

## EL RGPD UE 2016/679 EN APLICACIÓN

### El rol del responsable del tratamiento (I)

En el RGPD encontramos una definición del responsable del tratamiento como aquella persona física, jurídica o autoridad, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento de los datos personales. Es decir, es el que da las instrucciones de cómo han de tratarse los datos de los cuáles es responsable.

A lo largo del RGPD y LOPDGD se establecen las obligaciones que como responsable ha de cumplir para garantizar un tratamiento de los datos personales acordes con los principios generales relativos al tratamiento.

Para cada actividad de tratamiento de datos personales se deben tener en cuenta, entre otros, los siguientes requisitos:

- Designación de DPD en caso de ser obligatorio, o en su caso un coordinador de protección de datos.
- Elaborar un registro de actividades de tratamiento teniendo en cuenta la finalidad y la base jurídica.
- Realizar un análisis de riesgos.
- Establecer mecanismos para notificar las brechas de seguridad.
- Analizar la necesidad de realizar una evaluación de impacto en protección de datos.

#### Contenido

- 1.El rol del responsable de tratamiento (I).
- 2.Una compañía de mensajería es sancionada con una multa de 84.000 euros por falta de medidas de seguridad.
- 3.Inteligencia Artificial: principio de exactitud en los tratamientos(I).
- 4.La AEPD publica la Circular sobre el derecho de los usuarios a no recibir llamadas comerciales no solicitadas. La AEPD publica la Circular sobre el derecho de los usuarios a no recibir llamadas comerciales no solicitadas.
- 5.¿La privacidad y la ciberseguridad se complementan?



#### IMPORTANTE

El responsable de tratamiento debe valorar la capacidad de cumplimiento de los encargados antes de realizar la formalización del contrato de acceso a datos.

## SANCIONES DE LA AEPD

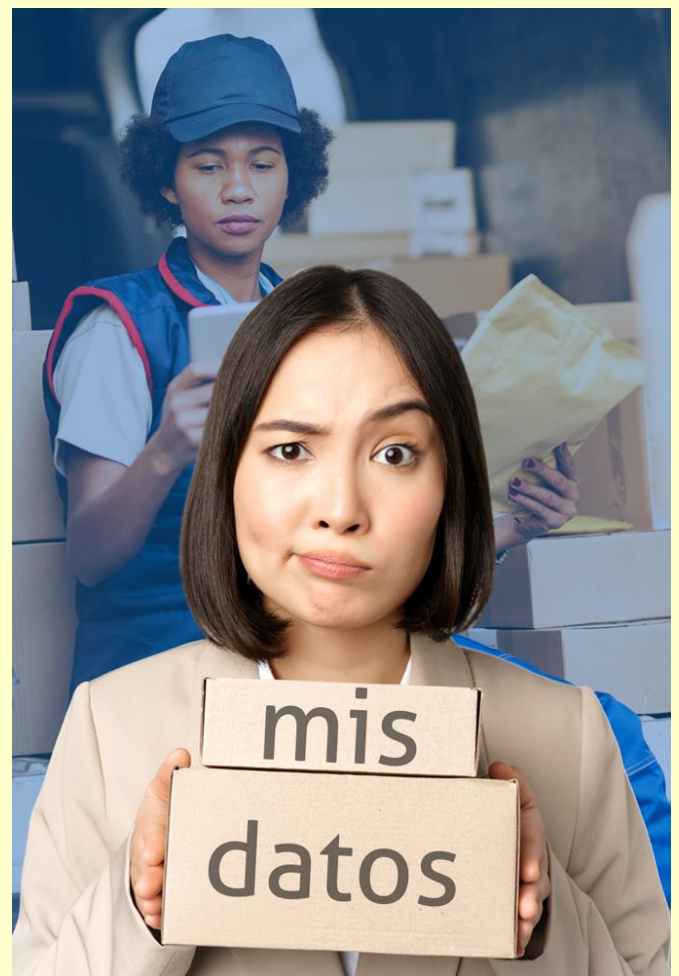
# Una compañía de mensajería es sancionada con una multa de 84.000 euros por falta de medidas de seguridad

En la resolución de la [AEPD](https://www.aepd.es/es/documento/reposicion-ps-00637-2022.pdf) <https://www.aepd.es/es/documento/reposicion-ps-00637-2022.pdf>, se sanciona a una empresa de mensajería por la falta de confidencialidad en el tratamiento de los datos personales y no aplicar suficientes medidas de seguridad.

