# Protecció de dades

## Gestió legal, fiscal i comptable

Centre de Recursos per a les Associacions Juvenils de Barcelona

**Juliol 2018**

**Fitxa temàtica 27**

*"La llei de protecció de dades pretén protegir tot allò referent al tractament de dades personals, les llibertats públiques i els drets fonamentals de les persones, especialment l'honor i la intimitat personal i familiar."*

### 1. Introducció legal

A Europa tenim un nou **Reglament General de Protecció de Dades** que pretén unificar la legislació entorn a la privacitat de les dades dels diversos estats membres de la Unió Europea, ja que fins ara cada país tenia la seva pròpia regulació.
Les noves tecnologies han fet canviar la forma d'emmagatzemar i treballar amb les dades, de manera que ha forçat a adequar la normativa als avenços tecnològics i dotar la ciutadania d'un major control sobre el tractament que es fa de les dades de caràcter personal.

El 25 de maig del 2018 entra en vigor el Reglament (UE 2016/679) del Parlament Europeu i del Consell de 27 d'abril de 2016 relatiu a la protecció de les persones físiques en el que respecta al tractament de dades personals i a la seva lliure circulació. Aquest fet fa que la **Llei orgànica 15/1999 de protecció de dades de caràcter personal (LOPD)** i el seu Reglament de desenvolupament (RLOPD) així com la Directiva 95/46/CE deixen de tenir vigència.

En aquesta Fitxa temàtica es tractaran els diferents aspectes que consten en el RGPD seguint el **següent esquema:**

- Objectius de la llei de protecció de dades
- A qui afecta aquesta normativa
- Quines són les dades personals?
- Quins són els drets que tenen les persones que cedeixen dades personals?
- L'avaluació de riscos: com apliquem un mètode per evitar fugues de dades

1. De quines dades disposem?
2. Qui en té accés?
3. On estan emmagatzemades les dades?
4. Es fa tractament de les dades i quina és la finalitat?
5. En tenim consentiment explícit?
6. Clàusula de sol·licitud de dades personals
7. Política de privacitat visible
8. Com analitzem les possibles fugues de dades personals?
9. És obligatori redactar un registre d'activitats de seguretat?
10. Cal redactar una avaluació d'impacte?

- Webs d'interès

## 2. Objectius de la llei de protecció de dades

El **Reglament General de Protecció de dades (RGPD)** pretén protegir tot allò que fa referència al **tractament de dades personals, les llibertats públiques i els drets fonamentals de les persones,** especialment l'honor i la intimitat personal i familiar. Per aquest motiu, el nou reglament garanteix el dret a controlar què es fa amb les nostres dades, saber qui té informació sobre nosaltres i de quin tipus, d'on l'ha obtingut, amb quina finalitat i si té intenció de facilitar-les a un tercer.

Aquest nou reglament té **l'objectiu** de:
• Protegir la privadesa de les persones.
• Donar transparència al tractament de dades i possibilitar l'oposició o correcció.
• Regular el lliure moviment de dades a Europa.

A més, el nou RGPD permet que la ciutadania i també els i les responsables establertes en diferents estats membres o que facin tractaments que afecten diferents estats membres tinguin una única autoritat de protecció de dades com a interlocutora a tot Europa.

**Principi de responsabilitat proactiva**

El principi de responsabilitat proactiva és un dels elements clau de la nova normativa. Aquest principi estableix que **els i les responsables del tractament ha d'aplicar mesures tècniques i organitzatives apropiades, a fi de garantir i poder demostrar que el tractament és conforme al Reglament.**

En termes pràctics, aquest principi requereix que les organitzacions analitzin quines dades tracten, amb quines finalitats ho fan i quin tipus de tractament duen a terme i millorar-ne la seva custòdia.

Així mateix, s'han d'assegurar que aquestes mesures de custòdia i de tractament són les adequades i que poden demostrar-ne el compliment davant les persones que ens han cedit dades (d'ara en endavant interessades) i davant les autoritats de supervisió.

En síntesi, aquest principi e**xigeix que les organitzacions tinguin una actitud conscient, diligent i proactiva** davant de tots els tractaments de dades personals que duguin a terme.

L'aplicació de les mesures previstes per l'RGPD **s'ha d'adaptar a les característiques de les organitzacions.** Aquelles organitzacions que manegen dades de milions de persones interessades a través de tractaments complexos que involucren informació personal sensible o volums importants de dades hauran de fer un esforç més important per adaptar-se a la nova normativa. En canvi, les organitzacions que duen a terme un tractament d'un volum limitat de dades no sensibles hauran d'efectuar modificacions menors.

D'acord amb aquest enfocament, algunes de les mesures que l'RGPD estableix només s'han d'aplicar quan hi hagi un alt risc per als drets i les llibertats, mentre que d'altres s'han de modular d'acord amb el nivell i tipus de risc que presentin els tractaments.

Per tant, l'aplicació de les mesures previstes per l'RGPD s'ha d'adaptar a les característiques de les organitzacions.
A destacar que l'RGPD suprimeix, **a partir del 25 de maig de 2018,** la necessitat de crear formalment els fitxers i notificar-los al registre de protecció de dades de les autoritats de control. Això no vol dir que no tinguem responsabilitats en relació les dades!

