

EL RGPD UE 2016/679 EN APLICACIÓN

Ejercicio de derechos: obligaciones, plazos y riesgos para el responsable

En el actual entorno digital, donde el dato se ha convertido en un activo estratégico, el ejercicio de derechos en materia de protección de datos no puede abordarse como un mero trámite administrativo. Desde la experiencia práctica, atender correctamente estos derechos es una prueba real del nivel de madurez de una organización en cumplimiento normativo.

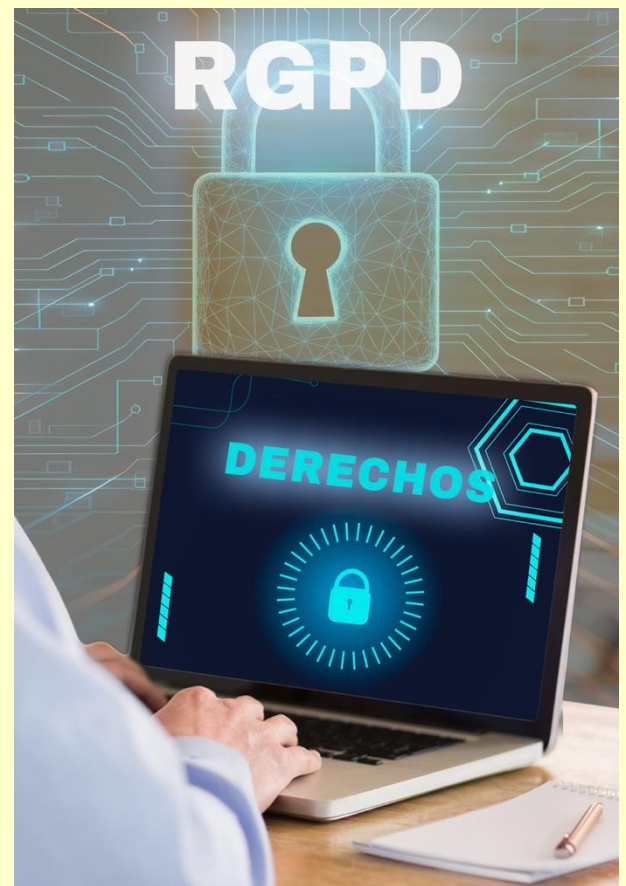
El RGPD reconoce a los interesados derechos como acceso, rectificación, supresión, oposición, limitación y portabilidad. Para el responsable del tratamiento, esto implica una obligación clara: establecer procedimientos eficaces que permitan gestionar estas solicitudes de forma ágil, segura y trazable. No se trata solo de responder, sino de hacerlo correctamente.

Desde una visión práctica, el RGPD exige responder a los derechos en un mes, sin demoras injustificadas.

Puede ampliarse hasta dos meses más, pero solo si se justifica y se comunica a tiempo. Si no se atiende la solicitud, hay que responder igualmente y motivar la decisión. También debe informarse del derecho a reclamar ante la autoridad de control. Aquí es donde se mide el cumplimiento real: en tener procedimiento, control y capacidad de acreditarlo.

Contenido

1. Ejercicio de derechos: obligaciones, plazos y riesgos para el responsable.
2. Multa de 10.000 € por tratamiento excesivo de datos en la verificación de identidad de un usuario.
3. Tratamientos que requieren especial análisis en una EIPD: claves prácticas(I).
4. Las Autoridades de Protección de Datos suscriben una declaración conjunta para reforzar la colaboración y afrontar los retos digitales en el décimo aniversario del RGPD.
5. ENS y sector privado: adaptación y oportunidades en la gestión de la seguridad de la información.



IMPORTANTE

Si no se atiende la solicitud, es imprescindible responder de forma motivada e informar al afectado del derecho a reclamar ante la autoridad de control.

SANCIONES DE LA AEPD

Multa de 10.000 € por tratamiento excesivo de datos en la verificación de identidad de un usuario

La Agencia Española de Protección de Datos, en su resolución [PS-00476-2024](#), sanciona a una entidad del sector financiero, dedicada a la concesión de préstamos online a consumidores, por un tratamiento excesivo de datos personales.

