PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

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

Boletín 08/26

EL RGPD UE 2016/679 EN APLICACIÓN

Plazos de conservación y excepciones: los retos del derecho de supresión (III)

El informe del EDPB identifica tres áreas especialmente problemáticas: los plazos de conservación, las copias de seguridad y la aplicación de las excepciones previstas en el artículo 17 del RGPD.

Uno de los problemas más frecuentes es la falta de criterios claros para determinar cuánto tiempo deben conservarse los datos. La ausencia de políticas de conservación bien definidas dificulta justificar por qué determinada información sigue almacenada o cuándo debe eliminarse definitivamente.

A ello se suma la complejidad técnica de las copias de seguridad. Muchas organizaciones encuentran dificultades para garantizar que los datos suprimidos desaparezcan también de los sistemas de respaldo, especialmente cuando estos han sido diseñados con finalidades de recuperación ante desastres y continuidad de negocio.

Las excepciones previstas como la conservación por obligación legal, la defensa de reclamaciones o determinados intereses públicos requieren un análisis jurídico riguroso y adecuadamente documentado.

Una gestión eficaz del derecho de supresión exige combinar criterios jurídicos sólidos con mecanismos técnicos capaces de garantizar una eliminación efectiva y trazable de la información.

Contenido

1. Plazos de conservación y excepciones: los retos del derecho de supresión (III).
2. Sancionado un hospital con 1,2 millones de euros por la supresión indebida de datos de salud.
3. Supervisión humana efectiva: la exigencia clave de la nueva IA (II).
4. La AEPD analiza la calidad, exactitud y minimización de datos personales en tratamientos realizados con sistemas de IA.
5. ENS y gestión de incidentes: anticiparse, reaccionar y minimizar el impacto.

IMPORTANTE

El derecho de supresión evidencia que muchas organizaciones tienen dificultades internas para localizar, gestionar y eliminar correctamente los datos personales.

SANCIONES DE LA AEPD

Sancionado un hospital con 1,2 millones de euros por la supresión indebida de datos de salud

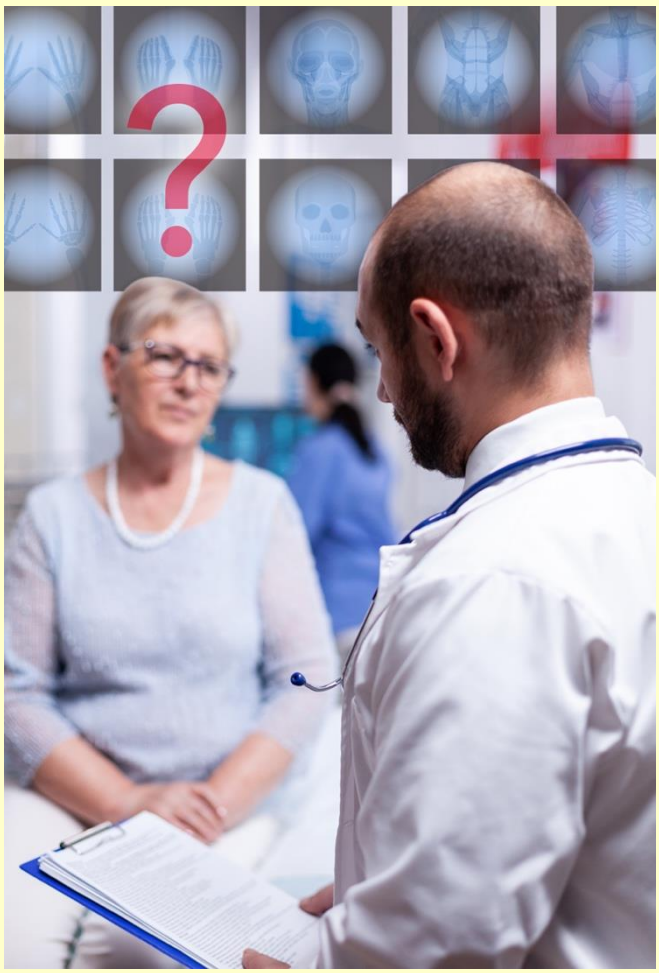
La Agencia Española de Protección de Datos, en la resolución PS-00288-2024, sanciona con 1,2 millones de euros a un hospital por vulnerar el Reglamento General de Protección de Datos, en relación con la eliminación de documentación clínica aportada por un paciente y la falta de medidas adecuadas para garantizar su conservación, custodia y correcta gestión.

La reclamación tiene su origen en la pérdida de un CD que un paciente entregó al hospital en su cita médica. El soporte contenía resonancias magnéticas de 2018, 2019 y 2020 y fue aportado para comparar dichas pruebas con una nueva resonancia. Cuando el paciente acudió meses después a recuperarlo, el hospital le comunicó que las imágenes ya no estaban disponibles, justificándolo en su política interna de archivo.

La Agencia consideró que su destrucción constituía un tratamiento de datos personales relativos a la salud y que el centro no podía eliminar libremente esa documentación mientras existiera un deber legal de conservación.

Se imponen las siguientes multas:100.000 euros al no existir una excepción que legitimara la supresión de datos de salud; 100.000 euros al no acreditarse una base jurídica para dicha eliminación y se sanciona con 1.000.000 de euros la vulneración del artículo 25 RGPD, al detectar una deficiencia en los procedimientos de conservación, custodia y devolución de documentación.

La infracción más grave derivó por no disponer de procedimientos adecuados para conservar, custodiar y devolver correctamente la documentación clínica aportada.



IMPORTANTE

La eliminación de datos personales también exige control: suprimir información sin analizar previamente los plazos legales de conservación puede constituir una infracción del RGPD.

