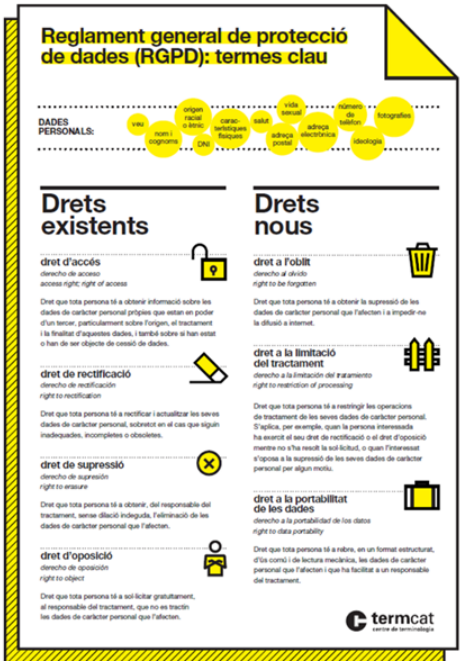
LA PROTECCIÓ DE DADES

A QUÈ ENS REFERIM?



Les dades de caràcter personal són qualsevol informació referent a persones físiques identificades o identificables. Es considera que pot ser identificable tota persona la identitat de la qual es pugui determinar mitjançant un identificador (per exemple: un nom, un número d'identificació, dades de localització, etc.) o mitjançant l'ús d'un o diversos elements propis de la identitat física, fisiològica, genètica, psíquica, econòmica, cultural o social.

La normativa diferencia dos tipus de dades personals:

• **Dades bàsiques no sensibles**: nom, llinatges, domicili, adreça electrònica, telèfon, número d'identitat, compte bancari, professió, experiència, etc.

• **Dades sensibles especialment protegides**: les relatives a origen ètnic o racial, opinions polítiques, conviccions religioses, dades de salut i fisiològiques, afiliació sindical o relatives a la vida o orientació sexual.
La normativa vigent inclou dues noves categories especials de dades: les dades genètiques i les dades biomètriques (imatges facials, dades dactiloscòpiques, etc.).

Les noves tecnologies han fet canviar la forma d'emmagatzemar i treballar amb les dades i han forçat a adequar la normativa als avenços tecnològics i a dotar la ciutadania d'un control major sobre el tractament que es fa de les seves dades de caràcter personal.

Les organitzacions han de tenir una actitud responsable i proactiva davant els tractaments de dades personals que facin. Les associacions estan subjectes a la Llei, ja que disposen d'informació de persones físiques, ja siguin les pròpies persones associades o les que són subjecte de les seves actuacions.

COM TRACTAM LES DADES

Quines dades tractam?

Generalment, la major part de les associacions tracten dades bàsiques. En tot cas, és imprescindible haver informat la persona interessada dels fins amb els quals poden ser tractades, qui ho fa i qui és la persona responsable. És imprescindible, també, que la persona doni el consentiment i que aquest quedi registrat.

Qui hi té accés?

- La persona (o persones) **responsable** de la protecció de dades, que determina els fins i els mitjans del tractament i que es fa responsable de la custòdia i dels permisos.

Obligacions de la persona responsable del tractament:

- Facilitar a la persona encarregada del tractament l'accés als equips, a fi de prestar el servei contractat.
- Vetllar, de forma prèvia i durant tot el tractament, pel compliment del RGPD per part de l'encarregat.
- Supervisar el tractament.

- La persona **encarregada** del tractament, per exemple: la persona que programa la pàgina web, la que gestiona els llibres de socis o la que fa qualsevol feina que implica utilitzar les dades personals a disposició de l'entitat.

Obligacions de la persona encarregada del tractament:

• Utilitzar les dades personals a les quals té accés només per a la finalitat autoritzada. En cap cas pot utilitzar-les per a fins propis.

• Tractar les dades d'acord amb les instruccions de la persona responsable del tractament.

• Informar immediatament la persona responsable, si la persona encarregada del tractament considera que alguna de les instruccions infringeix el RGPD o qualsevol altra disposició en matèria de protecció de dades.

• No comunicar les dades a terceres persones, llevat que disposi de l'autorització expressa del responsable del tractament, en els supòsits legalment admissibles.

• Mantenir el deure de secret respecte a les dades de caràcter personal a les quals ha tingut accés, fins i tot una vegada finalitzat el contracte.

• Garantir que les persones autoritzades per tractar dades personals es comprometen, de forma expressa i per escrit, a respectar la confidencialitat i a complir les mesures de seguretat corresponents de les quals han estat prèviament informades.

• Mantenir a disposició de la persona responsable la documentació acreditativa del compliment de l'obligació establerta en l'apartat anterior.

• Garantir la formació necessària en matèria de protecció de dades personals de les persones autoritzades per tractar-les.

• Notificar les violacions de la seguretat de les dades a la persona responsable, juntament amb tota la informació rellevant per a la documentació i comunicació de la incidència.

On estan emmagatzemades les dades?

Per exemple:

- Fitxes d'inscripció de persones sòcies
- Fulls d'autorització de menors
- Llistes d'assistència
- Grups de WhatsApp
- Llistes de distribució de correu i correus electrònics

- Actes d'assemblees
- Eines electròniques d'ús compartit (Google Drive, Lumio...)
- Documents en el servidor de l'ordinador
- Programari que s'utilitza per a la gestió de persones sòcies
- Concepte de les transferències bancàries que van dirigides a l'entitat
- Etc.