La reclamación ante la AEPD tiene su origen en una relación contractual de préstamo entre el reclamante y la entidad reclamada. Tras abonar íntegramente la deuda y solicitar la cancelación, el interesado fue requerido para remitir una fotografía sosteniendo su DNI como condición necesaria para tramitar dicha solicitud.

De la investigación se constata que la entidad reclamada impuso este requisito con la finalidad de verificar la identidad del cliente. Sin embargo, la AEPD determina que dicha práctica no se encuentra amparada por la normativa de prevención del blanqueo de capitales y que existen medios alternativos menos intrusivos, como la firma electrónica o mecanismos de verificación ya disponibles.

La infracción principal consiste en la vulneración del principio de minimización de datos (art. 5.1.c RGPD), al solicitar información excesiva y no necesaria. Asimismo, se aprecia un uso indebido de la normativa sectorial como justificación y un tratamiento desproporcionado que incrementa riesgos para el interesado, como la suplantación de identidad.

Se imponen medidas alternativas menos invasivas como sistemas de verificación ya existentes en la entidad y/o firma electrónica.



IMPORTANTE

El pago de la sanción no elimina la obligación de corregir la infracción; incumplir las medidas impuestas puede implicar nuevas sanciones por parte de la AEPD.

LA AEPD ACLARA

Tratamientos que requieren especial análisis en una EIPD: claves prácticas(I)

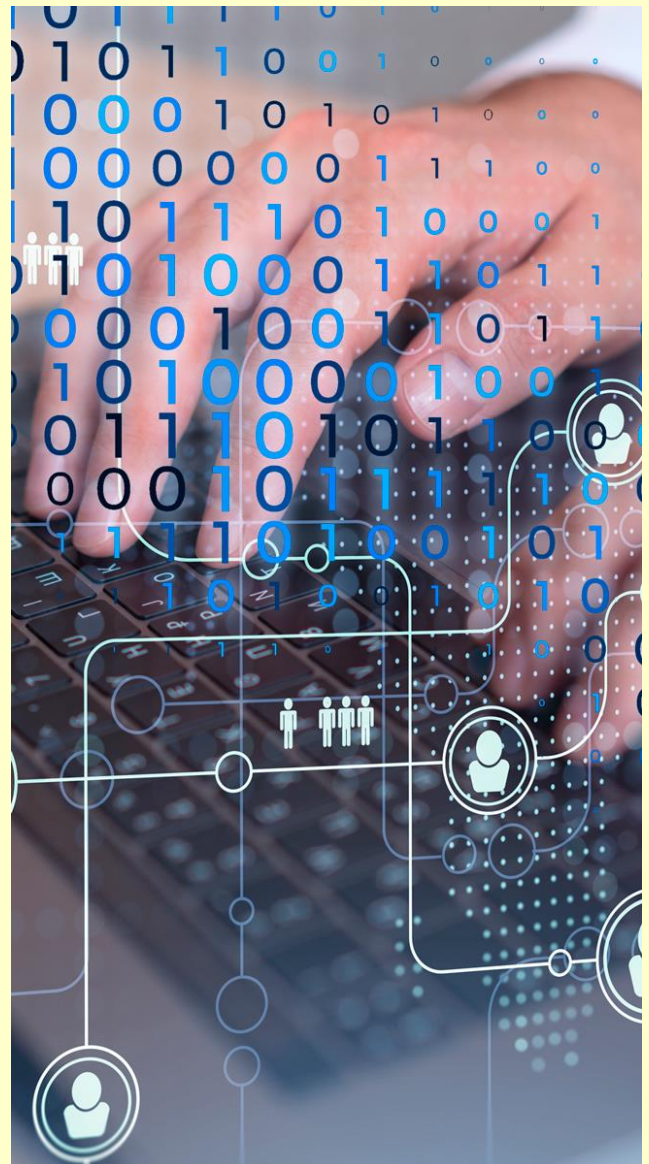
Desde la experiencia en gestión de cumplimiento, hay determinados tratamientos que, por su naturaleza, exigen una especial atención y, en muchos casos, la realización de una [Evaluación de Impacto](#).