La reclamación fue interpuesta por la destinataria de un envío gestionado por la entidad sancionada. En el escrito de reclamación se indica que el repartidor entregó el envío sin su consentimiento en un local comercial, y no en su domicilio. Lo que supuso una exposición de los datos postales y el número de teléfono de la reclamada, puesto que figuraban en el paquete y en el albarán de entrega.

La AEPD estimó que se había vulnerado el principio de integridad y confidencialidad (art. 5.1.f RGPD). Los datos personales de la reclamante, nombre, apellidos, teléfono y dirección se expusieron indebidamente a un tercero. Como agravantes se estableció la vinculación de la actividad de la entidad con la realización de tratamientos de datos personales y haber cometido la misma infracción por el que se inició un procedimiento sancionador en el año 2022. **Además, se le sanciona también, por la falta de aplicación de medidas de seguridad para evitar que el paquete se entregara otra persona que no fuera el destinatario del envío o alguien autorizado por él.**

Las reclamaciones por la publicación de datos en Internet sin consentimiento, videovigilancia y otros trámites se realizan a través de la [SEDE ELECTRÓNICA](#) de la AEPD.



### IMPORTANTE

Se considera una infracción grave la falta de adopción de las medidas técnicas y organizativas apropiadas para garantizar la seguridad del tratamiento.

## LA AEPD ACLARA

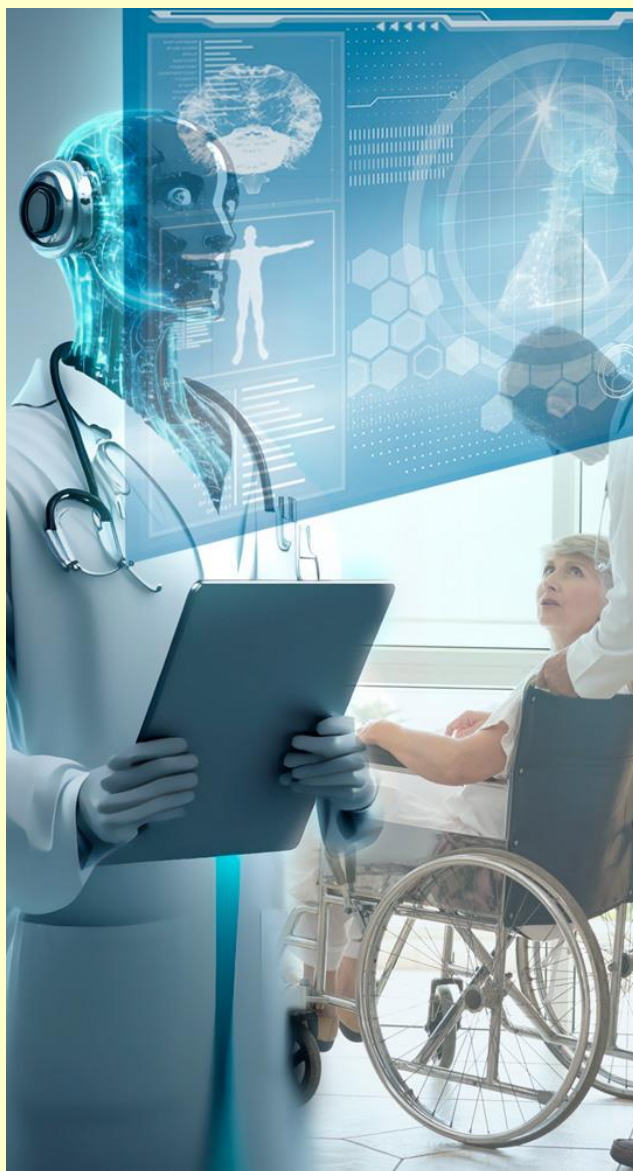
# Inteligencia Artificial: principio de exactitud en los tratamientos(I)

En el apartado de [prensa y actualidad](#) de la AEPD se desarrolla un amplio contenido sobre el fenómeno de la Inteligencia Artificial (IA) y sus implicaciones en la privacidad.

**En concreto, al hablar de IA tenemos que hacer referencia también al principio de exactitud.** En aquellos tratamientos en los que se incorpora un sistema de IA es necesario evaluar la exactitud de los datos de entrada, puesto que de no realizarse se podrían introducir sesgos y comprometer el rendimiento del algoritmo y del tratamiento.