## 3. A qui afecta aquesta normativa?

La normativa afecta tan a totes aquelles organitzacions i persones físiques com empreses, entitats socials, comunitats de veïns, organismes públics, botigues, etc. que en definitiva facin recollida i tractament de dades referents a les persones físiques.

Les associacions, en tant que obligades a mantenir actualitzat, entre d'altres documents, un llibre registre de persones sòcies i de voluntariat **(article 313-3.2 del Llibre III del Codi Civil de Catalunya)**, ja estan sota el ventall de subjecció a la

Llei de protecció de dades, ja que disposa d'informació de persones físiques.

L'Agència Espanyola de Protecció de Dades ha dissenyat una eina d'ajuda per a organitzacions que realitzin un tractament de dades personals d'escàs risc per al compliment del Reglament General de Protecció de Dades que ajuda a conèixer si la normativa afecta a l'organització en un baix grau (havent d'aplicar les directives bàsiques) o si afecta de forma intensa (havent de dissenyar una anàlisi de l'impacte, un registre d'activitats i altres documents especificats al RGPD).

L'eina s'anomena **Facilita RGPD** i funciona com un recurs útil per a qualsevol empresa o professional. Amb tan sol tres pantalles de preguntes molt concretes permet a qui la utilitza valorar la seva situació respecte del tractament de dades personals i genera diversos documents adaptats a l'organització concreta: les clàusules informatives que ha d'incloure en els seus formularis de recollida de dades personals, les clàusules contractuals per annexar als contractes d'encarregat de tractament, el registre d'activitats de tractament i un annex amb mesures de seguretat orientatives considerades mínimes, textos que s'aniran detallant al llarg del document.

Aquí es facilita l'enllaç a un tutorial: **Tutorial Facilita RGPD**

## 4. Quines són les dades personals?

Les dades de caràcter personal són qualsevol informació concernent a persones físiques identificades o identificables, tant les bàsiques com les especialment protegides:

• **Dades bàsiques no sensibles:** nom, cognoms, adreça postal, adreça electrònica, telèfon, D.N.I., compte bancari, professió, experiència, etc.
• **Dades especialment protegides sensibles:** ideologia, religió i creences, orígens, salut (malalties i al·lèrgies), etc. Totes aquelles dades que puguin determinar el nivell socio-econòmic o un perfil que pugui avaluar determinats aspectes de les persones (per exemple, un informe mèdic).

* A part de les dades especialment protegides que ja preveia l'LOPD, que ara passen a anomenar-se **"categories especials de dades",** el Reglament inclou dues noves categories especials de dades: **les dades genètiques i dades biomètriques** (imatges facials, dades dactiloscòpiques, etc.).

## 5. Quins són els drets que tenen les persones que cedeixen dades personals?

L'anterior Llei Orgànica 15/1999, de 13 de desembre, de Protecció de dades de caràcter personal (LOPD), recollia els anomenats drets ARCO; drets d'accés, rectificació, cancel·lació i oposició. Ara el RGPD inclou, a més, el dret a l'oblit i a la portabilitat de dades.

Aquests drets pretenen garantir que les persones usuàries, consumidores, o qualsevol ens pugui tenir el control sobre les seves dades, quan aquestes estiguin en mans d'altres persones o empreses.
La vulneració d'aquests drets pot portar a la obligació de pagar indemnització pels perjudicis que se li ocasionin.
A continuació farem una breu exposició sobre cadascun d'aquests drets:

### Dret d'accés a la informació

Mitjançant aquest dret, les persones usuàries tenen la capacitat de dirigir-se als i les responsables d'un fitxer (una empresa per exemple) i sol·licitar a aquest que informi sobre quines dades té aquesta empresa en el seu poder, des de quan, per a què s'estan utilitzant i qualsevol altra informació relativa a les dades.

### Dret de rectificació

És el dret que tota persona usuària disposa per sol·licitar als i les responsables d'un fitxer que modifiqui les dades personals en la seva propietat per tal de garantir l'ús correcte de les dades.

### Dret de cancel·lació

Aquest dret faculta un usuari a sol·licitar que les dades personals que constin en propietat d'una persona responsable d'un fitxer siguin eliminats permanentment, sempre que aquestes siguin inadequades o excessives (és a dir que no siguin pertinents per a la finalitat per a la qual es van recollir).

### Dret d'oposició

Potser el més exercit de tots. Aquest dret permet al consumidor i/o usuari sol·licitar als i les responsables d'un fitxer que deixi de disposar les seves dades personals quan es tractin sense consentiment (adquirits de fonts accessibles al públic, per exemple) i quan aquests s'estiguin utilitzant amb fins comercials o qualsevol altre fi pel que no s'hagi consentit.

El RGPD incorpora el dret a l'oblit, el dret a la limitació del tractament i  al dret a la portabilitat.

### Dret a l'oblit

Els interessats tenen dret a obtenir la supressió de les dades ("dret a l'oblit"), quan:

- Les dades ja no són necessàries per a la finalitat per a la qual es van recollir.
- Es revoca el consentiment en el qual es basava el tractament.
- L'interessat s'oposa al tractament.
- Les dades s'han tractat il·lícitament.
- Les dades s'han de suprimir per complir una obligació legal.
- Les dades s'han obtingut en relació amb l'oferta de serveis de la societat de la informació adreçada a menors.