En primer lugar, encontramos los tratamientos que implican perfilado o valoración de personas. Por ejemplo, una empresa que analiza el rendimiento laboral, hábitos digitales y comportamiento de sus empleados para tomar decisiones internas está construyendo perfiles que pueden afectar significativamente a los interesados.

En segundo lugar, destacan los tratamientos con decisiones automatizadas. Un caso habitual es el uso de algoritmos para aprobar o denegar créditos, donde una decisión automatizada puede limitar el acceso a un servicio esencial sin intervención humana directa.

También son especialmente sensibles los tratamientos que implican monitorización sistemática. Pensemos en aplicaciones móviles que rastrean la ubicación del usuario de forma continua o en sistemas de videovigilancia en espacios públicos con reconocimiento de patrones.

Por último, requieren un análisis reforzado los tratamientos de categorías especiales de datos o información sensible, como historiales médicos, datos biométricos o información sobre solvencia económica, por ejemplo, en procesos de *scoring* financiero.



IMPORTANTE

Estos tratamientos incrementan el riesgo para los derechos de las personas, lo que exige una evaluación rigurosa previa.

ACTUALIDAD CIBERSEGURIDAD Y PRIVACIDAD

Las Autoridades de Protección de Datos suscriben una declaración conjunta para reforzar la colaboración y afrontar los retos digitales en el décimo aniversario del RGPD

Fuente: [AEPD](#)

(24 de abril de 2026). Las autoridades de protección de datos han suscrito una declaración institucional en la que, por primera vez, adoptan un compromiso conjunto que **refuerza la cooperación para hacer frente a los retos relacionados con la transformación digital**, la creciente economía del dato y el uso intensivo de tecnologías emergentes, incluidas las nuevas formas de tratamiento masivo de información personal.

La [‘Declaración institucional sobre el fortalecimiento de la cultura de la privacidad y la protección de datos personales’](#) está suscrita por la **Agencia Española de Protección de Datos (AEPD)**, la **Autoridad Catalana de Protección de Datos (APDCAT)**, la **Autoridad Vasca de Protección de Datos (AVPD)**, el **Consejo de Transparencia y Protección de Datos de Andalucía (CTPDA)** y la **Dirección de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial (CGPJ)**. El texto se ha presentado durante la celebración de la jornada ‘10º aniversario del RGPD (2016-2026): Una década de retos y desafíos’.

Las autoridades parten del reconocimiento al Reglamento General de Protección de Datos (RGPD) como referente normativo global para la protección de un derecho fundamental vinculado a la dignidad de la persona, al libre desarrollo de la personalidad y al funcionamiento de una sociedad democrática. Por otro lado, subrayan que la privacidad es también un elemento clave para **generar confianza en los entornos digitales**, condición necesaria para el desarrollo de una economía del dato legítima y sostenible.

La declaración pública aborda expresamente la cooperación y colaboración entre autoridades para **mejorar la eficiencia y avanzar hacia enfoques comunes** orientados a la promoción de una cultura de la privacidad, la prevención de riesgos y el fortalecimiento de la confianza de la ciudadanía, teniendo en cuenta la creciente complejidad de los tratamientos de datos personales, la aceleración de la innovación tecnológica y su impacto transversal en la sociedad.(...)

El texto también reconoce el papel estratégico de las **personas delegadas de protección de datos y profesionales de la privacidad**. Estas figuras son consideradas esenciales para garantizar la aplicación efectiva del RGPD en las organizaciones, y por ello se comprometen a reforzar su posición impulsando redes de colaboración y espacios de intercambio de conocimiento.

