiento de datos personales: licitud, lealtad y transparencia; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación; integridad y confidencialidad; y, finalmente, la responsabilidad proactiva o *accountability*.

El principio de responsabilidad proactiva representa supone un cambio en la forma de afrontar la protección de datos. Ya no basta con cumplir la norma, sino que el responsable del tratamiento debe ser capaz de demostrarlo. La responsabilidad proactiva implica integrar la privacidad en todas las fases del ciclo de vida del dato: desde el diseño de procesos, medidas técnicas y organizativas adecuadas, hasta la documentación y revisión continua de dichas medidas.

La responsabilidad proactiva constituye el fundamento de una cultura de cumplimiento efectivo y verificable. Su adecuada implementación contribuye a la mitigación de riesgos legales y sancionadores.

Contenido

1. Responsabilidad proactiva y buen gobierno del dato personal en las organizaciones.
2. Una cadena de cines es sancionada con 30.000€ por falta de medidas adecuadas de seguridad y exactitud de datos
3. Los Neurodatos: el nuevo horizonte de la privacidad y la protección de datos personales (I).
4. Nota informativa sobre la baliza V16 conectada, el dispositivo que deberán llevar los vehículos desde enero de 2026.
5. Cómo deberán notificar los incidentes las entidades esenciales e importantes según la NIS2.



IMPORTANTE

La responsabilidad proactiva implica que el responsable del tratamiento debe garantizar y demostrar el cumplimiento del RGPD, integrando la protección de datos personales en todas sus acciones.

SANCIONES DE LA AEPD

Una cadena de cines es sancionada con 30.000€ por falta de medidas adecuadas de seguridad y exactitud de datos

La Agencia Española de Protección de Datos (AEPD) en su [expediente sancionador https://www.aepd.es/documento/ps-00536-2024.pdf](https://www.aepd.es/documento/ps-00536-2024.pdf) impuso una multa de 30.000 euros a una cadena de cines.

Una usuaria presentó una denuncia ante la AEPD tras comprobar que, al acceder a la aplicación móvil de una cadena de cines para comprar entradas, aparecían automáticamente datos personales de otra persona. Además, la aplicación autocompletaba el campo de la tarjeta de fidelización con un número ajeno al de la denunciante, exponiendo información de terceros sin su consentimiento.

El incidente se originó por un error técnico en la sincronización de las bases de datos de la aplicación de fidelización, que provocó el cruce de información entre usuarios registrados el mismo día en distintos cines. Los datos comprometidos eran nombre, apellidos, correo electrónico, teléfono y número de tarjeta que incorporaba el DNI del cliente.

La entidad incurrió en dos infracciones relevantes del Reglamento General de Protección de Datos: artículo 5.1.d (principio de exactitud) por mantener información inexacta que se mostraba erróneamente entre usuarios y el artículo 32 (seguridad del tratamiento): por no aplicar medidas técnicas y organizativas adecuadas para proteger la confidencialidad e integridad de los datos personales.

El responsable actuó con grave negligencia al analizar diversas incidencias sin detectar adecuadamente los riesgos que las vulneraciones suponían para los derechos y libertades de las personas afectadas.



IMPORTANTE

El número de DNI, por su capacidad de identificar de forma única a una persona, es un dato sensible cuyo uso indebido puede facilitar la suplantación de identidad y fraudes que comportan un riesgo para la privacidad.

LA AEPD ACLARA

Los Neurodatos: el nuevo horizonte de la privacidad y la protección de datos personales (I)

