10 Preguntas y respuestas frecuentes sobre el GDPR

Resuelva sus dudas sobre la aplicación del Reglamento General de Protección de Datos (GDPR)

1. ¿Qué es el GDPR?

El Reglamento General de Protección de Datos (GDPR por sus siglas en inglés) es la nueva normativa europea de privacidad.

2. ¿A quién afecta?

A instituciones públicas, organizaciones sin ánimo de lucro y todo tipo de empresas que recopilan y analizan datos de ciudadanos residentes en la Unión Europea (UE).

3. ¿Cuándo entra en vigor?

El Parlamento Europeo aprobó el GDPR en abril de 2016, pero **su aplicación comenzó el 25 de mayo de 2018.**

4. ¿Qué cambios introdujo el GDPR?

La principal novedad es que otorga a los residentes de la UE un mayor control sobre sus datos personales, ampliando las obligaciones que deben cumplir las organizaciones.

5. Los 6 requisitos clave

01 Transparencia, imparcialidad y licitud en el manejo y uso de datos personales. Los usuarios deben tener claro cómo se están usando sus datos.

02 El procesamiento de datos personales queda limitado a los fines específicos, explícitos y legítimos para los que fueron recopilados originalmente.

03 Se debe minimizar la recopilación de datos personales en función del fin previsto.

04 Las organizaciones deben garantizar la exactitud de los datos personales y permitir su borrado o rectificación.

05 Limitar el almacenamiento de datos personales solo al tiempo necesario para lograr los fines para los cuales se recopilaron.

06 Garantizar la seguridad, integridad y confidencialidad de los datos personales.

6. ¿Qué tipo de sanciones conlleva su incumplimiento?

Las organizaciones pueden enfrentarse a multas de **hasta 20 millones de euros o el 4% de su volumen de negocio global anual.**

7. ¿Cómo obtener el consentimiento inequívoco del usuario?

El Reglamento recoge que el consentimiento, con carácter general, debe ser **libre, informado, específico e inequívoco.** Esto supone que debe existir una declaración del interesado o una acción positiva. El consentimiento no puede deducirse del silencio o de la inacción de los ciudadanos.

El denominado 'consentimiento tácito' dejará de ser legal.

Cuando se trate de datos "sensibles" no será suficiente con una acción positiva de carácter general, sino que deberá especificarse explícitamente el tipo de tratamiento de los datos que se realizará.

Las organizaciones deben ser capaces de demostrar que el usuario ha otorgado su consentimiento y para ello necesitará usar sistemas técnicos verificables.

8. ¿Cómo debe ser un aviso de privacidad?

El GDPR obliga a las entidades a informar en sus avisos de privacidad de: la base legal que da cobertura al tratamiento de los datos; el periodo de retención de los mismos; y los pasos que deben seguir los interesados para realizar cualquier reclamación.

La norma exige de forma expresa que la información que se proporcione sea fácil de entender y que se presente en un lenguaje claro y conciso.

9. ¿Es obligatorio tener un 'responsable de datos'?

Es recomendable -y en ciertos casos obligatorio- que las organizaciones nombren un representante de protección de datos o DPO que actuará como punto de contacto de las Autoridades de supervisión y de los ciudadanos.

Los datos de contacto de ese representante deberán proporcionarse a los interesados.

10. ¿Qué es la responsabilidad proactiva?

Hace referencia a la obligación de las organizaciones de garantizar técnicamente el cumplimiento del GDPR. Engloba varias medidas que toda entidad debe tener en cuenta y que sirven como hoja de ruta para el diseño de un proceso estándar de tratamiento de datos:

- **Protección de datos desde el diseño**
- **Protección de datos por defecto**
- **Medidas de seguridad**
- **Mantenimiento de un registro de tratamientos**
- **Realización de evaluaciones de impacto sobre la protección de datos**
- **Nombramiento de un delegado de protección de datos**
- **Notificación de violaciones de la seguridad de los datos**
- **Promoción de códigos de conducta y esquemas de certificación**

Los productos y servicios de Microsoft, como Azure, Dynamics 365, Enterprise Mobility + Security, Microsoft 365 y Windows 10 garantizan la detección y evaluación de amenazas de seguridad y el cumplimiento de las obligaciones del GDPR.

Infórmese de nuestra propuesta en seguridad y cumplimiento

https://www.microsoft.com/es/trust-center/privacy/gdpr-overview

Microsoft

tipsa
Tecnología de la Información

DATOS DE CONTACTO
Teléfono: 941 202 069
Web: www.tipsa.net
comunicacion@tipsa.net

TIPSA | www.tipsa.net

- Somos una consultora tecnológica especializada en el desarrollo, puesta en marcha y mantenimiento de soluciones de gestión empresarial con tecnología Microsoft. Desde 1992 trabajamos con las pymes facilitándoles su trabajo diario, ayudándoles a gestionar mejor sus recursos y capacidades, contribuyendo en su proceso de transformación digital.
- La tecnología de Microsoft nos permite ofrecer soluciones informáticas globales orientadas hacia la eficiencia en la gestión, la productividad, la colaboración y la mejora en los procesos de toma de decisiones en cualquier momento y lugar.
- Todas ellas se apoyan en una infraestructura segura con capacidad de crecimiento.
- Los proyectos se abordan pensando en el usuario final, y se diseñan atendiendo a criterios de sencillez, eficacia y funcionalidad.
- Implantaciones realizadas bajo la norma ISO 9001 y una alta especialización en las *Business Applications* de Dynamics 365 del mercado de SMB.