

EL RGPD UE 2016/679 EN APLICACIÓN

Principio de minimización de datos, claves para proteger los datos personales

Hoy en día, los datos personales son activos muy importantes para la entidad. El cumplimiento del principio de minimización de datos es fundamental para la privacidad. El RGPD indica en el artículo 5.1.c) que solo deben recogerse datos adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

El responsable del tratamiento debe llevar a cabo las actuaciones necesarias para conocer qué información es estrictamente necesaria. Desde el punto de vista práctico tiene que revisar los formularios, procesos y sistemas para eliminar, en la medida de lo posible, la recogida excesiva de datos personales. Por ejemplo, evitar datos sensibles salvo que sean imprescindibles, o usar listas cerradas en lugar de campos abiertos.

Las medidas técnicas y organizativas resultan imprescindibles: implementar políticas de privacidad por diseño, aplicar técnicas de anonimización o seudonimización, y establecer controles de acceso según roles. Además, el responsable del tratamiento debe mantener un registro de actividades de tratamiento en el que identifique la finalidad y necesidad de los datos personales tratados.

Contenido

- 1.Principio de minimización de datos, claves para proteger los datos personales.
- 2.Tratamiento de datos de menores sin base legal ni garantías de seguridad: resolución sancionadora de 10.000 euros en el sector educativo.
- 3.Privacidad por defecto: fundamentos y obligaciones (I).
- 4.La AEPD presenta su Plan Estratégico 2025-2030: Innovación responsable y defensa de la dignidad en la era digital.
- 5.Cómo impacta la Directiva NIS2 en las empresas esenciales y estratégicas.



IMPORTANTE

La LOPDGDD califica como infracción muy grave tratar datos personales sin respetar principios como el principio de minimización, con sanciones significativas.

SANCIONES DE LA AEPD

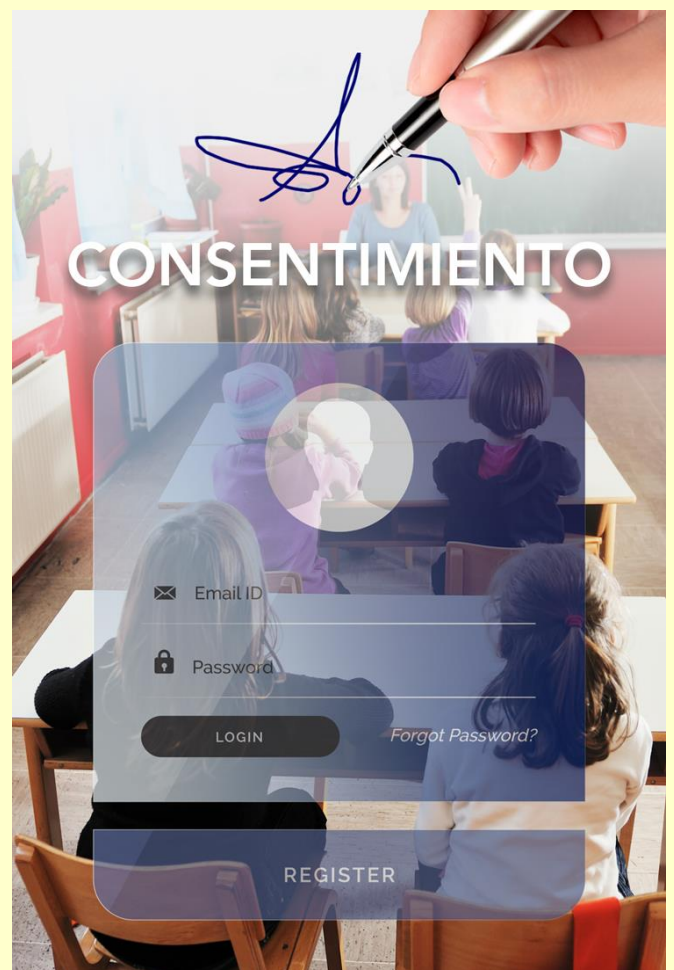
Tratamiento de datos de menores sin base legal ni garantías de seguridad: resolución sancionadora de 10.000 euros en el sector educativo

La Agencia Española de Protección de Datos (AEPD) en el [expediente sancionador https://www.aepd.es/documento/ps-00502-2023.pdf](https://www.aepd.es/documento/ps-00502-2023.pdf) impuso una multa de 10.000 euros a un centro educativo privado por diversas infracciones del 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).

