Reglamento General de Protección de Datos

El **Reglamento General de Protección de Datos (RGPD)**, conocido en inglés como **General Data Protection Regulation (GDPR)**, es una normativa de la Unión Europea que regula la protección de los datos personales y la privacidad de los ciudadanos de la UE. Entró en vigor el 25 de mayo de 2018, con el objetivo de armonizar las leyes de protección de datos en Europa, reforzar los derechos de las personas y responsabilizar a las empresas y organizaciones en el tratamiento de los datos.

—

Aspectos clave del RGPD 1. **Ámbito de aplicación**:

1. Abarca cualquier organización, dentro o fuera de la UE, que procese datos personales de personas ubicadas en la UE.
2. Se aplica a empresas, administraciones públicas, organizaciones sin ánimo de lucro, entre otros.

2. **Datos personales**:

1. Cubre cualquier información que identifique o pueda identificar a una persona, como nombre, dirección, correo electrónico, número de teléfono, IP, historial médico, etc.

3. **Principios fundamentales**:

1. **Licitud, lealtad y transparencia**: El tratamiento de datos debe ser justo y transparente para el interesado.
2. **Limitación de la finalidad**: Los datos solo pueden usarse para los fines específicos para los que se recopilaron.
3. **Minimización de datos**: Solo se deben recopilar los datos estrictamente necesarios.
4. **Exactitud**: Los datos deben ser precisos y estar actualizados.
5. **Limitación del plazo de conservación**: Los datos deben almacenarse solo el tiempo necesario.
6. **Integridad y confidencialidad**: Se deben garantizar medidas de seguridad adecuadas.

4. **Derechos de los interesados**:

1. **Acceso**: Derecho a conocer qué datos se tienen y cómo se procesan.
2. **Rectificación**: Corregir datos inexactos.
3. **Supresión (“derecho al olvido”)**: Solicitar la eliminación de los datos bajo ciertas condiciones.
4. **Portabilidad**: Transferir los datos a otro controlador.
5. **Oposición**: Rechazar el tratamiento de los datos.
6. **Limitación**: Restringir el procesamiento de los datos.

5. **Consentimiento**:

1. Debe ser explícito, informado, específico e inequívoco.
2. No se permite el consentimiento tácito o por omisión.

6. **Responsabilidad proactiva (Accountability)**:

1. Las organizaciones deben demostrar que cumplen con el RGPD (mediante registros, auditorías, evaluaciones de impacto, etc.).

7. **Evaluaciones de Impacto en la Protección de Datos (DPIA)**:

1. Obligatorias cuando el tratamiento de datos puede suponer un alto riesgo para los derechos de los interesados.

8. **Transferencias internacionales de datos**:

1. Solo están permitidas a países con un nivel de protección adecuado, o mediante cláusulas contractuales estándar, reglas corporativas vinculantes o mecanismos similares.

9. **Sanciones**:

1. Las infracciones pueden conllevar multas de hasta **20 millones de euros** o el **4% del volumen de negocio global anual**, lo que sea mayor.

—

Beneficios del RGPD - Empoderar a los ciudadanos en el control de sus datos. - Aumentar la confianza de los consumidores en las empresas que cumplen con la normativa. - Armonizar la legislación de protección de datos en la UE.