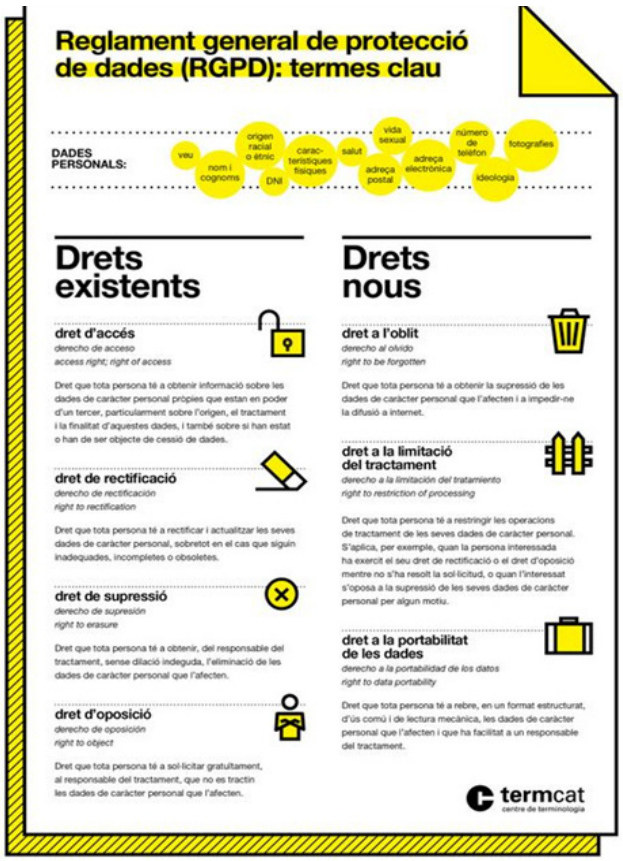
Quan la persona responsable ha fet públiques les dades personals i s'han de suprimir, ha d'adoptar mesures raonables per informar de la supressió els i les responsables que estan tractant les dades.

### Dret a la limitació

És un dret de la persona interessada consistent a marcar les seves dades de caràcter personal conservades, amb la finalitat de limitar-ne el tractament en el futur.

### Dret a la portabilitat de les dades

Es refereix a la cessió de les dades obtingudes en un format estructurat, d'ús comú i de lectura mecànica, a una altra persona responsable. Aquest dret s'exerceix sempre hi quan el tractament estigui basat en el consentiment de la persona interessada o mitjançant un contracte entre les parts. Vegeu un resum dels diferents drets que designa el RGPD (Font: Termcat, Centre de terminologia):



## 6. L'avaluació de riscos: com apliquem un mètode per evitar fugues de dades

Per aplicar la llei correctament, cal designar una persona que haurà d'assegurar que es duen a terme les accions necessàries per complir amb les noves obligacions, aquesta persona se la denomina com a persona responsable de la protecció de dades. Malgrat calgui designar una persona encarregada, tothom n'ha de ser responsable del seu compliment.

Els passos a seguir que us recomanem per assegurar complir el RGPD són els següents:

1.- De quines dades disposem?

Ser conscient del tipus de dades que l'entitat té al seu abast:

• Analitzar de quins grups es disposa de les seves dades (persones sòcies, persones voluntàries, simpatitzants, clients, etc.),
• De quina tipologia són les dades que es mouen des de l'entitat (noms i cognoms, DNIs, edats, correus electrònics, telèfons),
• De quin tipus són (si són sensibles o no) per tal d'aplicar mesures més segures o no.

Cal avaluar si el fet de disposar de certes dades, una vegada fet l'anàlisi, ens és completament útil per a la nostra entitat, o si no són en realitat necessàries, i quin perjudici provocaria en l'entitat el fet d'eliminar-les.

2.- Qui en té accès?

Caldrà avaluar les persones de l'entitat que hi tenen accés i a través de quins canals, i reiterem, si realment es necessari que en tinguin accés. S'analitzaran els accessos a les dades de persones sòcies, junta directiva, usuàries, etc.

El RGPD anomena diferents figures en la gestió de la protecció de dades que segur que hi tindran accés:

• **Persona responsable de la Protecció de Dades:** aquella persona que, sola o juntament amb altres, determini els fins i mitjans del tractament de les dades, i que es fa responsable de la custòdia i dels permisos a gestionar per part de les interessades.

• **Persona delegada de Protecció de Dades:** persona treballadora, sòcia de l'entitat o contractada per a tal fi, que informa i assessora la persona responsable, a l'encarregat i a altres empleats sobre les obligacions del RGPD i supervisa el seu compliment, cooperant i actuant com a punt de contacte amb les autoritats de control. Aquesta figura tan sols serà obligatòria en organitzacions amb més de 250 treballadores.

• **Persona encarregada de tractament:** persona que tracta dades personals per compte del responsable del tractament, com per exemple la persona que treballa en l'empresa que treballa per l'entitat programant la pàgina web o qualsevol altra organització proveïdora que utilitzi les dades personals a disposició de l'entitat. Per assegurar que no s'utilitzen per a cap altre fi, caldrà complimentar un contracte de confidencialitat.

El contracte de confidencialitat:

Caldrà firmar un contracte de confidencialitat amb la persona encarregada de dades com a membre de les organitzacions col·laboradores (proveïdors, talleristes, assessores, personal d'informàtica, persones treballadores...) que utilitzen les dades per tal d'assegurar que en facin un bon ús.