Quin tractament es fa de les dades i amb quines finalitats?

Es passen dades a tercers? Per a la prestació de serveis com les assegurances, per dirigir factures...
Es guarden? On i quant de temps?
Es fan anàlisis o estadístiques? Per elaborar perfils, per elaborar projectes...?
Per a comunicacions internes, per elaborar actes...?
S'il·lustren documents o es fa publicitat amb imatges de les persones?

La normativa estableix uns principis que han de regular el tractament de les dades que, en qualsevol cas, han de ser:

- Legalitat, lleialtat i transparència
- Les dades s'han de recollir i tractar segons els fins estipulats
- Només s'han de recollir i tractar les dades imprescindibles
- Exactitud de les dades i dret de correcció
- Durabilitat determinada: no es pot disposar eternament de les dades facilitades
- Confidencialitat

ELS RISCOS

El tractament d'informació implica un risc que pot ser baix o alt.

La normativa no estableix una llista de les mesures de seguretat a aplicar, d'acord amb la tipologia de dades objecte de tractament, sinó que estableix que les persones responsables i les encarregades del tractament han d'aplicar les mesures tècniques i organitzatives adequades al risc que comporta el tractament.

Això implica que cal fer una **avaluació dels riscos** associats a cada tractament per determinar les mesures de seguretat que cal implementar: establir fins a quin punt una activitat de tractament, per les seves característiques o pel tipus de dades que maneja, pot causar dany en els drets i en les llibertats de les persones. Per a això, hem de:

Identificar el risc.: de divulgació, destrucció, modificació ... de la informació.

Avaluar el risc.: en quin context es pot manifestar o materialitzar.

Tractar el risc: quines mesures adoptam i aplicam perquè el risc o amenaça no es produeixin.

MESURES DE PROTECCIÓ

La persona responsable del tractament ha d'establir procediments de control que garanteixin complir els principis de protecció des del primer moment. La gestió de la protecció ha de ser útil, àgil i 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

Mesures bàsiques:

- Assegurar que quan es tanca l'ordinador es tanquen les sessions obertes.
- Controlar les contrasenyes.
- Eliminar els accessos a persones un cop es desvinculen de l'entitat.
- Guardar les dades sensibles en documents amb contrasenya.
- Tancar la documentació en un lloc determinat i segur i fora de l'accés al públic.
- Assegurar que ningú escriu dades personals en llocs visibles i desprotegits o que es comenten en veu alta.
- No compartir ni deixar mòbils que contenguin dades.
- Controlar els accessos a les bases de dades.
- Controlar quins fitxers es comparteixen i amb qui.
- Eliminar dades innecessàries.
- Xifrar els document que s'envien.
- Configurar correctament les opcions de privacitat i seguretat.
- Utilitzar contrasenyes segures.
- Fer còpies de seguretat en suports alternatius i emmagatzemades en entorns segurs.

PROTOCOLS

Per tractar dades de persones físiques cal que la persona interessada les hagi facilitat i n'autoritzi l'emmagatzematge i la utilització exclusivament per als fins manifestats.

El consentiment es pot expressar sota la fórmula d'**avís legal, clàusula informativa o política de privacitat**. Aquest document o text és un acord entre dues parts, per tant s'ha d'haver firmat. En cas de recollir dades de menors, el consentiment el dóna el titular de la pàtria potestat o de la tutela sobre l'infant.

IMPORTANT

S'ha de donar tota la informació a la persona interessada en el moment en què se sol·liciten les seves dades, amb un llenguatge clar i senzill, de manera concisa, transparent, intel·ligible i d'accés fàcil.

Hi ha altres protocols, com el **registre d'activitats de seguretat** o **l'avaluació d'impacte (AIPD)** però, generalment, la majoria d'associacions no tenen l'obligació de tenir-los.

Són preceptius quan es manegen dades sensibles o a gran escala, quan les conseqüències del tractament poden tenir abast legal o econòmic, quan les dades es manipulen constantment, les utilitzen moltes persones o si els fins del tractament impliquen, per exemple, la presa de decisions importants, relacionades amb la salut, etc.

És a dir, cal fer una AIPD quan un tractament pot suposar un risc alt per als drets i les llibertats de les persones físiques, especialment (però no exclusivament) si s'utilitzen noves tecnologies, i tenint en compte la naturalesa, l'abast, el context o les finalitats del tractament. En aquells casos en què no està clara la necessitat o no de dur a terme una AIPD, és recomanable fer-la.

L'Agència Espanyola de Protecció de Dades disposa d'un seguit d'eines per fer aquests protocols:
https://www.aepd.es/sites/default/files/2019-09/guia-analisis-de-riesgos-rgpd.pdf

DADES I ADRECES D'INTERÈS

Agència Espanyola de Protecció de Dades:
https://www.aepd.es/es

Reglament (UE 2016/679) del Parlament Europeu i del Consell de 27 d'abril de 2016 relatiu a la protecció de les persones físiques, pel que respecta al tractament de dades personals i a la seva lliure circulació:
https://www.boe.es/doue/2016/119/L00001-00088.pdf

Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals:
https://www.boe.es/boe_catalan/dias/2018/12/06/pdfs/BOE-A-2018-16673-C.pdf