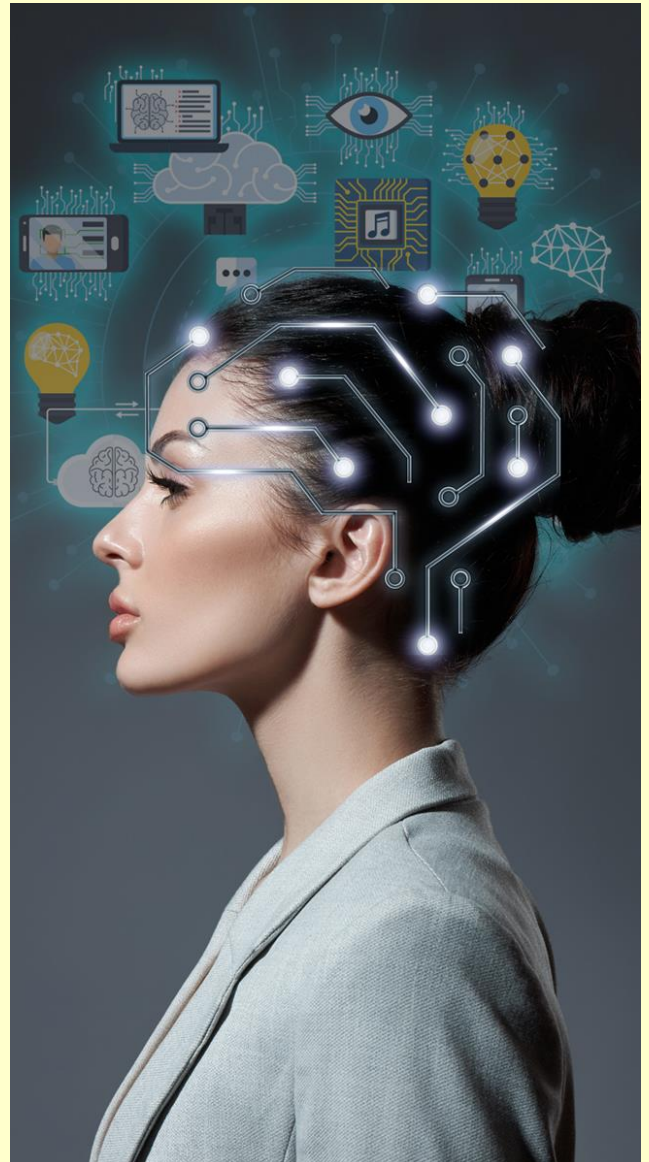
Los llamados neurodatos son información obtenida del cerebro y sistema nervioso que revela emociones, pensamientos o decisiones.

Su carácter único convierte estos datos en una categoría especialmente sensible, ya que pueden identificar de forma inequívoca a una persona y revelar aspectos íntimos de su identidad cognitiva y emocional.

El [documento conjunto de la AEPD y el EDPS](#) (Supervisor Europeo de Protección de datos) advierte que el tratamiento de neurodatos plantea riesgos inéditos para derechos como la privacidad, la integridad mental o la dignidad humana. En contextos no médicos, como la educación, el entretenimiento o el neuromarketing, el uso de estas tecnologías, implican una recolección masiva y continua de información cerebral sin un fin estrictamente justificado.

La integración de inteligencia artificial en el análisis de neurodatos amplifica los riesgos: se pueden dar sesgos discriminatorios o usos no consentidos que den lugar a graves violaciones de los derechos de las personas.

En este sentido, los expertos europeos subrayan que cualquier tratamiento de neurodatos debe someterse a una evaluación ética y jurídica rigurosa, priorizando siempre la minimización y la transparencia en este tipo de tratamientos.



IMPORTANTE

El principio de minimización obliga a tratar solo los datos personales necesarios, adecuados y pertinentes para la finalidad prevista, evitando cualquier recopilación excesiva.

ACTUALIDAD CIBERSEGURIDAD Y PRIVACIDAD

Nota informativa sobre la baliza V16 conectada, el dispositivo que deberán llevar los vehículos desde enero de 2026

Fuente: [AEPD](#)

20 de Noviembre de 2025

A partir del 1 de enero de 2026 será obligatorio que los vehículos utilicen la baliza V16 conectada para señalar averías o situaciones de emergencia en carretera. En relación con los mensajes que están circulando en diversos foros sobre este tema y con el propósito de ofrecer información a la ciudadanía, la Agencia Española de Protección de Datos expone lo siguiente:

La baliza de preseñalización de peligro V16 incorpora una luz visible y envía un aviso automático a los sistemas de tráfico cuando se activa. Esta comunicación transmite el lugar donde se encuentra el vehículo detenido y un identificador técnico del propio dispositivo. Ese identificador no está asociado a una persona o matrícula, sin que exista un registro que vincule el dispositivo con la identidad de quien lo utiliza.

La persona que adquiere la baliza no tiene que dar sus datos personales a ninguna administración al adquirirlo, por lo que la Dirección General de Tráfico (DGT) no conocería quién ha comprado el dispositivo.

Mientras no se activa, la baliza no transmite ningún dato y, en caso de ser activada ante una situación de emergencia, la información que se envía no permitiría conocer quién es la persona que conduce ni reconstruir sus desplazamientos. La baliza emite una señal mientras está encendida y deja de hacerlo al apagarse, sin generar historiales de movimientos o envío de datos de manera continua.

La norma recoge que estos dispositivos están destinados exclusivamente a la visibilización del vehículo accidentado y el envío de la ubicación de un incidente al activarse, prohibiendo expresamente que incorporen funcionalidades adicionales.

