PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

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

Boletín 09/26

EL RGPD UE 2016/679 EN APLICACIÓN

Derecho de oposición y comunicaciones comerciales

El derecho de oposición, regulado en el artículo 21 del Reglamento General Europeo de Protección de Datos (RGPD), permite al interesado solicitar que sus datos personales dejen de ser tratados en determinados supuestos. En el ámbito de la mercadotecnia directa, este derecho tiene un alcance especialmente claro.

El artículo 21.2 del RGPD reconoce que, cuando los datos personales sean tratados con fines de mercadotecnia directa, el interesado podrá oponerse en cualquier momento. A su vez, el artículo 21.3 establece que, una vez ejercitado este derecho, los datos dejarán de ser tratados para dicha finalidad.

En la práctica, la empresa no debe limitarse a retirar al interesado de una campaña concreta. Debe adoptar medidas que eviten su reincorporación posterior a nuevas acciones comerciales. Para ello puede mantener una lista interna de exclusión publicitaria, limitada a los datos imprescindibles para identificar al interesado y garantizar que no vuelva a recibir comunicaciones comerciales.

Esta exclusión debe trasladarse de forma coherente a los distintos sistemas utilizados por la organización: CRM, herramientas de email marketing, bases de datos comerciales y, cuando proceda, proveedores externos.

Contenido

1. Derecho de oposición y comunicaciones comerciales.
2. La AEPD sanciona con 680.000 € a una empresa de automoción tras una brecha de seguridad.
3. Trazabilidad y control: las claves para implantar agentes inteligentes con garantías.
4. La AEPD analiza la calidad, exactitud y minimización de datos personales en tratamientos realizados con sistemas de IA.
5. El registro de actividad en el ENS: una medida clave para detectar y acreditar incidentes.

IMPORTANTE

Las entidades deben conservar evidencias de que recibieron, y aplicaron correctamente el derecho de oposición, pudiendo demostrarlo ante cualquier reclamación o auditoría.

SANCIONES DE LA AEPD

La AEPD sanciona con 680.000 € a una empresa de automoción tras una brecha de seguridad

La Agencia Española de Protección de Datos (AEPD), en la resolución PS-00540-2025, sanciona con 680.000 euros a una empresa del sector de la automoción especializada en la compraventa de vehículos de ocasión, tras una brecha de seguridad que permitió el acceso y exfiltración de datos personales de clientes y potenciales clientes.

El incidente afectó a información identificativa y de contacto facilitada a través de formularios web, incluyendo, en determinados casos, números de DNI. La investigación puso de manifiesto deficiencias en las medidas técnicas y organizativas de seguridad, algunas de ellas previamente identificadas mediante auditorías y no corregidas de forma eficaz antes del ciberataque.

La AEPD aprecia como principales incumplimientos la vulneración del principio de integridad y confidencialidad, la insuficiencia de las medidas de seguridad y deficiencias en el deber de información, especialmente respecto de los plazos de conservación de los datos de potenciales clientes que no llegaron a formalizar una contratación. En la resolución se impusieron sanciones de 400.000, 250.000 y 30.000 euros, respectivamente, alcanzando un total de 680.000 euros.

La resolución también resulta relevante desde la perspectiva del ejercicio de derechos, al evidenciar la importancia de disponer de criterios claros sobre conservación, supresión y bloqueo de datos.

La infracción más grave derivó por no disponer de medidas de seguridad adecuadas que garanticen la confidencialidad de los datos.

IMPORTANTE

El ejercicio de derechos exige criterios claros sobre conservación, supresión y bloqueo, evitando mantener indefinidamente datos de relaciones comerciales no formalizadas.

