

Guía práctica: Normativa básica RGPD para empresas

El Reglamento General de Protección de Datos (RGPD) es una normativa europea que regula el tratamiento de datos personales. Afecta a todas las empresas que manejen información de clientes, empleados o proveedores. Esta guía resume los puntos esenciales que deben cumplirse.

1. Principios básicos del RGPD

- Licitud, lealtad y transparencia: los datos deben recogerse con consentimiento válido y ser tratados de forma clara.
- Limitación de la finalidad: los datos solo pueden usarse para el fin concreto para el que se recogieron.
- Minimización: solo se deben recoger los datos estrictamente necesarios.
- Exactitud: los datos deben mantenerse actualizados.
- Limitación del plazo de conservación: no se deben conservar más tiempo del necesario.
- Integridad y confidencialidad: se deben proteger los datos frente a accesos no autorizados.

2. Obligaciones de las empresas

- Informar al interesado sobre el uso de sus datos (política de privacidad clara).
- Obtener consentimiento explícito cuando sea necesario.
- Permitir a los usuarios ejercer sus derechos (acceso, rectificación, supresión, portabilidad, oposición).
- Firmar contratos de encargo de tratamiento con proveedores que gestionen datos en nombre de la empresa.
- Notificar brechas de seguridad a la Agencia Española de Protección de Datos (AEPD) en un plazo máximo de 72 horas.

3. Buenas prácticas recomendadas

- Nombrar un responsable de protección de datos (DPO) en empresas que lo requieran.
- Implantar medidas de seguridad como contraseñas robustas, copias de seguridad y cifrado.
- Formar al personal en protección de datos.
- Revisar periódicamente los procedimientos internos para asegurar el cumplimiento.
- Mantener registros de actividades de tratamiento de datos.

4. Ejemplo práctico

Una academia de formación que guarda datos de sus alumnos debe:

- Informar a los alumnos de qué datos recoge y para qué (ej. facturación, certificaciones).
- Pedir consentimiento para enviar comunicaciones comerciales.
- Guardar solo los datos necesarios y eliminarlos al terminar la relación contractual.