



PROTECCIÓN DE DATOS PARA ENCARGADOS DEL TRATAMIENTO

¿Qué es un *dato personal*?

Dato personal es más que el nombre, apellidos, fecha de nacimiento o dirección. Se extiende a identificadores online y **todo tipo de datos que, directa o indirectamente, permitan determinar la identidad de una persona**. Por ejemplo, dirección IP, IMSI de la tarjeta SIM, o el identificador de su terminal.

Los **datos seudonimizados** también forman parte del concepto de dato personal, es decir, datos que cabría atribuir a una persona física mediante la utilización de información adicional.

También estarían sujetos a la normativa los datos biométricos (por ejemplo, la imagen, la voz o la huella de las personas) y aquellos datos personales accesibles públicamente en internet o redes sociales.

Ejemplos de datos personales:



Localización — Atributos físicos — Información económica
Cultural o social — Identificación online — IPS

Tratamiento de datos personales

Se considera tratamiento a cualquier **operación** realizada sobre datos personales, ya sea manual o automatizada. Por ejemplo: el registro de **alta** a un servicio, mero **acceso** o consulta de una base de datos, la **destrucción o borrado** de documentos con datos personales, la **modificación** de datos, la **cesión** de datos a terceros o la restricción de acceso entre otros.

Principios del tratamiento de datos personales

Cualquier tratamiento de datos personales debe respetar los principios de protección de datos.



LICITUD, LEALTAD Y TRANSPARENCIA

El tratamiento debe estar basado en una base que lo legitime, contar con una finalidad determinada y ser fiel a ese compromiso adquirido a la hora de informar.



LIMITACIÓN DE LA FINALIDAD

Compromiso de tratar la información exclusivamente para la finalidad informada.



MINIMIZACIÓN DE LOS DATOS

Se utilizarán exclusivamente los datos necesarios para la finalidad objeto del tratamiento.



EXACTITUD

Los datos personales deben ser exactos y encontrarse actualizados.



PLAZO DE CONSERVACIÓN

La información tiene que conservarse el tiempo necesario para fines los definidos.



INTEGRIDAD Y SEGURIDAD

Proteger los datos personales de cualquier riesgo manteniendo la Integridad, Disponibilidad y Confidencialidad.



RESPONSABILIDAD PROACTIVA

Mantener conciencia y cultura de privacidad cumpliendo el detalle de los principios anteriores.

Responsabilidades de los proveedores

El proveedor debe conocer sus responsabilidades en el tratamiento de la información con el objeto de garantizar la privacidad de las personas cuyos datos van a ser tratados. Los términos del servicio prestado se recogen a través de un documento contractual denominado Data Protection Agreement (DPA). Dicho documento contiene, entre otros, los siguientes compromisos:



- Tratar los datos siguiendo **instrucciones** del responsable
- **Deber de confidencialidad** de todas personas que accedan a los datos
- Garantizar el cumplimiento de las **medidas de seguridad**
- En los casos de **contratación de subencargados** por parte del proveedor, será necesaria la autorización del responsable del tratamiento
- **Ayuda** al responsable en el cumplimiento de determinadas obligaciones, siempre que apliquen al servicio prestado, como soporte en el ejercicio de derechos o comunicación en relación con incidencias de seguridad en relación al servicio provisto
- **Al finalizar la prestación del servicio**, la devolución o destrucción de datos (a elección del responsable).

