Guía Práctica LOPDGDD

Tus Datos a Salvo

www.tusdatosasalvo.com
Tlf: 658342479
e-mail:
patricia@tusdatosasalvo.es
info@tusdatosasalvo.es

01

La Protección de Datos, ¿por qué? Novedades del Reglamento Europeo de Protección de Datos (RGPD)

¿Puedo tratar datos? Activo principal de la Empresa

SI, pero con las medidas de seguridad y condiciones que marca la ley o que me permitan cumplir con el RGPD:

1.- Consentimiento previo e informado del titular, salvo excepciones.

2.- Medidas establecidas en el Reglamento de Desarrollo de la LOPD: arts 89 y ss

¿Qué es un dato de carácter personal?

Un **dato de carácter personal** es cualquier información numérica, alfabética, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables, tanto la relativa a su identidad (como nombre y apellidos, domicilio, filiación, una fotografía o video, etc...) como la relativa a su existencia y ocupaciones (estudios, trabajo, enfermedades, etc.)
Ejemplos de datos de carácter personal son: las direcciones postales, las cuentas de correo electrónico, el DNI,, las altas y bajas médicas, la información financiera y fiscal o la afiliación política.

Los datos relativos a una persona jurídica (domicilio, denominación social, CIF, etc.) no tienen la consideración de datos de carácter personal, por lo tanto, no le será de aplicación el Reglamento de Protección de Datos.

DATOS DE CATEGORÍAS ESPECIALES

El Reglamento establece en el artículo 9, las categorías especiales de datos refiriéndose a los datos sensibles que precisan una especial protección, ya sea por su naturaleza o por la relación que puedan tener con los derechos y las libertades fundamentales de las personas y les aplica disposiciones específicas cuando su tratamiento pueda entrañar altos riesgos en la protección de datos.

Siguen los mismos y se añaden algunos nuevos: origen étnico o racial, opinión política (no sólo ideología), confesión religiosa, datos genéticos, salud, afiliación sindical, datos biométricos (huella, retina, iris, dibujo de las venas), vida u orientación sexual.

Principales actuaciones:

1. Realizar un **Registro de actividades de tratamiento**.
2. Realizar un **Análisis de riesgos**.
3. Solicitar el **consentimiento a los clientes**.
4. Facilitar los **derechos de los usuarios**.
5. Firmar los **contratos con los empleados**.
6. Firmar los **contratos con terceros**.
7. Incluir los **textos legales** en la **página web**.
8. Notificar las **Brechas de Seguridad**.
9. Nombrar un **DPO si fuera necesario**.

1. Registro de actividades de tratamiento

Lo primero a tener en cuenta es qué tipo de datos se manejan y qué cantidad:
- ¿Cuáles son los **datos que recopilamos**?
- ¿Por qué los necesitamos?
- ¿Cuál es la **política de almacenamiento** de esos datos?
- ¿**Cedemos esos datos** o los transferimos fuera de nuestro país?
- ¿A través de qué medios realizamos el tratamiento?
- ¿Cuáles son los plazos de conservación?

Los tratamientos más habituales son:

Clientes y/o proveedores
Contabilidad
Recursos Humanos
Curriculum
Videovigilancia

2. ANÁLISIS DE RIESGOS.

La empresa debe también realizar **análisis del riesgo** en el que se valoren las posibles contingencias de los tratamientos que se realicen, teniendo en cuenta, entre otras cuestiones:

- Tipo de datos.
- Naturaleza de los datos.
- Medios de tratamiento.
- Cesiones previstas.
- Transferencias internacionales.
- Número de interesados afectados.

3. SOLICITAR EL CONSENTIMIENTO A LOS CLIENTES

- Eliminación del consentimiento tácito: necesidad de acción afirmativa del afectado.
- Como el contenido del derecho de información se ve muy ampliado, hay que recoger de nuevo el consentimiento de los que ya son clientes.
- Si es en papel: firma del cliente.
- Si es on line: con el cuadradito del Check-box.

4. FACILITAR LOS DERECHOS DE LOS USUARIOS.

Los interesados, los dueños de los datos personales, pueden ejercer, según el RGPD, sus derechos. Estos son los derechos que pueden ejercer los interesados:

1. **Acceso** a los propios datos personales;
2. **Rectificación** si los datos son inexactos;
3. **Supresión**(derecho al olvido) si se tratan de forma ilegal o ya no son necesarios para la finalidad con que se recogieron;
4. **Limitación** del tratamiento;
5. **Portabilidad** de los datos;
6. **Oposición** a un uso posterior con fines de prospección comercial (marketing directo), investigación científica o histórica, o fines estadísticos; y a no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles).

https://www.aepd.es/reglamento/derechos/index.html

5. FIRMAR LOS CONTRATOS CON LOS EMPLEADOS

- Los empleados suelen tener acceso a toda la información que se maneja y, por tanto, deben firmar un **acuerdo de confidencialidad** para evitar que esa información sea revelada a personas no autorizadas. También deben **cumplir las medidas de seguridad** establecidas por la empresa para garantizar la protección de los datos personales.