El contracte de confidencialitat haurà d'incloure **les següents clàusules contractuals**:

*1. Objecte de l'encàrrec del tractament*

Mitjançant les presents clàusules s'habilita a (Nom organització), com a encarregat del tractament, per tractar per compte d'Associació X, en qualitat de persona responsable del tractament, les dades de caràcter personal necessàries per a

prestar el servei que d'ara endavant s'especifiquen.

El tractament consistirà en (servei que us presta).

*2. Identificació de la informació afectada*

Per a l'execució de les prestacions derivades del compliment de l'objecte d'aquest encàrrec, la (Associació X) com a persona responsable del tractament, posa a disposició de (Nom organització) la informació disponible en els equips informàtics que donen suport als tractaments de dades realitzats per la persona responsable.

*3. Durada*

El present acord té una durada de (temps que es defineixi).
Un cop finalitzi el present contracte, l'encarregat del tractament ha de tornar a la persona responsable les dades personals, i suprimir qualsevol còpia que mantingui en el seu poder. No obstant, podrà mantenir bloquejats les dades per atendre possibles responsabilitats administratives o jurisdiccionals.

*4. Obligacions de l'encarregat del tractament*

L'encarregat del tractament i tot el seu personal s'obliga a:

• Utilitzar les dades personals a les quals tingui accés només per a la finalitat objecte d'aquest encàrrec. En cap cas podrà utilitzar les dades per a fins propis.

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

• Si l'encarregat del tractament considera que alguna de les instruccions infringeix el RGPD o qualsevol altra disposició en matèria de protecció de dades, l'encarregat d'informar immediatament a la persona responsable.

• No comunicar les dades a terceres persones, llevat que compti amb 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 hagi tingut accés en virtut del present encàrrec, fins i tot després que finalitzi el contracte.

• Garantir que les persones autoritzades per tractar dades personals es comprometin, de forma expressa i per escrit, a respectar la confidencialitat i a complir les mesures de seguretat corresponents, de les que cal informar-los convenientment.

• 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 dades personals.

• Notificació de violacions de la seguretat de les dades

• L'encarregat del tractament ha de notificar a la persona responsable del tractament, sense dilació indeguda i a través de l'adreça de correu electrònic que li indiqui el la persona responsable, les violacions de la seguretat de les dades personals al seu càrrec de les quals tingui coneixement, juntament amb tota la informació rellevant per a la documentació i comunicació de la incidència.

**• Es facilitarà, com a mínim, la informació següent:**

a) Descripció de la naturalesa de la violació de la seguretat de les dades personals, fins i tot, quan sigui possible, les categories i el nombre aproximat d'interessats afectats, i les categories i el nombre aproximat de registres de dades personals afectats.

b) Dades de la persona de contacte per a més informació.
c) Descripció de les possibles conseqüències de la violació de la seguretat de les dades personals. Descripció de les mesures adoptades o propostes per posar remei a la violació de la seguretat de les dades personals, incloent-hi, si escau, les mesures adoptades per mitigar els possibles efectes negatius.

• Si no és possible facilitar la informació simultàniament, i en la mesura que no ho sigui, la informació es facilitarà de manera gradual sense dilació indeguda.

• Posar disposició de la persona responsable tota la informació necessària per demostrar el compliment de les seves obligacions, així com per a la realització de les auditories o les inspeccions que realitzin la persona responsable o un altre auditor autoritzat per ell.

• Auxiliar la persona responsable de tractament a implantar les mesures de seguretat necessàries per a:
a) Garantir la confidencialitat, integritat, disponibilitat i resiliència permanents dels sistemes i serveis de tractament.
b) Restaurar la disponibilitat i l'accés a les dades personals de forma ràpida, en cas d'incident físic o tècnic.
c) Verificar, avaluar i valorar, de manera regular, l'eficàcia de les mesures tècniques i organitzatives implantades per garantir la seguretat del tractament.

• Destinació de les dades:
El o la responsable del tractament no conservarà dades de caràcter personal relatives als tractaments de l'encarregat llevat que sigui estrictament necessari per a la prestació del servei, i només durant el temps estrictament necessari per a la seva prestació.

*5. Obligacions de la persona responsable del tractament*

Correspon a aquesta el tractament següent:
a) Facilitar a l'encarregat l'accés als equips a fi de prestar el servei contractat.
b) Vetllar, de forma prèvia i durant tot el tractament, pel compliment del RGPD per part de l'encarregat.
c) Supervisar el tractament.

### 3. On estan emmagatzemades les dades?

En segon lloc s'estudiarà on queden emmagatzemades les dades de caràcter personal. A continuació es faciliten alguns exemples per a ajudar a fer-ne l'estudi:

• fitxes d'inscripció de persones sòcies
• fulls d'autorització de menors
• llistes d'assistència
• grup compartit de whatsapp
• llistes de distribució de correu
• actes de les assemblees
• correu electrònic, guardades en el text d'un correu.
• Google drive (o altre eines d'ús compartit)
• document de càlcul en el servidor de l'ordinador de presidència/secretaria
• programari/software que s'utilitza per a la gestió de persones sòcies
• concepte de les transferències bancaries que van dirigides a l'entitat
• post-its a les taules
• etc.

Caldrà posar mesures de control, sobretot si estem fent ús de noves tecnologies que són especialment invasives en termes de privacitat. Caldrà comprovar què inclouen a la seva política de privacitat.

