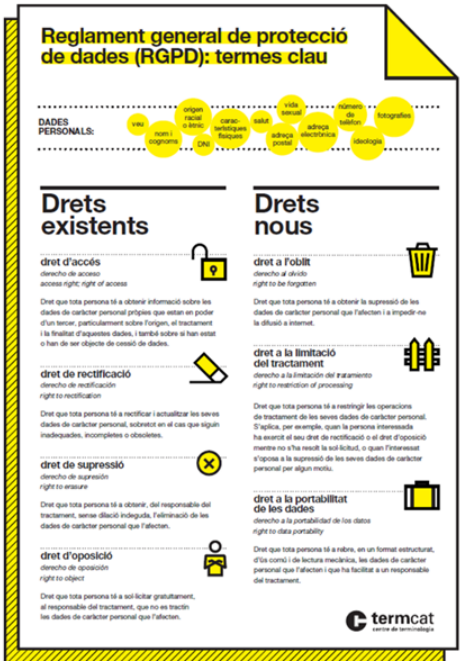
LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

¿A QUÉ NOS REFERIMOS?

Los datos de carácter personal son cualquier información referente a personas físicas identificadas o identificables. Se considera que puede ser identificable toda persona cuya identidad se pueda determinar mediante un identificador (por ejemplo: un nombre, un número de identificación, datos de localización, etc.) o mediante el uso de uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social.



La normativa diferencia dos tipos de datos personales:

. **Datos básicos no sensibles**: nombre, apellidos, domicilio, dirección electrónica, teléfono, número de identidad, cuenta bancaria, profesión, experiencia, etc.

. **Datos sensibles especialmente protegidas**: las relativas a origen étnico o racial, opiniones políticas, convicciones religiosas, datos de salud y fisiológicos, afiliación sindical o relativas a la vida u orientación sexual.

La normativa vigente incluye dos nuevas categorías especiales de datos: los datos genéticos y los datos biométricos (imágenes faciales, datos dactiloscópicos, etc.).

Las nuevas tecnologías han hecho cambiar la forma de almacenar y trabajar con los datos y han forzado a adecuar la normativa a los avances tecnológicos y a dotar la ciudadanía de un mayor control sobre el tratamiento que se hace de sus datos de carácter personal.

Las organizaciones tienen que tener una actitud responsable y proactiva ante los tratamientos de datos personales que hagan. Las asociaciones están sujetas a la Ley, ya que disponen de información de personas físicas, ya sean las propias personas asociadas o las que son sujeto de sus actuaciones.

¿CÓMO TRATAMOS LOS DATOS?

¿Qué datos tratamos?

Generalmente, la mayor parte de las asociaciones tratan datos básicos. En todo caso, es imprescindible haber informado a la persona interesada de los fines con los cuales pueden ser tratadas, quien lo hace y quien es la persona responsable. Es imprescindible, también, que la persona dé el consentimiento y que éste quede registrado.

¿Quién tiene acceso?

La persona (o personas) **responsable** de la protección de datos, que determina los fines y los medios del tratamiento y que se hace responsable de la custodia y de los permisos.

Obligaciones de la persona responsable del tratamiento:

Facilitar a la persona encargada del tratamiento el acceso a los equipos, con el fin de prestar el servicio contratado.

Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del Reglamento de Protección de Datos por parte de la persona encargada.

Supervisar el tratamiento.

La persona **encargada** del tratamiento, por ejemplo: la persona que programa la página web, la que gestiona los libros de socios o la que hace cualquier trabajo que implica utilizar los datos personales a disposición de la entidad.

Obligaciones de la persona encargada del tratamiento:

. Utilizar los datos personales a los cuales tiene acceso sólo para la finalidad autorizada. En ningún caso puede utilizarlos para fines propios.

. Tratar los datos de acuerdo con las instrucciones de la persona responsable del tratamiento.

. Informar inmediatamente a la persona responsable si la considera que alguna de las instrucciones infringe el Reglamento de Protección de Datos (RGPD) o cualquier otra disposición en la materia.

. No comunicar los datos a terceras personas, a menos que disponga de la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles.

. Mantener el deber de secreto con respecto a los datos de carácter personal a los cuales ha tenido acceso, incluso una vez finalizado el contrato.

. Garantizar que las personas autorizadas para tratar datos personales se comprometen, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes de las cuales han sido previamente informadas.

. Mantener a disposición de la persona responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.
. Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratarlas.

. Notificar las violaciones de la seguridad de los datos a la persona responsable, junto con toda la información relevante para la documentación y comunicación de la incidencia.

¿Dónde están almacenados los datos?

Por ejemplo en:

Fichas de inscripción de personas socias
Hojas de autorización de menores
Listas de asistencia
Grupos de WhatsApp
Listas de distribución de correo y correos electrónicos
Actas de asambleas

Herramientas electrónicas de uso compartido (Google Drive, Lumio...)
Documentos en el servidor del ordenador
Software que se utiliza para la gestión de personas socias
Concepto de las transferencias bancarias que van dirigidas a la entidad
Etc.

¿Qué tratamiento se hace de los datos y con qué finalidades?

¿Se pasan datos a terceros? Para la prestación de servicios como los seguros, para dirigir facturas...

¿Se guardan? ¿Dónde y cuánto tiempo?

¿Se hacen análisis o estadísticas? Para elaborar perfiles, proyectos, para comunicaciones internas, para elaborar actas...

¿Se ilustran documentos o se hace publicidad con imágenes de las personas?