5.1. Para qué se recogen sus datos y a quiénes se les van a ceder.
5.2. Confidencialidad con los datos de la empresa.

6. FIRMAR LOS CONTRATOS CON TERCEROS: E.T.

El RT debe tener presente una **lista de esas empresas externas** con las que tienen contacto y asegurar que también cumplan la normativa de Protección de Datos. Por ejemplo:

- Asesorías.
- Empresas informáticas.
- Empresas de video vigilancia.
- Empresas de mensajería, etc.

Para ello es necesario que firmes un contrato de **encargo de tratamiento** con esos terceros en el que se establezcan las obligaciones de estos para proteger los datos personales a los que accedan.

7. INCLUIR TEXTOS LEGALES EN LA WEB

Si tienes una **página web** debes incluir en ella los textos exigidos por la **ley de Protección de Datos y la LSSI**:

- **Aviso legal**
- **Política de privacidad**
- **Política de cookies**

8. NOTIFICAR LAS BRECHAS DE SEGURIDAD.

Una de las obligaciones que establece el nuevo Reglamento es la notificación de los incidentes de seguridad que se produzcan en la empresa, tanto a los afectados como a la AEPD.

- **En el caso de que se dé una situación de ciberataque o infracción, lo ideal es estar prevenidos con un plan de respuesta ante incidentes.**
- **Debes notificar las brechas de seguridad en un plazo de 72 horas.**
- Cabe destacar que, aunque no se permitirán infracciones intencionadas de la ley, existirán atenuantes si se puede demostrar a las autoridades y a los clientes que se está haciendo todo lo posible para cumplir con ella.

Definiciones de los conceptos generales de la protección de datos

Estructura de los datos:

Datos personales: Información relativa a una persona física, identificada o identificable, por la cual pueda determinarse, directa o indirectamente, su identidad.

Identificable: Cuando se pueda determinar la identidad de una persona mediante: nombre, número, datos de localización, identificador, identidad física, fisiológica, genética, psíquica, económica, cultural, social u otros elementos propios de su identidad.

Interesado: Persona física sometida al tratamiento de sus datos personales.

Tratamiento: Operaciones realizadas sobre datos personales: recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Fichero: Conjunto estructurado de datos personales susceptibles de tratamiento para un fin determinado.

Tratamiento de datos:

RESPONSABLE del tratamiento (RT): Persona física o jurídica, Autoridad pública, servicio u organismo que, solo o conjuntamente con otros Corresponsables, determine los fines y los medios del tratamiento.

ENCARGADO del tratamiento (ET): Persona física o jurídica, Autoridad pública, servicio u organismo que, solo o conjuntamente con otros Encargados, trate datos personales por cuenta del RT.

CORRESPONSABLE del tratamiento: cuando varios RT determinen los fines y los medios del tratamiento.

DESTINATARIO de datos: Persona física o jurídica, autoridad pública, servicio u organismo que reciba una comunicación de datos personales. No se aplica a las Autoridades públicas para investigaciones concretas de interés general reguladas por la ley.

PERSONAL autorizado: Persona autorizada para realizar un tratamiento de datos personales bajo la autoridad directa del RT o ET, que se haya comprometido a respetar la confidencialidad o tengan la obligación legal de confidencialidad.

DELEGADO de protección de datos (DPO): Persona encargada de informar y asesorar al RT, ET y al Personal autorizado de las obligaciones relativas a la protección de datos personales.

AUTORIDAD de control (AC): Autoridad pública independiente con la función de supervisar la aplicación del Reglamento.

Categorías de datos:

Datos BÁSICOS: Datos personales que no correspondan a categorías Especiales de datos ni a condenas y delitos penales. Por ejemplo: nombre, dirección, email, teléfono, edad, sexo, firma, imagen, aficiones, patrimonio, datos bancarios, información académica, profesional, social, comercial, financiera, etc.

Categorías ESPECIALES de datos: Datos relativos al origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos o biométricos que permitan la identificación unívoca de una persona, datos relativos a la salud o a la vida y orientación sexuales.

Condenas y delitos PENALES: Datos relativos a condenas y delitos penales o medidas de seguridad afines.

Categorías de tratamiento:

Tratamiento con ALTO RIESGO: Tratamiento sujeto a una **evaluación de impacto** por ser susceptible de comportar un Alto Riesgo para la protección de los derechos y libertades de los Interesados.

TRANSFERENCIAS internacionales de datos: Traspaso de datos a RT, ET o Destinatarios de terceros países u organizaciones internacionales no establecidos en la UE.

Elaboración de PERFILES: Confección de decisiones individuales basadas en un tratamiento automatizado de datos, destinadas a evaluar aspectos personales o analizar o predecir el rendimiento profesional, situación económica, salud, preferencias o intereses personales, fiabilidad, comportamiento, ubicación o movimientos de una persona.

Datos tratados por GRUPOS de empresas: Grupo que comprende una empresa que ejerce el control y las empresas controladas.

Datos de titularidad o interés PÚBLICO:
Tratamientos realizados por Autoridades u Organismos Públicos en el ejercicio de sus funciones.
Tratamientos con finalidades de interés Público fundamentados en la legislación vigente.
Tratamientos con finalidades de investigación histórica, estadística o científica.