



ÁREA DE
CONSULTORÍA

Protección de Datos Personales y garantía de los derechos digitales

La Protección de Datos de Carácter Personal es un **derecho fundamental** tal y como se recoge en el artículo 18.4 de la Constitución Española (CE). Este derecho se traduce en la **potestad de control y uso** que poseen todas las personas sobre sus datos de carácter personal. Este control, permite evitar que a través del tratamiento de los datos personales que se realiza por parte de entidades públicas o privadas, estos puedan disponer o usar la información que poseen de tal manera que afecte a la privacidad y demás derechos fundamentales y libertades públicas, utilizándolos para una finalidad distinta que para la que fueron recogidos.

La actual normativa, **Ley Orgánica 3/2018, de Protección de datos de Carácter Personal y Garantía de los Derechos Digitales (LOPDGDD)**, aplicable desde el 25 de Mayo de 2018 y que deroga la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD), tiene por objeto adaptar y regular en nuestro ordenamiento jurídico interno lo dispuesto en el **REGLAMENTO (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD)**, por el que se deroga la Directiva 95/46/CE.

En esta pantalla podrá acceder a una práctica **ficha informativa** sobre la actual normativa de protección de datos si desea más información.





Principales **REQUISITOS**

- Análisis de Riesgos y Evaluación de Impacto en la Protección de Datos Personales (EIPD) en función del tratamiento.
- Elaboración del documento o procedimiento de seguridad e implantación de medidas de seguridad de carácter técnico, organizativo y legal en el sistema de información.
- Cumplimiento del deber de información del interesado y la obtención del consentimiento para el tratamiento de su información de carácter personal.
- Formalización de contratos de acceso a datos por cuenta de terceros (contratos de encargo de tratamiento) y contratos de prestación de servicios sin acceso a datos por terceros (contratos de confidencialidad).
- Formación del personal y responsable de la organización: personal laboral y responsable de seguridad.
- Designación del encargado de seguridad o del Delegado de Protección de Datos.
- Realización de auditorías internas como medidas de revisión y comprobación del cumplimiento.
- Elaboración del Registro de Actividades de Tratamiento (RAT)
- Aplicación del principio de responsabilidad proactiva y protección desde el diseño y por defecto.
- Bases legítimas para el tratamiento de datos personales, incluyendo los datos denominados sensibles o de riesgo alto.
- Consentimientos expresos, informados e inequívocos para cualquier tratamiento de datos personales.
- Prohibición de tratamiento de categoría de datos especiales, salvo determinadas circunstancias.
- Elección de los encargados de tratamiento que ofrezcan garantías suficientes del cumplimiento de la normativa.
- Cooperación con la Autoridad de Control Nacional (AEPD) o las autonómicas (APDCAT, AVPD o el CTPDA)

Ejemplos de **ACCIONES PRÁCTICAS A IMPLEMENTAR**

- Realizar un Análisis de Riesgos (AR) y una Evaluación de Impacto en la Protección de Datos Personales (EIPD) en función del tipo de tratamiento que se realice.
- Firma del contrato de acceso y/o tratamiento de datos, por parte de los encargos de tratamiento como asesorías, empresa de video-vigilancia, empresas de mantenimiento informático, empresas de hosting web, etc.
- Redacción de contratos de confidencialidad con proveedores que no tienen acceso directo a datos personales.
- Redacción e implantación de avisos legales, políticas de privacidad, política de cookies e información y/o consentimientos web.
- Redacción de cláusulas de protección de datos relativas a la información.
- Elaboración e implantación de un procedimiento para el ejercicio de los derechos de protección de datos (Acceso, Rectificación, Supresión o Derecho al Olvido, Limitación, Portabilidad y Oposición).
- Realización de una Auditoría interna para la verificación del cumplimiento o mejoras.
- Redacción de contratos, formularios y cláusulas necesarias para la recogida de datos, los tratamientos por terceros y las cesiones o comunicaciones de datos.
- Realización de procedimiento para las copias de seguridad o recuperación de desastres.
- Designación responsable de seguridad o Delegado de Protección de Datos.
- Comunicación del DPD en la AEPD.
- Apoyo en la gestión las incidencias detectadas en el tratamiento de datos personales.
- Firma de cláusulas de confidencialidad con el personal de la organización.



- Registro de acceso a los distintos ficheros de la empresa.
- Política de gestión de contraseñas.
- Relación actualizada de usuarios y perfiles de acceso.
- Identificación del personal externo con acceso a los datos personales.
- Identificación de soportes automatizados y no automatizados con datos personales.
- Documentación relativa a la utilización de sistemas de videovigilancia en función de su finalidad

**Las acciones indicadas son sólo ejemplos, éstas deberán ser adaptadas a la realidad y necesidades de cada organización*





Ventajas para LA ORGANIZACIÓN

- Mejora de la imagen de la empresa de cara a los clientes.
- Control eficaz sobre los datos personales tratados y almacenados en la entidad.
- Ofrece garantía de seguridad en la gestión de los datos de carácter personal.
- Evita posibles sanciones derivadas por el órgano de control, la Agencia Española de Protección de Datos (AEPD), sobre incumplimientos de la normativa.
- Ayuda a establecer pautas y medidas necesarias que de forma directa ayudan a la empresa a proteger su activo más valioso: la información y sus clientes.
- Identifica las funciones de cada individuo dentro de cada entidad, identificando los accesos permitidos a datos personales en la empresa.
- Mejor gestión de la seguridad de la información, impidiendo fugas y brechas de seguridad.
- Optimización de procesos y selección de proveedores.
- Formación y sensibilización del personal y definición de funciones y responsabilidades.
- En los casos en que aplique, nombramiento y capacitación de/de la DPD.

Ventajas para LOS CLIENTES

- Garantía de que sus datos personales son tratados con transparencia y cumpliendo con los requisitos exigidos en la normativa.
- Le ofrece una mayor confianza a la hora de contratar con la empresa.
- Certeza de que se garantiza y se le facilita el ejercicio de sus derechos.
- Percepción de que sus datos se tratan respetando su privacidad, honor e intimidad.
- Genera la confianza de estar tratando con una organización que respeta la normativa vigente, preocupándose por la calidad de sus servicios o productos.

Ventajas para EL MERCADO

Cualquier empresa que quiera diferenciarse y volverse más **competitiva** debe cumplir con ciertos estándares mínimos. El cumplimiento de la normativa de protección de datos proporciona un aumento de la **confianza** en el mercado, redundando en un mayor **prestigio** dentro del mismo ante clientes, organismos públicos u otras empresas.

La posibilidad establecida en el Reglamento General de Protección de Datos de poder **certificarse** como entidad que cumple y mantiene un compromiso con la protección de datos, mediante elementos distintivos otórganos por entidades certificadoras demuestran la importancia en el mercado de dicho cumplimiento.

Sectores DE APLICACIÓN

La normativa de protección de datos personales de 2018 **obliga a todas las entidades públicas o privadas**, independientemente del



sector y tamaño, siempre que realicen cualquier tratamiento de datos personales, bien sea de clientes, trabajadores/as, proveedores, o cualquier otra parte interesada. Nos podemos referir a: grandes empresas, PYMES, autónomos, asociaciones, ONGs, fundaciones, ayuntamientos, colegios públicos y privados, corporaciones, cooperativas, starups etc.