LA AEPD ACLARA

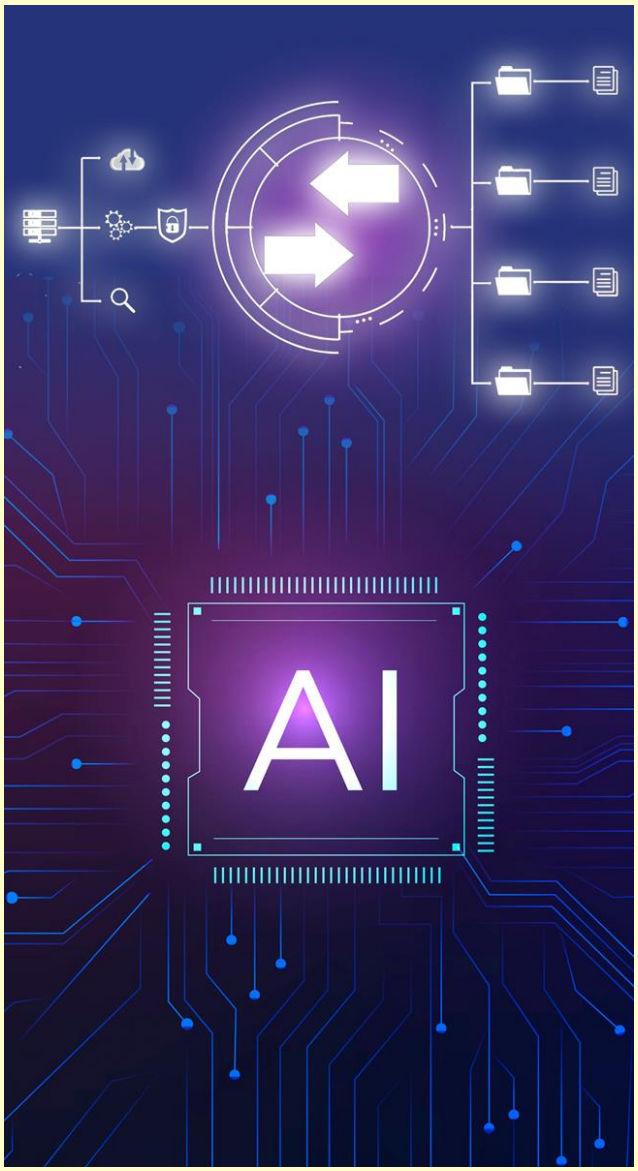
Trazabilidad y control: las claves para implantar agentes inteligentes con garantías

La AEPD destaca que la trazabilidad es uno de los pilares sobre los que debe construirse la gobernanza de la IA agéntica. La capacidad de un sistema de IA para ejecutar tareas de forma autónoma obliga a replantear cómo se documentan y supervisan sus actuaciones.

Registrar únicamente el resultado final ya no es suficiente. Las organizaciones necesitan poder reconstruir el proceso seguido por el agente: qué información utilizó, qué decisiones adoptó, qué herramientas consultó y qué acciones ejecutó. Esta capacidad resulta esencial para investigar incidentes, justificar actuaciones y demostrar el cumplimiento del principio de responsabilidad proactiva del RGPD.

La trazabilidad también facilita el cumplimiento del AI Act, que refuerza la importancia del registro de eventos, la documentación técnica y la supervisión durante todo el ciclo de vida de los sistemas de IA.

Además de ser una medida de control, disponer de registros adecuados permite mejorar el propio funcionamiento del sistema, detectar desviaciones y corregir comportamientos inesperados antes de que produzcan impactos relevantes sobre la organización o sobre los derechos de las personas.



IMPORTANTE

Las entidades deben implantar registros trazables, integrar la supervisión de IA en cumplimiento, y revisarlos periódicamente para detectar incidencias y corregirlas.