La obligatoriedad de la utilización de la baliza V16 está recogida en el [Real Decreto 159/2021](#) que regula los servicios de auxilio en las vías públicas, modificado por el [Real Decreto 1030/2022](#).

Puede ver información relacionada en el siguiente enlace:

[Real Decreto 1030/2022, de 20 de diciembre, por el que se modifica el Real Decreto 159/2021, de 16 de marzo, por el que se regulan los servicios de auxilio en las vías públicas.](#)

EL PROFESIONAL RESPONDE

Cómo deberán notificar los incidentes las entidades esenciales e importantes según la NIS2

En el marco de la Directiva NIS2 y del Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad la gestión de incidentes debe articularse conforme a un proceso estructurado y ágil:

1. Obligación de notificación temprana

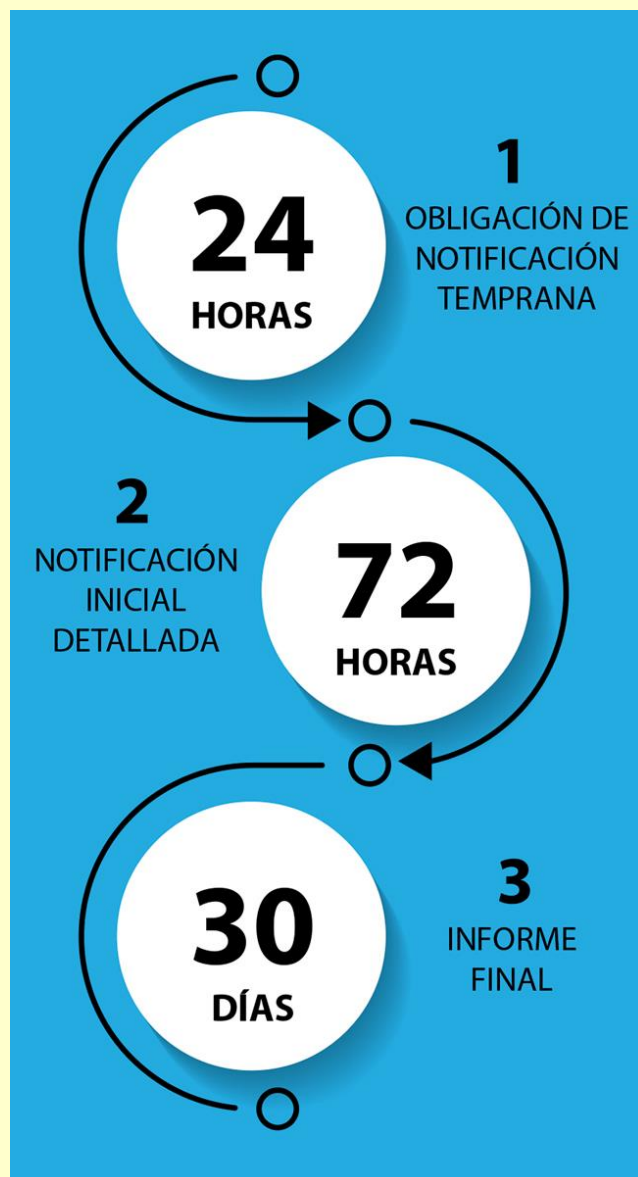
Las entidades clasificadas como “esenciales” o “importantes” deben remitir sin dilación indebida y en todo caso dentro de las 24 horas siguientes a la detección de un incidente significativo una “advertencia temprana” a la autoridad competente o al equipo *CSIRT* (Equipo de Respuesta ante Incidentes de Seguridad Informática) nacional. Se trasladará información preliminar sobre el incidente, incluso si aún no es posible determinar el alcance total del impacto.

2. Notificación inicial detallada

Posteriormente, la entidad debe remitir una notificación formal en un plazo máximo de 72 horas desde la detección, aportando un análisis inicial del incidente: naturaleza, alcance, impacto, causas conocidas, indicadores de compromiso, y medidas de contención adoptadas.

3. Informe final

Finalmente, en un plazo máximo de un mes se presentará un informe completo que incluya lecciones aprendidas, medidas correctivas adoptadas y, en caso necesario, solicitud de prórroga justificando la necesidad de ampliación hasta otro mes.



IMPORTANTE

Establecer roles como es el *CISO* clasificar incidentes, definir plazos de notificación, realizar simulacros y documentar todo el proceso garantiza cumplimiento NIS2 y respuesta eficaz ante incidentes graves.