La reclamación fue presentada por el padre de una alumna menor de edad, quien denunció que el centro había creado una cuenta de correo electrónico institucional y un perfil en una plataforma educativa sin haber recabado el consentimiento de los tutores legales, tal como exige la normativa en el caso de menores de 14 años. Se produjo además un incidente de suplantación de identidad, por una seguridad deficiente: la contraseña que se utilizó no cumplía con las medidas de seguridad adecuadas.

La AEPD determinó las siguientes infracciones: tratamiento de datos sin una base legítima; falta de información sobre el Delegado de Protección de Datos en la política de privacidad y aplicación de medidas de seguridad inadecuadas.

No aplicar medidas técnicas y organizativas adecuadas al riesgo del tratamiento, conforme al artículo 32 del RGPD, constituye una infracción grave según el artículo 73.d de la LOPDGDD.



IMPORTANTE

Tratar datos personales sin una base jurídica válida conforme al artículo 6 del RGPD constituye una infracción grave según la LOPDGDD.

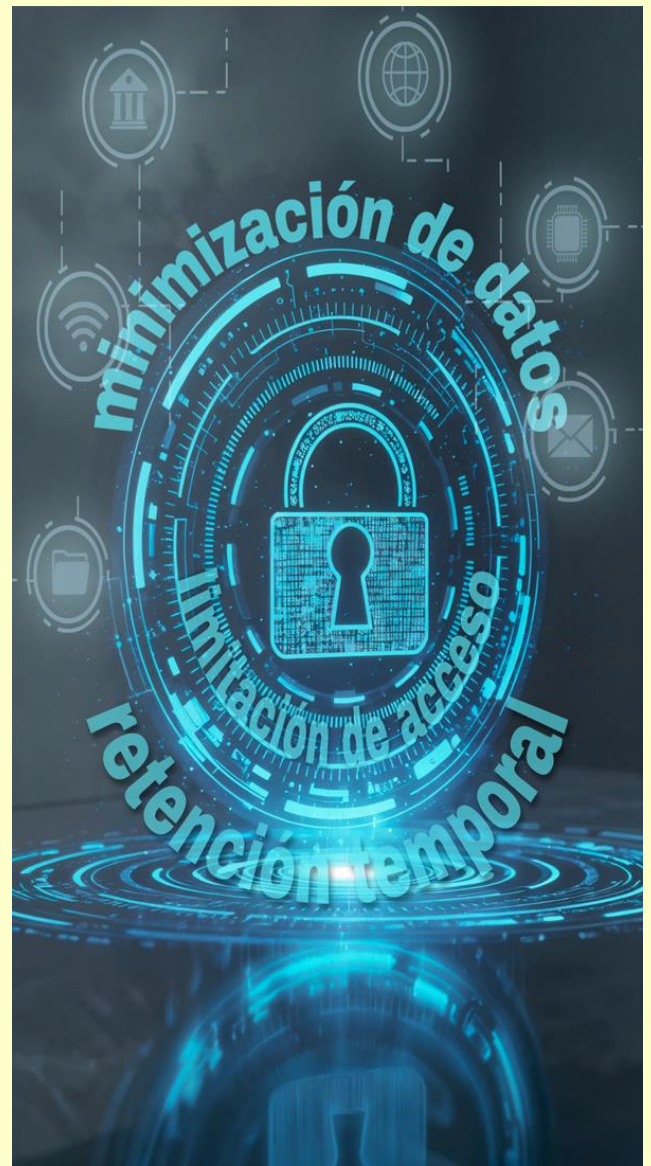
LA AEPD ACLARA

Privacidad por defecto: fundamentos y obligaciones (I)

La protección de datos por defecto es un principio esencial del Reglamento General de Protección de Datos (RGPD), recogido en su artículo 25. La Agencia Española de Protección de Datos (AEPD) ha elaborado una [guía específica](#) para facilitar su comprensión e implementación por parte de responsables y encargados del tratamiento.

Este principio obliga a garantizar que, por defecto, solo se traten los datos personales necesarios para cada finalidad específica del tratamiento. En otras palabras, el sistema debe estar configurado desde el inicio para aplicar la minimización de datos, limitación de acceso, y una conservación de los datos durante el tiempo mínimo que se haya establecido en función de la finalidad del tratamiento.

