PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

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

Boletín 05/25

EL RGPD UE 2016/679 EN APLICACIÓN

Licitud, lealtad y transparencia generan confianza y garantizan el cumplimiento normativo

El principio de licitud, lealtad y transparencia recogido en el artículo 5.1.a) del Reglamento General de Protección de Datos (RGPD) constituye el pilar sobre el que se edifica el tratamiento legítimo de los datos personales. La licitud exige que toda operación de tratamiento se base en una de las condiciones del artículo 6 del RGPD: consentimiento, cumplimiento de una obligación legal, ejecución de un contrato, interés vital, misión de interés público o interés legítimo. **Sin base jurídica, no hay tratamiento lícito.**

La lealtad implica una conducta coherente por parte del responsable, que debe actuar de manera ética, evitando prácticas ocultas, engañosas o desproporcionadas. Este aspecto se conecta directamente con la transparencia, que exige que los interesados comprendan con claridad cómo y por qué se tratan sus datos.

En este contexto, la Guía para el cumplimiento del deber de informar de la AEPD establece que la información debe proporcionarse por capas, ser accesible, clara, concisa y adaptada al usuario. El responsable debe informar, entre otros datos, sobre su identidad, finalidades del tratamiento, base jurídica, destinatarios, derechos de los interesados y, en su caso, transferencias internacionales.

Contenido

1. Licitud, lealtad y transparencia generan confianza y garantizan el cumplimiento normativo.
2. Sancionada una agencia de publicidad con 120.000€ por el incumplimiento de los principios del RGPD.
3. El deber de informar y otras medidas de responsabilidad proactiva en APPS para dispositivos móviles (I).
4. El Comité Europeo de Protección de Datos somete a consulta pública sus directrices sobre el tratamiento de datos personales mediante blockchain.
5. ¿Cuál es el objetivo y ámbito de aplicación de la Directiva NIS2?

IMPORTANTE

El incumplimiento del principio de licitud en el tratamiento de datos puede ser sancionado como infracción muy grave según la LOPDGDD, con multas significativas.

SANCIONES DE LA AEPD

Sancionada una agencia de publicidad con 120.000€ por el incumplimiento de los principios del RGPD

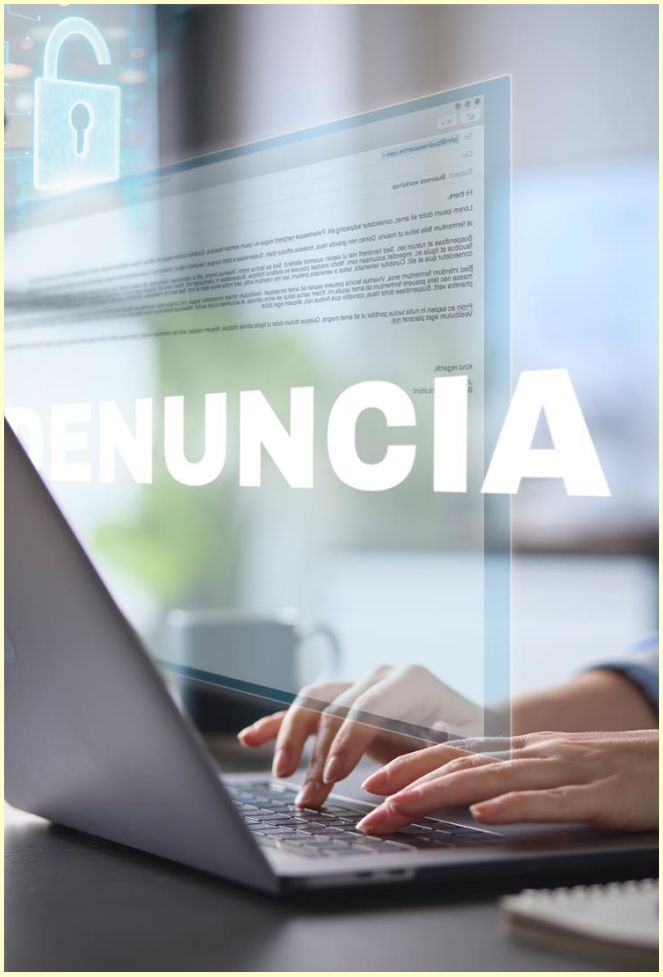
En la resolución de la AEPD https://www.aepd.es/documento/ps-00416-2023.pdf se sanciona a una agencia de publicidad por el incumplimiento de los principios del RGPD.

La parte reclamante denunció ante la AEPD que la agencia reclamada trataba sus datos personales (nombre, apellidos, NIF, teléfono y correo electrónico) sin existir relación contractual ni haber prestado consentimiento. La reclamación se originó tras recibir un correo en el que la reclamada le informaba de un incidente de seguridad que afectó a sus datos y que habían sido obtenidos a través de la consulta al servicio de la Lista Robinson para evitar el envío de comunicaciones comerciales.

La investigación acreditó que los datos fueron remitidos a la agencia publicitaria por ADIGITAL en 2018, a través de una solicitud de revocación de consentimiento iniciada por la propia reclamante mediante el servicio de la Lista Robinson. No obstante, en agosto de 2022, la entidad sufrió una brecha de seguridad que comprometió los datos personales de más de 80.000 personas. **La AEPD constató que la entidad no notificó adecuadamente la violación ni a la autoridad ni a los afectados en los plazos legales, e identificó deficiencias graves en las medidas técnicas y organizativas de seguridad.**

Como resultado, la AEPD declaró la existencia del incumplimiento del artículo 5.1.f) RGPD que regula el principio de integridad y confidencialidad, del artículo 33 RGPD por la falta de la notificación de la brecha de seguridad a la autoridad de control y del artículo 34 RGPD por comunicar a los interesados fuera de plazo.

