

PROTECCIÓN DE DATOS PASO A PASO

Información básica para pymes y autónomos

Si tienes una empresa o trabajas como autónomo y tratas datos personales de empleados, proveedores o clientes (nombres, teléfonos, correo electrónico, direcciones, datos bancarios, etc.) eres responsable del tratamiento de esos datos, ya que decides sobre las finalidades del tratamiento (¿para qué voy a utilizar los datos?) y los medios (¿cómo voy a tratar los datos?). Y tienes que aplicar la normativa de protección de datos, en particular, el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y garantía de derechos digitales (LOPDPGDD). Ten en cuenta los siguientes apartados:

1. ¿Qué datos se pueden tratar?

Decide qué datos personales necesitarás tratar para llevar a cabo tu actividad, y para qué finalidad.

La finalidad es muy importante, ya que la ley obliga al responsable a utilizar únicamente aquellos datos estrictamente necesarios para cumplir con la finalidad que determine. Y de ello dependerán las obligaciones que debas cumplir.

Más información

1. ¿Qué son [datos personales](#)?
2. ¿Cuáles son los [principios del tratamiento](#)?
3. ¿Cuáles son las [obligaciones](#) del responsable del tratamiento?

2. ¿Cuándo se pueden usar?

Antes de comenzar a tratar los datos, confirma que cuentas con una base de legitimación del tratamiento: cumplimiento de un contrato, consentimiento del titular, obligación legal, etc.

Algunos tipos de datos, como los de salud o los relativos a la vida sexual, son datos especialmente protegidos, que necesitan una habilitación para poder tratarlos.

Analiza cuál de las bases y, en su caso, de las habilitaciones es la que resulta de aplicación a tu actividad, ya que de no aplicar ninguna, no podrás tratar esa información.

Más información

4. ¿Cuáles son las [bases de legitimación](#)?

3. ¿Cómo se deben proteger?

Debes contar con medidas técnicas y organizativas que garanticen la seguridad de los tratamientos que realices.

Los datos especialmente protegidos necesitarán medidas más intensas.

Para los tratamientos que llesves a cabo deberás realizar, previamente, un análisis de riesgos o, si fuera necesario, una evaluación de impacto.

Más información

5. ¿Cuáles son las medidas de [seguridad de los tratamientos](#)?
6. ¿Cómo debo [valorar el nivel de riesgo](#)?
7. ¿Qué [herramientas de apoyo](#) puedo usar?

4. ¿Se debe informar a alguien?

Las personas titulares de los datos tienen derecho a saber qué datos tienes de ellos y qué vas a hacer con sus datos.

Y tú, como responsable del tratamiento, estás obligado a informarles de ello de forma clara antes de usar sus datos.

Más información

8. ¿Sobre qué debo [informar](#)?
9. ¿Me ofrece la AEPD [modelos de cláusulas informativas](#)?
10. Consulta la [Guía para el cumplimiento del deber de informar](#)

5. Derechos del titular

Tienes que facilitar a las personas cuyos datos tratas la posibilidad de ejercer sus derechos de protección de datos (acceso, rectificación, supresión, limitación, oposición y portabilidad), ofreciéndoles un procedimiento accesible.

Se les puede facilitar formularios claros para que puedan ejercer dichos derechos.

Más información

11. [¿Cómo se ejercen?](#)
12. [¿Qué formularios](#) puedo usar?

6. ¿Necesito un DPD?

La designación de una persona delegada de protección de datos (DPD) no es obligatoria para todas las empresas.

Te corresponde a ti determinar si, según la actividad de la entidad o los tratamientos que realizas, es necesario.

La actividad de DPD puede desarrollarse por alguien interno, con formación suficiente, o utilizar un servicio externo. Una vez designada, debe comunicarse su nombramiento a la AEPD.

Más información

13. [¿Cómo nombrar un DPD?: designación de un DPD](#)

7. ¿Qué documentación necesito?

Tienes que preparar y tener siempre a disposición una serie de documentación que acredite el cumplimiento de la normativa.

Entre otros documentos, necesitas disponer de tres documentos importantes:

- ✓ Un Registro de Actividades de Tratamiento (RAT)
- ✓ Cláusulas informativas
- ✓ Un contrato de encargo de tratamiento

Más información

15. [Registro de actividades de tratamiento](#)
16. [Cláusulas informativas de protección de datos](#)
17. [Política de privacidad](#) y [Política de cookies](#)
18. [Contrato encargado del tratamiento](#)

8. ¿Y si pasa algo?

Puede ocurrir que con ocasión del tratamiento se produzca una violación de la seguridad de los datos personales (brechas de seguridad). En ese caso, es conveniente disponer de medidas que permitan mitigar los efectos negativos.

Ciertos acontecimientos se deben notificar a las autoridades y en ocasiones a las personas afectadas por las brechas de seguridad.

Más información

19. [Plan de respuesta](#)
20. [Incidentes](#)
21. [Guía para la notificación de brechas de datos personales](#)