### 4. Es fa tractament de les dades i quina és la finalitat?

Ja ha arribat el moment, un cop analitzades les dades personals de que disposa l'entitat, de saber on s'emmagatzemen, caldrà reconèixer si se'n fa un tractament o no i quin, que és del què tracta bàsicament el RGPD:

L'objecte del RGPD és **fer complir l'obligació d'informar les persones interessades,** en virtut del principi de transparència, sobre les circumstàncies i condicions del tractament de dades a efectuar, així com dels drets que els assisteixen.

### Tractament de dades

Fer un anàlisi del tractament que se'n fa vol dir: veure si s'utilitzen les dades i es faciliten a altres organitzacions o persones per a la consecució dels objectius de l'entitat, com per exemple:
- es passen dades a altres entitats
- es guarden al servidor i després es guarden en un servidor extern
- es realitzen anàlisis de les dades per a fer estadístiques
- es faciliten a terceres persones com proveïdors, persones usuàries
- etc.

### La finalitat del tractament

També s'analitzarà la finalitat de conservar i tractar les dades personals, caldrà fer-ne un anàlisis, i les finalitats podrien ser:
- presa de decisions
- elaboració de perfils
- prestació de serveis
- facturació
- enviament de publicitat postal o per correu electrònic
- servei postvenda i fidelització
- etc.

Caldrà definir exactament les finalitats perquè és obligatori que la persona interessada hagi donat el permís per al tractament de dades per a les finalitats que se li han informat, no per altres.

Des del CRAJ us oferim aquesta senzilla eina d'auto-anàlisis amb un exemple pràctic per a una millor comprensió:

| Persones de qui disposem dades | Canal d'obtenció de dades | Dades no sensibles | Dades sensibles | Dades innecessàries | Qui hi té accés | On estan emmagatzemades les dades | Se'n fa tractament? |
|---|---|---|---|---|---|---|---|
| Persones sòcies | Formulari web | Nom cognoms<br>DNI<br>Adreça<br>Data de naixement<br>Telèfon de contacte<br>Correu electrònic<br>Xarxes socials | | DNI<br>Malalties | Junta directiva | Google drive (llibre de persones sòcies) | Per a contractació d'una assegurança<br>Llistes d'assistència<br>Actes d'assemblees i reunions<br>Enviament del butlletí electrònic<br>Posts a les xarxes socials |
| Junta directiva | | | | - | | | |
| Antigues persones sòcies | | | | Nom cognoms<br>DNI<br>Adreça<br>Data de naixement<br>Telèfon de contacte | | Llibre de persones sòcies a casa de presidència | NO |
| Professorat i educadors socials | Per correu electrònic | | CV | Data de naixement | | Correu gmail de diferents persones sòcies | Enviament de correus i trucades per organitzar activitats |
| Clientela i persones usuàries | | | Malalties<br>Al·lèrgies<br>etc. | DNI | Persones sòcies<br>Persones sòcies | | Enviament d'informació sobre activitats<br>Posts a les xarxes socials |
| Altres persones col·laboradores i voluntàries | | | | DNI<br>Adreça<br>Data de naixement<br>Telèfon | | | |
| Etc. | | | | | | | |

### 5. - En tenim consentiment explícit?

Caldrà assegurar-se que sempre es disposa del **consentiment corresponent** per poder tractar les dades de les persones interessades doncs és obligatori informar a les persones interessades sobre les circumstàncies relatives al tractament de les seves dades.

Per a tractar dades de persones físiques cal que l'interessat hagi prestat el seu consentiment per facilitar les seves dades, n'autoritzi el seu emmagatzematge i la seva utilització pel la persona responsable del fitxer i exclusivament per als fins manifestats.

En cas que aquestes dades es cedeixin o comuniquin a un tercer (una persona diferent del la persona responsable del fitxer), l'interessat haurà d'autoritzar-ho.

Les dades tractades no poden ser usades **mai per a finalitats incompatibles amb aquelles per a les quals han estat recollides.** Han de ser dades exactes i actualitzades, de manera que responguin a la situació actual de l'afectat, i han de ser cancel·lades quan hagin deixat de ser pertinents per a la finalitat per la qual han estat recollides.
Aquest consentiment pot ser autoritzat mitjançant un avís legal o clàusula informativa o l'acceptació de la política de privacitat per part de l'interessat.

Els procediments de recollida d'informació poden ser molt variats i, en conseqüència, les maneres d'informar a les persones interessades s'han d'adaptar a les circumstàncies de cada un dels mitjans emprats per a la recopilació o registre de les dades.

Per exemple, algunes de les formes més habituals de recollida de dades i, a través dels quals cal donar les informacions pertinents, poden ser:
• Formularis en paper
• Navegació o formularis web

D'altra banda, les comunicacions a les persones de qui disposem ja de dades personals, podrien fer-se arribar, entre d'altres, per mitjà de correu postal o missatgeria electrònica.

En qualsevol cas, la informació a les persones interessades s'ha de proporcionar amb un llenguatge clar i senzill, de manera concisa, transparent, intel·ligible i de fàcil accés.

IMPORTANT: La informació s'ha de posar a disposició dels interessats en el moment en què se sol·licitin les dades o prèviament a la recollida o registre, si és que les dades s'obtenen directament de la persona interessada.