El artículo 5.1.f del RGPD exige garantizar la seguridad de los datos personales, protegiéndolos contra el tratamiento no autorizado, pérdida, destrucción o daño accidental.



IMPORTANTE

La AEPD puede investigar documentos generales de privacidad si están relacionados con los hechos reclamados, para detectar deficiencias y sancionar adecuadamente.

LA AEPD ACLARA

El deber de informar y otras medidas de responsabilidad proactiva en *APPS* para dispositivos móviles (I)

Las aplicaciones móviles *(apps*), cada vez más presentes en nuestra vida diaria, representan un reto significativo en términos de protección de datos personales. El Reglamento General de Protección de Datos (RGPD) exige que los responsables del tratamiento proporcionen una información transparente, clara y accesible, obligación que cobra especial relevancia en el contexto de las *apps*.

En la nota técnica de la AEPD se hace especial referencia a la información que los responsables del tratamiento deben facilitar a los usuarios de la aplicación. Se tiene que cumplir con los artículos 13 y 14 del RGPD, aplicando criterios como la información por capas, el acceso en un máximo de dos clics y la disponibilidad de las políticas de privacidad tanto en la tienda de aplicaciones, en su caso, como en la propia aplicación.

La política de privacidad debe especificar con claridad qué datos se recogen, con qué fines, durante cuánto tiempo y quién los trata. Asimismo, el lenguaje debe adaptarse al perfil del usuario, especialmente si se trata de menores, y evitar generalidades que impidan comprender el alcance real del tratamiento.

La política de privacidad debe especificar claramente los permisos que solicita la *app*, su finalidad y alcance (lectura, escritura, uso en segundo plano), e informar al usuario cómo otorgarlos, revocarlos y gestionarlos en todo momento.

IMPORTANTE

La política de privacidad debe estar accesible tanto en la *app* como en la tienda, permitiendo al usuario consultarla antes de instalarla y en cualquier momento durante su uso.

ACTUALIDAD LOPD

El Comité Europeo de Protección de Datos somete a consulta pública sus directrices sobre el tratamiento de datos personales mediante blockchain

Fuente: AEPD

(5 de mayo de 2025). El Comité Europeo de Protección de Datos (CEPD) ha adoptado en su reunión plenaria de abril unas directrices sobre el tratamiento de datos personales mediante tecnologías blockchain)

Guidelines 02/2025 on processing of personal data through blockchain technologies), en las que **la Agencia Española de Protección de Datos (AEPD) ha sido la ponente principal** en la fase previa a su lanzamiento.

Estas directrices están sometidas a consulta pública **hasta el 9 de junio de 2025**, dando a las partes interesadas la posibilidad de presentar sus observaciones.

Blockchain es un registro digital distribuido que permite validar transacciones y garantizar la integridad de los datos sin una autoridad central. La tecnología blockchain también permite manejar y transferir datos de forma segura, garantizando su integridad y trazabilidad. Dado que el uso de las tecnologías blockchain se está extendiendo, el Comité se ha propuesto entre sus objetivos **ayudar a cumplir con el RGPD** a las organizaciones que utilizan estas tecnologías, objetivo compartido por la Agencia.

En sus directrices, el Comité explica cómo funcionan las cadenas de bloques, evaluando las diferentes arquitecturas posibles y sus implicaciones para el tratamiento de datos personales. Las directrices destacan la importancia de aplicar medidas técnicas y organizativas en las primeras fases del diseño del tratamiento. Además, destacan que las organizaciones deben llevar a cabo una evaluación de impacto sobre la protección de datos (EIPD) antes de tratar datos personales mediante tecnologías blockchain cuando sea probable que el tratamiento suponga un alto riesgo para los derechos y libertades de las personas.

Puede ver información relacionada en el siguiente enlace:

El Comité Europeo de Protección de Datos somete a consulta pública sus directrices sobre el tratamiento de datos personales mediante blockchain

EL PROFESIONAL RESPONDE

¿Cuál es el objetivo y ámbito de aplicación de la Directiva NIS2?

La Directiva (UE) 2022/2555, conocida como NIS2 *(Network and Information Security Directive 2)* refuerza el marco normativo en materia de ciberseguridad de la Unión Europea, con el objetivo de alcanzar un elevado nivel común de ciberresiliencia en los Estados miembros. Reemplaza a la Directiva NIS (2016/1148) y establece requisitos armonizados de seguridad y notificación, ampliando significativamente su ámbito de aplicación.

El ámbito de aplicación de la NIS2 se determina a partir de un criterio objetivo de tamaño y de la naturaleza de los servicios prestados. Quedan incluidas las entidades que operan en sectores considerados críticos o altamente relevantes para el funcionamiento del mercado interior y que desempeñan un papel clave para la sociedad o la economía.

Las entidades incluidas se clasifican en dos categorías:

1º Esenciales: las entidades esenciales pertenecen a sectores como energía, transporte, sanidad, agua potable, infraestructura digital o servicios financieros., **2º Entidades importantes:** abarcan sectores como manufactura crítica, servicios postales, alimentación o investigación.

Es importante preparase para para cumplir con la Directiva NIS2 y garantizar la continuidad del negocio, evitar sanciones, fortalecer la ciberresiliencia y proteger infraestructuras críticas ante amenazas crecientes.

IMPORTANTE

Actualmente, el anteproyecto de ley para transponer la Directiva NIS2 en España se encuentra en fase de tramitación, pendiente de aprobación definitiva, con implicaciones relevantes para sectores críticos y esenciales.