**Es muy importante que en el tratamiento con IA se incluyan salvaguardias adecuadas para evitar la inexactitud de los datos de entrada y proteger del impacto de los datos inexactos, con estrategias “desde el diseño”.**

La AEPD explica la importancia de este tratamiento con un caso real; una mujer de avanzada edad en situación crítica fue llevada al hospital por sus familiares. Para realizar el ingreso, los familiares tenían que responder rápidamente a las preguntas realizadas en el registro. Una de ellas era que si la paciente era una persona dependiente. La respuesta fue afirmativa, a pesar de que ella sí que podía valerse por sí misma, lo que supuso que se la enviara directamente a cuidados paliativos, ocasionando con ello un grave perjuicio para la paciente, que finalmente los familiares consiguieron revertir para que fuera atendida debidamente sin considerarla como dependiente.



### IMPORTANTE

Los datos personales serán, exactos y si fuera necesario, actualizados, se adoptarán medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos. (art.5.1.d RGPD)

## ACTUALIDAD LOPD

# La AEPD publica la Circular sobre el derecho de los usuarios a no recibir llamadas comerciales no solicitadas



Fuente: [AEPD](#)

(20 de junio de 2023). El Boletín Oficial del Estado ha publicado [la Circular de la Agencia Española de Protección de Datos](#) (AEPD) sobre el derecho de los usuarios a no recibir llamadas no solicitadas, fijando los criterios que aplicará la Agencia en relación con el artículo 66.1.b) de la Ley 11/2022 General de Telecomunicaciones.

Este artículo, aplicable desde **el 29 de junio de este año**, recoge el derecho de los usuarios a no recibir llamadas con fines de comunicación comercial no solicitadas, **salvo que exista consentimiento previo** del propio usuario para recibir este tipo de comunicaciones o que estas puedan **ampararse en otra base de legitimación** de las previstas en el Reglamento General de Protección de Datos (RGPD). El artículo de la Ley no limita exclusivamente la realización de las llamadas con fines de comunicación comercial al consentimiento e incluye la posibilidad de que estas puedan realizarse con otras bases jurídicas. Ante las dudas suscitadas en la interpretación de este artículo, la Circular de la Agencia contribuye a **clarificar el criterio, ofreciendo seguridad jurídica** tanto a aquellos que realizan las llamadas comerciales como a los usuarios que las reciben.

La Circular, que da continuidad al [informe](#) que la Agencia publicó en mayo, se publica tras haberse sometido al trámite de audiencia e información pública en el que **la Agencia ha recabado la opinión de los interesados**, dando audiencia a **las principales asociaciones y organizaciones representativas** de los afectados, y ha obtenido el dictamen favorable del Consejo de Estado.

El texto está compuesto por una parte expositiva, seis artículos y una disposición final. El artículo 1 establece el ámbito objetivo de la circular; el artículo 2, el consentimiento de los usuarios finales; el artículo 3, el interés legítimo del responsable o de terceros; el artículo 4, la consulta a los sistemas de exclusión publicitaria; el artículo 5, el tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales, y el artículo 6 otras garantías adicionales. La disposición final establece la entrada en vigor, fijando el día siguiente al de su publicación en el Boletín Oficial del Estado.

Puede ver más información en el siguiente enlace:

[Derecho a no recibir llamadas comerciales no solicitadas](#)

## EL PROFESIONAL RESPONDE

### ¿La privacidad y la ciberseguridad se complementan?

La respuesta a la pregunta es un rotundo sí. El tratamiento de datos personales debe realizarse en aplicación de los principios de limitación de finalidad, conservación, minimización y comunicación de datos. La implementación de la protección de datos por defecto y desde el diseño garantiza la privacidad de las personas, evitando que se conviertan en objetivos vulnerables. La ciberseguridad se convierte en un medio para proteger a las organizaciones y a las personas.

Sobre estos conceptos, la privacidad y la ciberseguridad, se ha ahondado de manera más pormenorizada en el canal que hemos inaugurado: CFI Tv.

Este canal se ha estrenado con la entrevista a Félix Barrio, director general del Instituto Nacional de Ciberseguridad (INCIBE). Durante la entrevista, ha explicado de forma pormenorizada el tipo de servicios de Ciberseguridad que ofrece el INCIBE, cuáles son los tipos de incidentes de seguridad que suelen sufrir las pymes de nuestro país, cuáles son las buenas prácticas que una pyme debería seguir para reducir el riesgo de sufrir un incidente de seguridad, entre otras cuestiones.

Toda la información que comparte Barrio durante la entrevista es una fuente de conocimiento y experiencia que proporcionan una radiografía completa del panorama de la Ciberseguridad en nuestro país. Puedes visualizarla al completo en este [enlace](#).



#### IMPORTANTE

El análisis de riesgos permite conocer a las empresas su nivel de dependencia de la tecnología para identificar las necesidades de inversión en medidas de ciberseguridad.