LA AEPD ACLARA

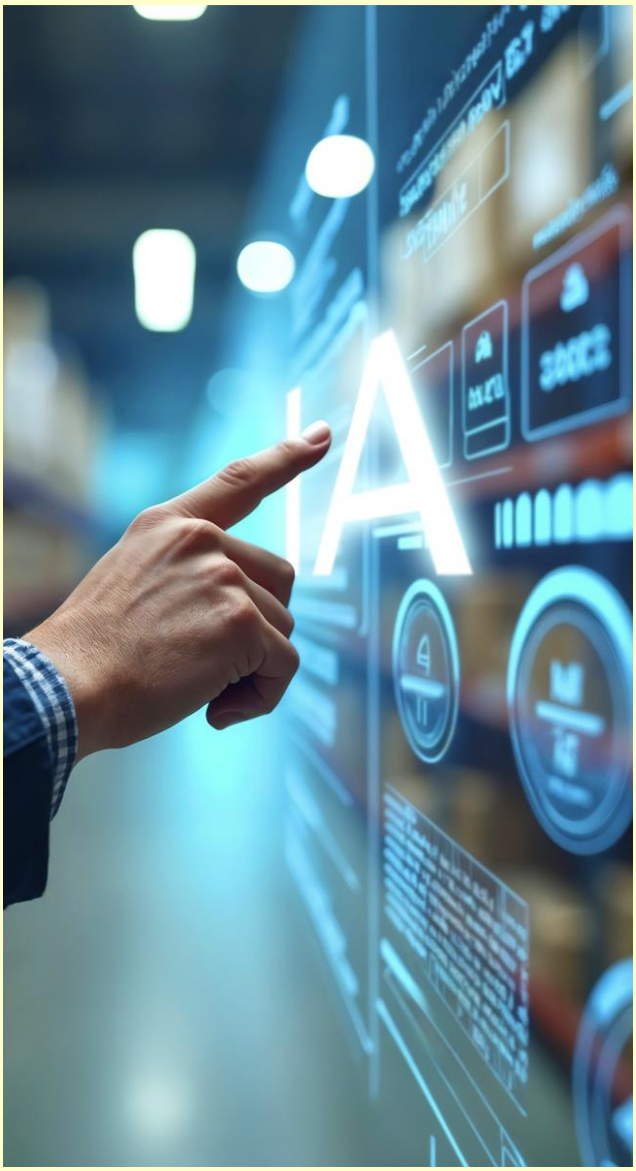
Supervisión humana efectiva: la exigencia clave de la nueva IA (II)

Uno de los mensajes más relevantes de las orientaciones de la AEPD es que la supervisión humana efectiva constituye un elemento esencial en el uso de la IA agéntica. No basta con que exista una persona responsable del sistema; esa supervisión debe permitir comprender, intervenir y, cuando sea necesario, detener las actuaciones del agente.

En la práctica, muchos sistemas de IA se utilizan para automatizar tareas repetitivas bajo un control relativamente sencillo. Sin embargo, cuando un agente es capaz de planificar acciones, utilizar herramientas externas o tomar decisiones encadenadas, la supervisión deja de ser una simple revisión final y pasa a convertirse en un mecanismo continuo de gobernanza.

Este enfoque coincide con el Reglamento de IA que exige supervisión humana para determinados sistemas de alto riesgo, y con el principio de responsabilidad proactiva del RGPD, que obliga a demostrar que el tratamiento de datos se realiza con garantías suficientes.

¿Qué debe hacer una organización? Definir qué decisiones puede adoptar el agente de forma autónoma y cuáles requieren validación humana. Establecer procedimientos que permitan detener o corregir las actuaciones y formar a los responsables de supervisión sobre el funcionamiento y las limitaciones de la IA utilizada.



IMPORTANTE

La IA agéntica requiere límites claros de actuación, evaluación previa de riesgos y control humano continuo.

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.

(…)

La Agencia también recuerda que los requisitos de calidad de los datos no se aplican únicamente a los datos personales, sino que **los datos no personales** utilizados en un tratamiento pueden ser también determinantes para su idoneidad. Además, subraya que el cumplimiento del RGPD exige diseñar tratamientos que gestionen adecuadamente las limitaciones de los sistemas de inteligencia artificial mediante medidas y salvaguardas adecuadas.

Puede ver información relacionada en el siguiente enlace:

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

EL PROFESIONAL RESPONDE

ENS y gestión de incidentes: anticiparse, reaccionar y minimizar el impacto

Los ciberincidentes forman parte del escenario actual de cualquier organización. Por ello, el Esquema Nacional de Seguridad no solo exige implantar medidas preventivas, sino también disponer de procedimientos eficaces para detectar, contener y recuperar los sistemas afectados. Los artículos 25 y 33 del Real Decreto 311/2022 establecen la obligación de gestionar los incidentes de seguridad de forma estructurada y documentada.

Una respuesta eficaz comienza con la identificación temprana del incidente, continúa con la adopción de medidas para limitar su impacto y finaliza con la recuperación de los servicios y el análisis de las causas que lo originaron. Todo ello debe quedar documentado para facilitar la mejora continua y acreditar el cumplimiento de las obligaciones de seguridad.

En este proceso, el CCN-CERT desempeña un papel esencial mediante la publicación de guías técnicas, indicadores de compromiso y procedimientos de coordinación para las entidades sujetas al ENS.

Además, cuando el incidente implique datos personales, será necesario valorar las obligaciones de notificación previstas en los artículos 33 y 34 del RGPD, reforzando la coordinación entre los equipos de ciberseguridad y protección de datos.

IMPORTANTE

La organización debe responder de forma rápida, coordinada y conforme a la normativa aplicable.