ACTUALIDAD CIBERSEGURIDAD Y PRIVACIDAD

La AEPD analiza la calidad, exactitud y minimización de datos personales en tratamientos realizados con sistemas de IA

Fuente: AEPD

(21 de julio de 2026). La Agencia Española de Protección de Datos (AEPD) ha publicado una nota técnica en la que analiza cómo se proyectan los principios de exactitud y minimización del RGPD en tratamientos de datos personales que incorporan sistemas de inteligencia artificial. Se trata de uno de los primeros trabajos en el mundo que aborda de forma sistemática esta cuestión, y tiene como objetivo de ofrecer criterios a responsables de tratamiento, encargados y delegados de protección de datos.

El documento parte de que los requisitos de calidad de los datos y el principio de exactitud establecido en el Reglamento General de Protección de Datos (RGPD) no pueden entenderse en términos absolutos, sino en relación con la finalidad del tratamiento. En este sentido, la AEPD aclara que **el principio de exactitud recogido en el RGPD no exige que los datos sean siempre plenamente veraces o estén completamente actualizados, sino que sean adecuados para cumplir el objetivo** del tratamiento en el que se utilizan y ello se garantice cuando resulte relevante para las personas afectadas.

Esta interpretación supone **una evolución respecto a enfoques más restrictivos** que vinculaban la exactitud exclusivamente a la veracidad de los datos. La Agencia subraya que una exigencia excesiva en este sentido podría entrar en conflicto con el principio de minimización o generar cargas desproporcionadas, especialmente en el desarrollo y uso de sistemas de inteligencia artificial.

La nota técnica explica que la calidad de los datos debe analizarse no solo en relación con cada dato individual, sino especialmente **respecto al conjunto de datos utilizado para el desarrollo de sistemas de IA**, lo que resulta especialmente relevante en el caso de modelos de aprendizaje automático. En estos sistemas, la representatividad, la ausencia de sesgos o la relevancia de los datos pueden ser determinantes para el resultado, incluso por encima de la exactitud individual de cada registro.

Asimismo, se pone de relieve que el requisito de calidad de los datos no se limita a los datos de entrada, sino que debe proyectarse sobre todo el tratamiento, incluyendo los resultados generados por sistemas de inteligencia artificial, como inferencias, predicciones o decisiones, que **no deben generar representaciones incorrectas o desproporcionadas de las personas afectadas**. Ello implica evaluar la idoneidad del tratamiento en su conjunto, teniendo en cuenta el diseño, las operaciones realizadas y las salvaguardas incorporadas. (…)

Puede ver información relacionada en el siguiente enlace:

Exactitud, idoneidad y calidad de los datos en tratamiento de datos personales con Inteligencia Artificial.

EL PROFESIONAL RESPONDE

El registro de actividad en el ENS: una medida clave para detectar y acreditar incidentes

La continuidad de la actividad constituye un requisito esencial del Esquema Nacional de Seguridad (ENS). El artículo 26 del Real Decreto 311/2022 establece que los sistemas deberán disponer de copias de seguridad y de los mecanismos necesarios para garantizar la continuidad de las operaciones cuando se pierdan los medios habituales.

En este caso, la resiliencia operativa exige ir más allá de disponer de copias. **El Anexo II del ENS, dentro de las medidas de continuidad del servicio, contempla el análisis de impacto destinado a identificar los requisitos de disponibilidad y los elementos críticos para prestar cada servicio. Esta medida resulta aplicable cuando la dimensión de disponibilidad alcanza nivel medio o alto.**

Para disponibilidad de nivel alto, el ENS exige además un plan de continuidad, que debe determinar funciones, responsabilidades, actividades y mecanismos para activar medios alternativos. También contempla pruebas periódicas para detectar y corregir deficiencias del plan.

Por tanto, una organización debe conocer qué servicios son críticos, qué recursos necesita para mantenerlos y quién debe actuar cuando se produce una interrupción.

la resiliencia no consiste únicamente en recuperar información, sino en disponer de medidas previamente definidas y probadas que permitan mantener los servicios esenciales.

IMPORTANTE

El ENS exige identificar servicios críticos, establecer medidas de continuidad y comprobar periódicamente su eficacia ante posibles interrupciones.