La Protección de Datos por Defecto se basa en tres estrategias: optimizar el tratamiento minimizando datos, conservación y accesos; configurar los sistemas para que el usuario controle los datos tratados; y restringir, por defecto, la recogida, tratamiento y accesibilidad, garantizando siempre la máxima privacidad posible. Se requiere, además, de una evaluación previa y la configuración de los sistemas debe responder a criterios de proporcionalidad y necesidad.



IMPORTANTE

La obligación afecta a la cantidad de datos recogidos, su tratamiento, conservación y acceso, evitando accesos indiscriminados por defecto.

ACTUALIDAD LOPD

La AEPD presenta su Plan Estratégico 2025–2030: Innovación responsable y defensa de la dignidad en la era digital



Fuente: [AEPD](#)

(3 de julio de 2025). La Agencia Española de Protección de Datos (AEPD) ha presentado hoy su [Plan Estratégico 2025–2030](#), un documento que establece las líneas clave de actuación de la autoridad para los próximos cinco años. Bajo el título ‘Innovación responsable y defensa de la dignidad en la era digital’, la Agencia reafirma su compromiso con una protección de datos proactiva, centrada en las personas y adaptada a los retos tecnológicos emergentes.

El Plan Estratégico 2025–2030 tiene como objetivo consolidar a la AEPD como una autoridad **abierta, eficaz y con capacidad de anticipación** ante los desafíos del entorno digital. Para ello, ha definido **ocho principios rectores** que estructuran sus actuaciones: Independencia, Innovación y adaptabilidad, Internacionalización e influencia, Cooperación, Proactividad y prevención, Excelencia y calidad técnica, Defensa del interés general y Agencia abierta y cercana. Con este marco, las actuaciones se estructuran en **siete grandes ejes que aglutinan 45 objetivos estratégicos** dirigidos a fomentar la prevención, la cooperación institucional, el acompañamiento normativo, el liderazgo internacional, la mejora continua y el refuerzo de la cultura de privacidad.

Entre las prioridades estratégicas destacan la supervisión proactiva de tecnologías disruptivas como la inteligencia artificial (IA) y las neurotecnologías, la promoción de una innovación tecnológica con garantías, la creación del Laboratorio de Privacidad, el apoyo a pymes y administraciones públicas en el cumplimiento normativo, el refuerzo del trabajo que realizan los delegados de protección de datos y los profesionales de la privacidad, y el impulso de alianzas con autoridades y entidades clave del ámbito público, privado, académico y del tercer sector.

Asimismo, el Plan contempla la evolución de la Agencia hacia una organización capaz de integrar con garantías herramientas basadas en IA en sus procesos internos, de forma que pueda servir como modelo a otros organismos públicos, y una apuesta firme por la transparencia y la rendición de cuentas. El documento se publicará en los próximos días en todas las lenguas cooficiales y en inglés.

Puede ver información relacionada en el siguiente enlace:

[Plan estratégico 2025-2030](#)

EL PROFESIONAL RESPONDE

Cómo impacta la Directiva NIS2 en las empresas esenciales y estratégicas

La Directiva NIS2 marca un antes y un después en la forma en que las organizaciones, tanto públicas como privadas, deben abordar su seguridad digital, se requiere una estrategia real, integrada y demostrable en materia de ciberseguridad.

En su anexo I, la norma enumera sectores considerados críticos, como energía, transporte, banca, salud, infraestructuras digitales o administraciones públicas. Las entidades que operan en estos ámbitos deben cumplir obligaciones reforzadas: planes de continuidad, auditorías periódicas(...). Este cumplimiento no es voluntario ni declarativo: estará sujeto a supervisión activa por parte de autoridades nacionales.

El anexo II incluye sectores importantes, como alimentación, servicios postales, industria farmacéutica, producción tecnológica o determinados servicios online. Aunque las obligaciones de supervisión son algo más flexibles, estas organizaciones también deben contar con medidas preventivas robustas, capacidad de detección y planes de respuesta.

En este sentido, muchas empresas deben considerar el impacto real que tiene el cumplimiento de la Directiva NIS2. La ciberseguridad en estas entidades de los sectores considerados como críticos y sectores importantes debe considerarse como un eje estratégico del negocio.



IMPORTANTE

Ya no es suficiente contar con políticas o herramientas técnicas; ahora se exige demostrar capacidad operativa real y compromiso directo de la dirección.