

EL RGPD UE 2016/679 EN APLICACIÓN

Supuestos de designación obligatoria del Delegado de protección de datos

El Reglamento General de Protección de Datos (RGPD) establece que ciertos responsables y encargados del tratamiento deben designar obligatoriamente un delegado de protección de datos (DPD).

Sector público: Cuando *«el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial»*.

Observación sistemática a gran escala: si *«las actividades principales [...] requieren una observación habitual y sistemática de interesados a gran escala»* (por ejemplo, monitorización masiva de comportamientos o perfiles en Internet).

Datos sensibles a gran escala: si *«las actividades principales [...] consisten en el tratamiento a gran escala de categorías especiales de datos personales [...] y de datos relativos a condenas e infracciones penales»*.

Además, la LOPD/GDD impone la designación obligatoriamente en ciertos sectores, como centros educativos, entidades financieras o aseguradoras, centros sanitarios o empresas de servicios de comunicaciones electrónicas.

Una vez designado el DPD su nombramiento debe notificarse a la autoridad de control en un plazo de 10 días y publicarse su contacto.

Contenido

1. Supuestos de designación obligatoria del Delegado de protección de datos.
2. Sancionada una clínica con 30.000 euros por falta de medidas de confidencialidad en sus campañas comerciales.
3. Neuroderechos: proteger la mente en la era de la inteligencia artificial (II).
4. Derecho de supresión para actividades públicas.
5. Sanciones por incumplimiento de la NIS2: riesgos y responsabilidades para la alta dirección.



IMPORTANTE

El DPD actúa como garante interno del cumplimiento normativo, asesorando, supervisando y sirviendo de enlace con la autoridad de control.

SANCIONES DE LA AEPD

Sancionada una clínica con 30.000 euros por falta de medidas de confidencialidad en sus campañas comerciales

La Agencia Española de Protección de Datos, en su Resolución [PS-00158-2023](#), sanciona a una clínica estética por vulnerar el principio de confidencialidad del artículo 5.1.f) del RGPD, tras la inclusión de clientes en un grupo de WhatsApp con fines promocionales sin adoptar las medidas adecuadas para garantizar la confidencialidad de los datos personales.

Los hechos se originan cuando la entidad reclamada creó un grupo de mensajería instantánea denominado “Medicina Estética 2”, en el que incorporó los números de teléfono de numerosos clientes, incluidos los reclamantes, permitiendo que todos los integrantes pudieran visualizar los datos personales del resto. La AEPD acreditó que el grupo fue creado sin base jurídica ni consentimiento expreso.

La autoridad de control subraya que, aunque el responsable podía tratar los datos con base en la ejecución del contrato o en su interés legítimo para promociones comerciales, estaba obligado a garantizar la confidencialidad.

La infracción reviste especial gravedad al afectar a datos de salud, categoría especial del artículo 9 del RGPD. En consecuencia, la AEPD impuso una multa de 30.000 euros y ordenó la eliminación del grupo y la implantación de sistemas de comunicación que impidan la visibilidad de los datos entre destinatarios.

Se imponen medidas para cumplir en el plazo de un mes la eliminación del grupo de WhatsApp y, en tres meses implantar sistemas de comunicación que impidan la visibilidad entre participantes.



IMPORTANTE

El artículo 5.1.f del RGPD exige que los datos personales se traten garantizando su seguridad y confidencialidad, evitando accesos, comunicaciones o usos no autorizados.

LA AEPD ACLARA**Neuroderechos: proteger la mente en la era de la inteligencia artificial (II)**

La evolución acelerada de las neurotecnologías plantea la necesidad de extender el marco jurídico vigente hacia una nueva frontera regulatoria: los denominados **neuroderechos**. Estos derechos emergentes buscan salvaguardar dimensiones de la autonomía humana frente al tratamiento de neurodatos, incluyendo la libertad cognitiva, la privacidad mental, la integridad psicológica y la continuidad de la identidad personal, todas ellas estrechamente vinculadas a la dignidad humana.