La normativa establece unos principios que tienen que regular el tratamiento de los datos que, en cualquier caso, tienen que ser:

- Legalidad, lealtad y transparencia
- Los datos se tienen que recoger y tratar según los fines estipulados
- Sólo se tienen que recoger y tratar los datos imprescindibles
- Exactitud de los datos y derecho de corrección
- Durabilidad determinada: no se puede disponer eternamente de los datos facilitados
- Confidencialidad

LOS RIESGOS

El tratamiento de información implica un riesgo que puede ser bajo o alto.

La normativa no establece una lista de las medidas de seguridad a aplicar, de acuerdo con la tipología de datos objeto de tratamiento, sino que establece que las personas responsables y las encargadas del tratamiento tienen que aplicar las medidas técnicas y organizativas adecuadas al riesgo que comporta el tratamiento.

Eso implica que hay que hacer una **evaluación de los riesgos** asociados a cada tratamiento para determinar las medidas de seguridad que hay que implementar: establecer hasta qué punto una actividad de tratamiento, por sus características o por el tipo de datos que maneja, puede causar daño en los derechos y en las libertades de las personas.

Identificar el riesgo. Divulgación, destrucción, modificación... de la información.

Evaluar el riesgo. En qué contexto se puede manifestar o materializar.

Tratar el riesgo. Qué medidas adoptamos y aplicamos para que el riesgo o amenaza no se produzca.

MEDIDAS DE PROTECCIÓN

La persona responsable del tratamiento tiene que establecer procedimientos de control que garanticen cumplir los principios de protección desde el primer momento. La gestión de la protección tiene que ser útil, ágil y efectiva.

Tipología de riesgo	Riesgo	Medidas de control
Integridad de los datos personales	Modificación o alteración de datos personales no intencionada	▪ Segregación de funciones mediante perfiles de acceso ▪ Controles de monitorización de amenazas en red
Disponibilidad de los datos personales	Pérdida o borrado no intencionado de datos personales	▪ Copias de seguridad ▪ Almacenamiento en dos ubicaciones diferentes
Confidencialidad de los datos personales	Acceso no autorizado a los datos personales	▪ Mecanismos de control de acceso ▪ Segmentación de la red
Garantizar el ejercicio de los derechos de los interesados	Ausencia de procedimientos para el ejercicio de derechos	▪ Procedimientos y canales para el ejercicio de derechos
Garantizar los principios relativos al tratamiento	Ausencia de legitimidad para el tratamiento de los datos personales	▪ Cláusulas informativas y base legitimadora para el tratamiento de datos
	Tratamiento ilícito de datos personales	▪ Monitorización del uso de datos personales

Medidas básicas

- Asegurar que cuando se cierra el ordenador se cierren las sesiones abiertas.
- Controlar las contraseñas.
- Eliminar los accesos a personas una vez se desvinculan de la entidad.
- Guardar los datos sensibles en documentos con contraseña.
- Guardar la documentación en un lugar determinado y seguro y fuera del acceso al público.
- Asegurar que nadie deposite datos personales en lugares visibles y desprotegidos o que se comenten en voz alta.
- No compartir ni dejar móviles que contengan datos.
- Controlar los accesos a las bases de datos.
- Controlar qué ficheros se comparten y con quien.
- Eliminar datos innecesarios.
- Cifrar los documentos que se envíen.
- Configurar correctamente las opciones de privacidad y seguridad.
- Utilizar contraseñas seguras.
- Hacer copias de seguridad en soportes alternativos y almacenadas en entornos seguros.

PROTOCOLOS

Para tratar datos de personas físicas hace falta que la persona interesada los haya facilitado y autorice el almacenaje y la utilización exclusivamente para los fines manifestados.

El consentimiento se puede expresar bajo la fórmula de **aviso legal, cláusula informativa o política de privacidad**. Este documento o texto es un acuerdo entre dos partes, por lo que se tiene que haber firmado. En caso de recoger datos de menores, el consentimiento lo da el titular de la patria potestad o de la tutela sobre el niño.

IMPORTANTE

Se tiene que dar toda la información a la persona interesada en el momento en que se solicitan sus datos, con un lenguaje claro y sencillo, de manera concisa, transparente e inteligible

Hay otros protocolos, como el **registro de actividades de seguridad** o **la evaluación de impacto (AIPD)**, pero, generalmente, la mayoría de asociaciones no tienen la obligación de tenerlos.

Son preceptivos cuando se manejan datos sensibles o a gran escala, cuando las consecuencias del tratamiento pueden tener alcance legal o económico, cuando los datos se manipulan constantemente, los utilizan muchas personas o si los fines del tratamiento implican, por ejemplo, la toma de decisiones importantes, relacionadas con la salud, etc.

Es decir, hay que hacer una AIPD cuando un tratamiento puede suponer un riesgo alto para los derechos y las libertades de las personas físicas, especialmente (pero no exclusivamente) si se utilizan nuevas tecnologías y teniendo en cuenta la naturaleza, el alcance, el contexto o las finalidades del tratamiento. En aquellos casos en que no está clara la necesidad o no de llevar a cabo una AIPD, es recomendable hacerla.

La Agencia Española de Protección de Datos dispone de una serie de herramientas para cumplimentar estos protocolos:

https://www.aepd.es/sites/default/files/2019-09/guia-analisis-de-riesgos-rgpd.pdf

DATOS Y DOCUMENTOS DE INTERÉS

Agencia Española de Protección de Datos::

https://www.aepd.es/es

Reglamento (UE 2016/679) del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas, por lo que respecta al tratamiento de datos personales y a su libre circulación:

https://www.boe.es/doue/2016/119/L00001-00088.pdf

Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales:

https://www.boe.es/boe_catalan/dias/2018/12/06/pdfs/BOE-A-2018-16673-C.pdf