Puede ver información relacionada en el siguiente enlace:

[Declaración institucional sobre el fortalecimiento de la cultura de la privacidad y la protección de datos personales.](#)

EL PROFESIONAL RESPONDE

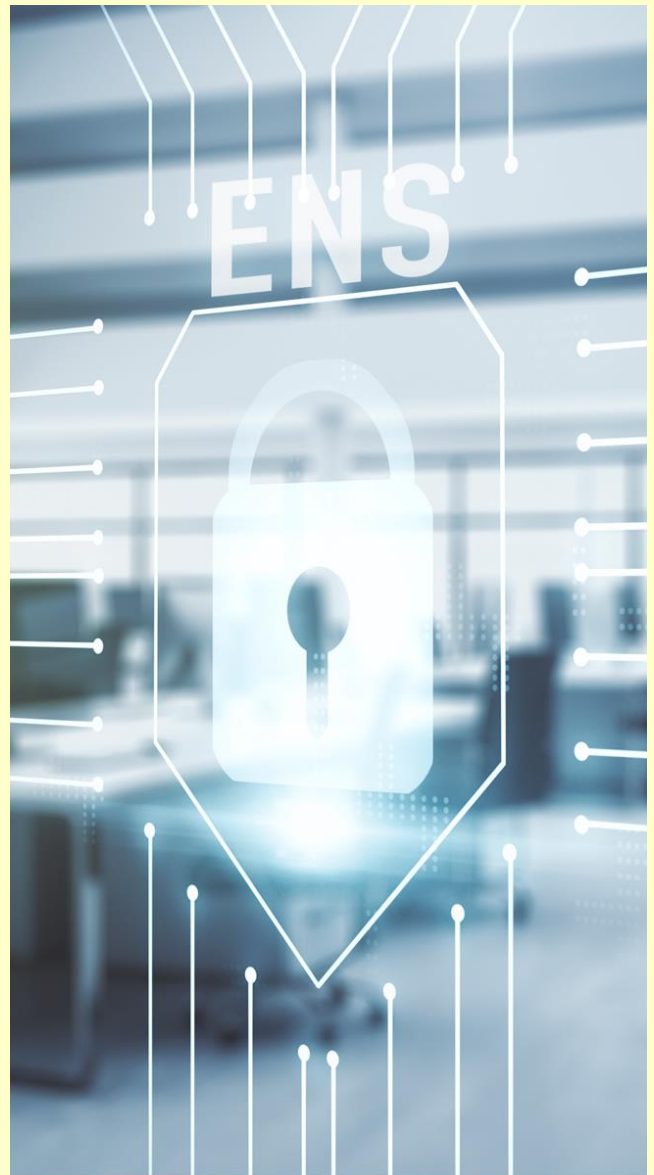
ENS y sector privado: adaptación y oportunidades en la gestión de la seguridad de la información

La aplicación del Esquema Nacional de Seguridad en el sector privado ha dejado de ser una cuestión residual para convertirse en un elemento relevante dentro de la estrategia de ciberseguridad de muchas organizaciones. Aunque su origen está vinculado al sector público, cada vez es más frecuente que empresas privadas deban alinearse con el ENS, especialmente cuando prestan servicios a Administraciones Públicas o forman parte de cadenas de suministro críticas.

Este escenario obliga a las organizaciones a adoptar un enfoque estructurado de la seguridad de la información, basado en la identificación de riesgos, la categorización de sistemas y la implantación de medidas proporcionales. No se trata solo de cumplir con un marco normativo, sino de integrar controles efectivos que aborden aspectos como el control de accesos, la gestión de incidentes, la protección de activos o la continuidad del servicio.

Uno de los principales retos para el sector privado es adaptar sus estructuras internas a los requisitos del ENS, lo que implica definir responsabilidades claras, formalizar políticas de seguridad y garantizar la trazabilidad de las actuaciones. Este proceso requiere, además, una coordinación real entre áreas técnicas y de cumplimiento.

Desde una perspectiva operativa, las entidades reducen su exposición a incidentes y mejoran su capacidad de respuesta ante amenazas cada vez más sofisticadas.



IMPORTANTE

el ENS exige a empresas privadas adaptarse cuando colaboran con Administraciones Públicas o participan en servicios esenciales.