En el [informe conjunto](#) de la Agencia Española de Protección de Datos y del Supervisor Europeo de Protección de Datos, se indica que estas garantías no constituyen solo construcciones éticas, sino una respuesta jurídica necesaria ante tecnologías capaces de registrar, analizar e incluso influir en la actividad cerebral. Los riesgos asociados a estas capacidades incluyen injerencias profundas en la esfera mental, con potencial impacto sobre la autodeterminación individual

Desde la perspectiva del Derecho de la Unión Europea, la tutela de los neurodatos debe integrarse de forma coherente en el marco del RGPD y de la Carta de los Derechos Fundamentales. En este contexto, los principios de licitud, proporcionalidad, minimización y transparencia resultan esenciales

**IMPORTANTE**

Los neuroderechos amplían la protección de datos para salvaguardar la mente humana frente al uso invasivo de neurotecnologías y neurodatos.

ACTUALIDAD CIBERSEGURIDAD Y PRIVACIDAD

Derecho de supresión para actividades públicas

Fuente: [AEPD](#)

5 de Diciembre de 2025

Derecho de supresión para actividades públicas

La resolución aborda la reclamación presentada por una persona que solicitó a una entidad la retirada de unas imágenes en las que aparecía participando en actos públicos debido a su cargo en la misma. La organización respondió fuera de plazo denegando la solicitud. La persona reclamante, que consideró que su petición no había sido atendida adecuadamente, acudió a la Agencia Española de Protección de Datos para que tutelase su derecho. La resolución completa, [que puede consultarse en este enlace](#), es susceptible de recurso

La Agencia Española de Protección de Datos (AEPD) analiza en esta resolución si procede eliminar datos personales publicados en internet, especialmente cuando se trata de **información vinculada a actividades públicas**. Una persona que había ostentado un cargo relevante en una entidad, una vez deja de ostentarlo, solicitó a dicha entidad la retirada de unos vídeos publicados en el canal corporativo en los que aparecía participando en actos públicos debido a su puesto. Las imágenes correspondían a eventos y campañas en los que la persona reclamante participaba debido a su cargo y se encontraban publicadas en la página web, el canal de YouTube y otros espacios digitales gestionados por la organización. La entidad respondió denegando la solicitud, aunque lo hizo fuera de plazo. (...)

La AEPD recuerda en su resolución que la publicación de imágenes en internet constituye un tratamiento de datos personales sujeto a los requisitos generales del RGPD. Por lo tanto, debe analizarse si el responsable cuenta con una base jurídica válida para ello. A su vez, debe **ponderarse si el derecho a la protección de datos del interesado prevalece sobre otros derechos fundamentales**, en particular, si el derecho de protección de datos prevalece frente a, por ejemplo, el derecho de libertad de información o el de libertad de expresión.

Aplicando estos criterios al caso concreto, la Agencia concluye que la información tratada **no se circunscribe a la vida personal de la persona reclamante, y no puede considerarse obsoleta o inexacta**. La parte reclamante tampoco ha alegado **circunstancias personales** que evidencien que debe prevalecer su derecho en este caso concreto, por lo que la Agencia considera que debe decaer el derecho a la protección de datos frente a la libertad de expresión y de información y frente al interés de los usuarios de internet en conocer la información.

Puede ver información relacionada en el siguiente enlace:

[Expediente N.º: EXP202506820](#)

EL PROFESIONAL RESPONDE

Sanciones por incumplimiento de la NIS2: riesgos y responsabilidades para la alta dirección

La Directiva (UE) 2022/2555 (NIS2) no es solo una nueva norma en materia de ciberseguridad; es un cambio cultural en la forma en que las organizaciones deben gestionar los riesgos digitales. Para responsables del tratamiento y equipos directivos, la NIS2 nos deja un mensaje claro: la ciberseguridad ya no puede delegarse exclusivamente en el departamento de IT.

La NIS2 introduce un marco sancionador armonizado que prevé multas de hasta 10 millones de euros o el 2 % del volumen de negocio anual global. Estas sanciones pueden ser impuestas entre otras causas:

- Ausencia de análisis de riesgos actualizado.
- Planes de respuesta a incidentes inexistentes.
- Notificaciones tardías a la autoridad competente.

Uno de los elementos más relevantes es la implicación directa de la alta dirección. ¿Cuáles son las exigencias que impone la NIS2 a la alta dirección?:

- Los órganos de administración deben aprobar y supervisar activamente las medidas de ciberseguridad.
- Asunción de responsabilidad por incumplimiento cuando exista negligencia grave y falta de supervisión.
- Formación obligatoria en ciberseguridad.



IMPORTANTE

La NIS2 prevé sanciones elevadas por incumplimientos habituales, como mala gestión de riesgos, falta de respuesta a incidentes o notificaciones tardías.