En el cas que les dades no s'obtinguin del propi interessat perquè procedeixen d'alguna cessió legítima o de fonts d'accés públic, cal informar les persones interessades dins d'un termini raonable.

### Clàusula de sol·licitud de dades personals

Per demanar el consentiment per utilitzar les dades, no pot prestar-se sota cap tipus de coacció ni tampoc pot condicionar-se com pot ser davant una rebaixa d'un servei, no es pot atorgar un consentiment general.

Es demanarà consentiment amb una clàusula adherida al final del document o aplicatiu mitjançant el qual es sol·liciten les dades, com el que es presenta seguidament:

Persona responsable: Associació X
NIF entitat: xxxxxxxxxx
Dir. Postal: xxxxxxxxxxxxxxxx
Telèfon: 666 66 66 66
Correu electrònic: info@associacio.org

En nom de l'organització tractem la informació que ens facilita per tal d'oferir el servei sol·licitat. Les dades proporcionades

es conservaran mentre es mantingui la relació o durant els anys necessaris per complir amb les obligacions legals.
Les dades no se cediran a tercers excepte en els casos en què hi hagi una obligació legal.
Vostè té dret a obtenir confirmació sobre si la (Associació X) estem tractant les seves dades personals per tant té dret a accedir a les seves dades personals, rectificar les dades inexactes o sol·licitar la seva supressió quan les dades ja no siguin necessaris. Així mateix sol·licitem la seva autorització per oferir serveis relacionats amb els sol·licitats.

SI
NO

**AVÍS:** Cal tenir en compte que si les persones usuàries marquen l'opció NO, en cap cas se'ls hi pot enviar informació de cap tipus. I sobretot, no s'admeten formes de consentiment tàcit o per omissió (que es basen en la inacció).

És important destacar que en cas de recollir dades de menors es recapta el consentiment de menors de la pàtria potestat o tutela sobre l'infant i es verifica que el consentiment va ser donat pel titular de la pàtria potestat o tutela sobre l'infant.

*Un exemple de clàusula podria ser:*

CLÀUSULA DE PROTECCIÓ DE DADES DE CARÀCTER PERSONAL: En compliment del nou Reglament General de Protecció de dades, t'informem del següent:

El responsable de les dades facilitades lliurement és el Associació X (NIF xxxxxxxxxxxxxxx), amb seu a xxxxxxxxxxxxxxx, Barcelona, telèfon 666666666 i correu electrònic info@associacio.org.

En nom de l'organització tractem la informació que ens facilites per tal d'oferir el servei sol·licitat. La finalitat d'aquest fitxer és facilitar la gestió dels serveis i activitats que s'ofereixen des de l'entitat amb l'objectiu de respondre a les necessitats de les persones sòcies. Les dades proporcionades es conservaran mentre es mantingui la relació o durant els anys necessaris per complir amb les obligacions legals. Les dades no se cediran a tercers excepte en els casos en què hi hagi una obligació legal.

Vostè té dret a obtenir confirmació sobre si l'Associació X estem tractant les seves dades personals per tant té dret a accedir a les seves dades personals, rectificar les dades inexactes o sol·licitar la seva supressió quan les dades ja no siguin necessaris. Així mateix sol·licitem la seva autorització per oferir serveis relacionats amb els sol·licitats.

En el cas en el que es contemplin les transferències de dades personals a un tercer país o una organització internacional, caldrà informar-se'n. Cal revisar la política de privacitat que tenim signada amb els proveïdors de serveis com Mailchimp, Google, etc.

**La política de privacitat visible:**

Per fer compatible la major exigència d'informació que introdueix el RGPD i la concisió i comprensió en la forma de presentar-la, des de les autoritats de Protecció de Dades es recomana adoptar un model d'informació per capes o nivells, que s'ha d'incloure al canal mitjançant el quan es recullen les dades, tant si és en format paper o online:

- **Nivell bàsic:** en el moment de recollir les dades personals consta el resum de la política de privacitat amb un enllaç al nivell 2.
- **Nivell addicional:** hi consta la informació addicional que completa la política de privacitat de l'entitat.

Com veureu, el RGPD proposa redactar la informació en el format d'un quadre de fàcil lectura. En una columna hi constarà la informació bàsica (nivell bàsic) i en l'altra la informació addicional (nivell addicional).

Així doncs, la informació bàsica de la política de privacitat de l'entitat (nivell bàsic), tant en format paper com en format electrònic tindria la següent forma:

| Informació bàsica sobre Protecció de Dades | |
|---|---|
| **Persona responsable** | Associació juvenil Suport |
| **Finalitat** | Incorporació en un fitxer per a gestionar els serveis de suport a l'associacionisme oferts. |
| **Legitimació** | Consentiment de l'interessat o per existència d'un contracte mercantil. |
| **Persones destinatàries** | No es cediran dades a tercers |
| **Drets** | Té dret a accedir, rectificar i suprimir les dades, així com altres drets, com s'expliquen a la informació addicional. Podeu consultar més informació sobre la política de privacitat: http://www.xxxxxxxxprotecciodedades |
| **Procedència** | De la persona interessada |

Si voleu saber la informació addicional (nivell addicional) que cal incloure a la pàgina web, podeu consultar la **Plantilla de Documentació Associativa "La llei de protecció de dades",** en format descarregable per a poder utilitzar-la a la vostra entitat!

