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 /23

EL RGPD UE 2016/679 EN APLICACIÓN

# El rol del encargado de tratamiento (II)

**La definición de encargado de tratamiento la podemos encontrar en el artículo 4.8 del RGPD: "aquella persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable".**

La empresa o entidad responsable del tratamiento está obligada por norma a elegir únicamente a los encargados más diligentes. Es decir, aquellos que le ofrezcan garantías suficientes de que van a aplicar las medidas técnicas y organizativas apropiadas, para cumplir con los requisitos del RGPD y garanticen la protección de los derechos del interesado.

**El encargado de tratamiento solamente podrá tratar los datos personales que pone a su disposición el responsable cuando se haya celebrado el contrato de acceso a datos.** Este contrato que está regulado en el artículo 28 del RGPD contiene las instrucciones mínimas documentadas que ha de seguir el encargado de tratamiento.

El encargado del tratamiento no podrá subcontratar con otro encargado los servicios que presta al responsable del tratamiento sin la autorización previa por escrito, específica o general del responsable. En el caso de que recurra a otro encargado se le imponen las mismas obligaciones de protección de datos.

## Contenido




**IMPORTANTE**

Tendrá la consideración de responsable del tratamiento y no la de encargado quién en su propio nombre establezca relaciones con los interesados aún cuando exista un contrato de acceso a datos.

SANCIONES DE LA AEPD

# Sancionada con 10.000 € una empresa organizadora de fiestas infantiles por publicar fotos de menores en RR.SS.

**En la resolución de la AEPD https://www.aepd.es/es/documento/reposicion-ps-00008-2023.pdf, se sanciona con 10.000 € a una empresa organizadora de fiestas infantiles por la publicación de fotografías de menores en Instagram.**

La madre de la menor presentó una reclamación ante la AEPD por la publicación de unas imágenes de su hija en la red social de Instagram. La menor había acudido a una fiesta de cumpleaños organizada en el establecimiento de la empresa sancionada.

**La reclamante en su escrito de reclamación manifestó que contactó con el autor de la publicación de las imágenes a través del servicio de mensajería proporcionado por el prestador del servicio, para que se eliminara la publicación o se pixelara la cara de los menores. No recibió respuesta y la publicación estuvo disponible 24hrs.**

La empresa reclamada alegó en su escrito que la petición de supresión no se hizo por los cauces adecuados por lo que no tuvieron conocimiento de dicha solicitud.

**La AEPD le impone una sanción de 10.000 € por el tratamiento de datos personales sin la legitimación adecuada. No consta en ningún documento acreditado que la entidad reclamada hubiera solicitado el consentimiento a los progenitores, en el caso de los menores de 14 años para la publicación y difusión de imágenes en la RR.SS.**

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**

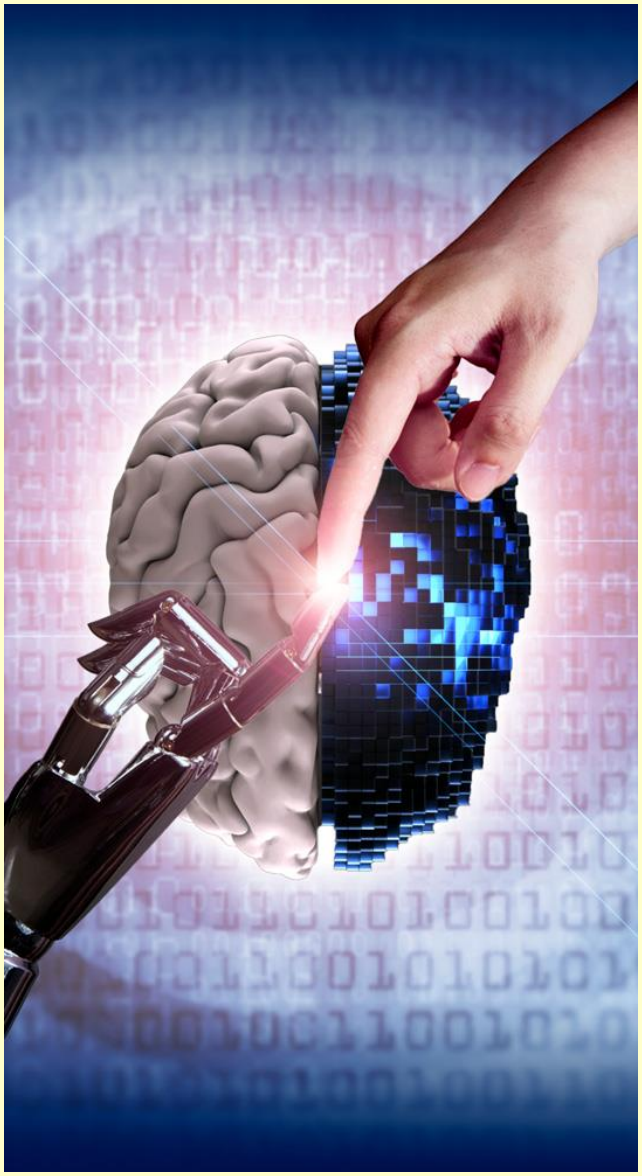
Se considera una infracción muy grave el tratamiento de datos personales sin que concurran alguna de las condiciones de licitud del tratamiento establecidas en la normativa.