### 6. Com analitzem les possibles fugues de dades personals?

El RGPD és molt clar en avaluar les possibles escletxes o fugues de seguretat que es podrien produir. Això vol dir avançar-se al que pugui ocórrer i preveure possibles fugues que puguin comportar la visualització pública de dades personals.

Les possibles fugues podrien ser:
- consten les dades penjades de forma pública
- es demanen dades a altres persones davant de tercers
- s'escriuen les dades en papers a sobre la taula amb accés a tothom
- es guarden en armaris o arxivadors no tancats en clau, etc.
- accés a servidors compartits.
- accés a arxius no xifrats
- contrasenyes poc segures
- etc.

Com es veu en l'exemple ja detallat anteriorment, seguirem emplenant-lo amb informació sobre les possibles fugues i les mesures de seguretat a aplicar:

| **Persones de qui disposem dades** | **Dades no sensibles** | **Dades sensibles** | **Qui hi té accés** | **On estan emmagatzemades les dades** | **Possibles fugues** | **Mesures de seguretat a aplicar** |
|---|---|---|---|---|---|---|
| Persones sòcies | Nom<br>cognoms<br>DNI<br>Adreça<br>Data de naixement<br>Telèfon de contacte<br>Correu electrònic<br>Xarxes socials | Al·lèrgies | Junta directiva | Google drive (llibre de persones sòcies) | Deixar el gmail obert en un ordinador aliè i tenir accés lliure al drive<br><br>Al tenir accés a dades no sensibles, s'accedeix directament a dades sensibles | Assegurar que quan es tanca l'ordinador es tanquen les sessions obertes<br><br>Guardar les dades sensibles en un altre document sota contrasenya o enviar xifrat a les persones sòcies que ho necessitin.<br><br>Tancar el llibre a un armari en clau (guardada en un lloc determinat i fora de l'accés al públic)<br><br>Assegurar que ningú escriu dades personals en post-its ni fulls bruts. |
| Junta directiva | | | | | | |
| Antigues persones sòcies | | | | Llibre de persones sòcies a casa de presidència | Que es perdi el llibre | |
| Professorat i educadors socials | | Currículum Vitae | | Correu gmail de diferents persones sòcies<br><br>Fulls i post-its d'ús momentani<br><br>Fulls d'inscripció en carpetes<br><br>CV guardats en carpetes | Deixar el gmail obert en un ordinador aliè i tenir accés lliure al drive<br><br>Que algú accedeixi a les carpetes<br><br>Al tenir accés a dades no sensibles, s'accedeix directament a dades sensibles | |
| Clientela i persones usuàries | | Malalties<br>Al·lèrgies<br>etc. | Persones sòcies | | | |
| Altres persones col·laboradores i voluntàries | | | Persones sòcies | | | |
| Etc. | | | | | | |

El Reglament no estableix un llistat de les mesures de seguretat que s'han aplicar d'acord amb la tipologia de dades objecte de tractament, sinó que estableix que la persona responsable i l'encarregat del tractament han d'aplicar les mesures tècniques i organitzatives adequades al risc que comporta el tractament. Això implica que cal fer aquesta avaluació dels riscos associats a cada tractament, per determinar les mesures de seguretat que cal implementar.

Així doncs, **algunes mesures per tal d'evitar aquestes fugues** serien:

• Assegurar que quan es tanca l'ordinador es tanquen les sessions obertes.
• Canvi de contrasenyes amb canvis de persones.
• Guardar les dades sensibles en un altre document sota contrasenya o enviar xifrat el document a les persones sòcies que ho necessitin.
• Tancar la documentació a un armari amb clau (guardada en un lloc determinat i fora de l'accés al públic).
• Assegurar que ningú escriu dades personals en post-its ni fulls bruts.
• Assegurar que la gent té accés des de correus laborals i no personals a formularis, etc.
• Deixar mòbils amb dades i correus.
• Etc.
A més, en el cas de tenir a disposició de l'organització de dades sensibles, el RGPD proposa el que anomena «seudonimització», o altrament dit disseminació de dades. És a dir, incloure procediments en els quals es separen les dades sensibles de les no sensibles, afegint una protecció extra a les sensibles. La manera de relacionar les dades entre sí pot ser a través de codis i xifres.

**Notificació de bretxes de seguretat de dades personals a l'autoritat de control:**

Des del RGPD s'ha establert un procediment per identificar i gestionar les bretxes de seguretat, les fugues que hagin ocorregut. Per exemple, si s'ha perdut la carpeta amb tota la informació amb les dades dels menors assistents a una excursió de l'esplai, si s'ha penjat públicament un document amb dades personals, si ha desaparegut un fitxer del servidor amb dades.

Hi ha un procediment mitjançant el qual es notifiquen les bretxes al responsable en el moment en què es tingui coneixement d'elles, en un termini màxim de 72 hores. En el cas en què no es cregui necessari ja que es valora que no hi ha suficient risc d'ús de les dades o es creu que es trobarà a informació en un termini raonable, també hi ha un procediment per documentar els motius pels quals no es pot notificar en aquest termini de 72 hores.
D'aquesta manera es pot facilitar la informació de manera gradual quan no sigui possible facilitar-la conjuntament. Per més informació consulteu: https://www.aepd.es/

En la documentació s'inclouen els fets relacionats amb ella, els seus efectes i les mesures correctives adoptades.