LA AEPD ACLARA

# Inteligencia Artificial: puntos clave del principio de exactitud en los tratamientos (II)

Los puntos clave que indica la AEPD en el apartado de prensa y actualidad para aplicar la Inteligencia Artificial en un tratamiento de datos personales y que cumpla con la normativa en protección de datos son los siguientes:

- **Definir con precisión los datos de entrada a un algoritmo** para evitar que de lugar a errores o sesgos que no forman parte del algoritmo en sí.
- **El principio de exactitud debe aplicarse en los datos de entrada, salida e incluso en los datos intermedios de todo el tratamiento.**
- La definición precisa de cada dato de entrada debe establecerse "por diseño" y documentarse adecuadamente, así como el rango de valores.
- **El impacto de cada dato de entrada en el resultado final debe evaluarse "por diseño", para cada fin específico, mediante pruebas de verificación de los requisitos y pruebas de validación en el contexto de la operación.**
- Los interesados y quiénes recopilan los datos deben conocer y comprender la semántica de los datos y el impacto de su respuesta.
- Los datos de entrada a un algoritmo pueden recopilarse de otras fuentes, como bases de datos, sensores con cámaras etc. Todas las operaciones forman parte del tratamiento junto con el algoritmo.
- **Para cada fin específico se aplicarán todas las medidas para suprimir y/o rectificar sin dilación los datos inexactos.**



**IMPORTANTE**

El responsable del tratamiento es quién ha de determinar si los resultados de un sistema de IA implicarán una decisión automática o determinará que se incluya una supervisión humana que tome la decisión final.

ACTUALIDAD LOPD

# La AEPD actualiza su Guía sobre el uso de cookies para adaptarla a las nuevas directrices del Comité Europeo de Proteccion de Datos

*Fuente: AEPD*

**(Madrid, 11 de julio de 2023)**. La Agencia Española de Protección de Datos (AEPD) ha actualizado la Guía sobre el uso de las cookies para adaptarla a las Directrices 03/2022 sobre patrones engañosos del Comité Europeo de Protección de Datos (CEPD). La nueva versión de la Guía realizada por la Agencia ha contado, tal y como ocurrió con versiones anteriores, con la participación de los sectores afectados (las asociaciones ADIGITAL, Anunciantes, AUTOCONTROL e IAB Spain).

El Comité Europeo de Protección de Datos publicó en febrero de 2023 las Directrices 03/2022 sobre patrones engañosos en redes sociales. La Agencia incorpora a la nueva versión de la Guía el criterio del Comité Europeo, que recoge que **las acciones de aceptar o rechazar cookies** tienen que presentarse en un lugar y formato destacados, y ambas acciones deben estar al mismo nivel, sin que sea más complicado rechazarlas que aceptarlas. La Guía incluye nuevos ejemplos sobre cómo deben mostrarse estas opciones ofreciendo indicaciones sobre, entre otros, el color, tamaño y lugar en el que aparecen.

En paralelo a esa incorporación, se han realizado una serie de modificaciones:

En el caso de las **cookies de personalización**, cuando el **propio usuario toma decisiones** sobre ellas (por ejemplo, la elección del idioma de la web o la moneda en la que desea realizar transacciones), se trata de cookies técnicas que no requieren de consentimiento, sin que puedan ser utilizadas para otras finalidades.

Sin embargo, cuando **es el editor el que adopta este tipo decisiones** sobre las cookies de personalización basándose en la información que obtiene del usuario deberá informar sobre ello ofreciendo de forma destacada la opción de aceptarlas o rechazarlas. En este caso, el editor tampoco podría utilizarlas para otras finalidades. (…)

Los criterios recogidos en la Guía deberán implementarse, a más tardar, el 11 de enero de 2024,

Puede ver más información en el siguiente enlace:

Guía sobre el uso de las cookies julio 2023

**EL PROFESIONAL RESPONDE**

# ¿Por qué es importante implementar una política de control de acceso en nuestra empresa? (I)

En boletines anteriores veíamos la importancia de la elaboración de las normas de uso interno para garantizar la seguridad de información en nuestra empresa. Se hacía referencia, entre otras, al desarrollo de las políticas de protección de datos personales, normas de uso de los dispositivos digitales y política de seguridad en el puesto de trabajo. **En este boletín abordaremos la importancia de la implementación de una política de control de acceso.**


Hoy en día el acceso a la información de la empresa no es solamente local e interno. La tecnología permite que los servicios y aplicaciones que ofrecemos a nuestros clientes se haga de forma remota o bien a través de aplicaciones en la nube. Los usuarios/as y empleados acceden a la información de la empresa través de Internet con los dispositivos digitales, en algunos casos facilitados por la empresa y en otros casos con dispositivos propios. El control de accesos se ha hecho más complejo.

**Para realizar un control de acceso adecuado se ha de establecer una política de acceso que defina una gestión de usuarios y una segregación de funciones. Esta política se caracteriza por el principio de mínimo conocimiento, conocido como *need-to-know*.** Este principio consiste en que cada persona de la organización accederá solamente a lo que necesita saber para realizar sus funciones.

**IMPORTANTE**

El control de acceso a la información de la empresa es necesario para la prevención de situaciones de fugas de información del personal interno o borrado de información.