A més, el RGPD també obliga a informar a les persones interessades de les quals se'ls han extraviat les dades en aquest mateix termini.

**7.- És obligatori redactar un registre d'activitats de seguretat?**

El registre d'activitats que defineix el RGPD, altrament dit protocol, és el detall de les mesures adients per a una correcta protecció de les dades personals.

L'RGPD preveu noves obligacions de documentació del tractament per als i les responsables o els i les encarregades del tractament.

S'exceptuen d'aquesta obligació els i les responsables o encarregades del tractament que comptin amb menys de 250 persones treballadores i que duguin a terme tractaments que no puguin comportar un risc-llevat que sigui ocasional-, per als drets i les llibertats de les persones interessades, i que no incloguin categories especials de dades personals, o dades personals relatives a condemnes i infraccions penals.

Des de l'experiència i coneixement que tenim des del CRAJ som conscients que la majoria d'entitats juvenils no esteu dins de les organitzacions amb l'obligació de tenir aquest registre d'activitats. Igualment, vetllem per al correcte tractament

de les dades personals a disposició de les entitats i per tal, aconsellem redactar un document a disposició de tothom que tingui accés a dades de caire personal on incloguin les mesures de seguretat dur a terme, havent fet l'anàlisi que s'ha vingut fent al llarg d'aquesta publicació.

Entre aquestes activitats hi podríem **fer constar i implementar accions genèriques** decidides a partir de l'estudi prèviament detallar com:

- Custodiar les dades en un mateix servidor sota contrasenya.
- Donar accés a la base de dades a determinades persones.
- Eliminar dades innecessàries.
- Xifrar el document per a que aquest sigui enviat, i assegurar-se que la contrasenya del document xifrat que conté dades personals sigui facilitada per un altre canal amb el que s'envia (telèfon, persona, etc.).
- Configurar correctament les opcions de privacitat i seguretat.
- Utilitzar contrasenyes robustes.
- Fer còpies de seguretat en suports alternatius emmagatzemades en entorns segurs.
- Si es comparteixen fitxers, assegurar que la persona destinatària sigui realment qui es desitgi.
- Assegurar que quan es tanca l'ordinador es tanquen les sessions obertes.
- Guardar les dades sensibles en un altre document sota contrasenya o enviar xifrat a les persones sòcies que ho necessitin.
- Assegurar que ningú escriu dades personals en post-its ni fulls bruts.
- Assegurar que no es repeteixin en veu alta dades personal a l'escolta d'algú del voltant.
- Etc.

També aconsellem incloure en el registre d'activitats com cal adaptar tots els documents de recollida de dades als requeriments que estableix el nou reglament com són les plantilles de sol·licitud de dades i de política de privacitat, donant la possibilitat de modificar les finalitats per les quals es recull la informació personal.

Caldrà inclús definir detalladament els mecanismes i procediments per l'exercici dels drets ARCO i dret a l'oblit i portabilitat. Per exemple, en el moment en el que una persona informi de la intenció de dur a la pràctica els seus drets, qui rebrà la demanda, com es complirà i qui ho farà.

En el cas en el que hi hagi bloqueig de dades personals, una acció permesa en el RGPD, detallar que no se'n farà cap ús, sinó que es guarden a mode històric. Si al recollir-les s'ha informat que en un termini màxim de 10 anys s'eliminaran, caldrà complir el què s'ha informat.

### 8. - Cal redactar una avaluació d'impacte?

Quan sigui probable que un tractament suposi un risc alt per als drets i les llibertats de les persones físiques, per la seva naturalesa, abast, context o finalitats, especialment si s'utilitzen les noves tecnologies, abans d'iniciar el tractament la persona responsable ha de fer una avaluació de l'impacte de les operacions de tractament en la protecció de dades personals.

L'RGPD conté una llista indicativa de **tres supòsits en els quals es considera que els tractaments comporten un alt risc:**
- Elaboració de perfils sobre la base dels quals es prenen decisions que produeixen efectes jurídics sobre els interessats o que els afecten significativament de manera similar.
- Tractament a gran escala de dades sensibles.
- Observació sistemàtica a gran escala d'una zona d'accés públic.

Les associacions juvenils no compleixen cap d'aquests supòsits de manera que en un primer moment no caldrà redactar l'avaluació d'impacte, limitant-se a determinades organitzacions.
Recordeu que el RGPD es basa en el principi de responsabilitat activa de la persona responsable, que en últim extrem sempre és la persona responsable de decidir quines mesures s'han d'aplicar i com s'ha de fer.

A més, l'Autoritat Catalana de Protecció de Dades, l'Agència Espanyola de Protecció de Dades i l'Agència Basca de Protecció de Dades publicaran durant el període transitori recursos per ajudar als i les responsables a determinar la necessitat de fer una avaluació d'impacte.

## 7. Webs d'interès

**Els recursos de l'Agència espanyola de protecció de dades** (AEPD): www.agpd.es
**Els recursos de l'Agència de Protecció de Dades de Catalunya** (APDCAT): www.apdcat.gencat.cat
**Els recursos de l'Agència Basca de Protecció de Dades:** www.avpd.euskadi.eus

I altra informació penjada per la xarxa:

- http://xarxanet.org/juridic/recursos/les-10-claus-sobre-el-nou-reglament-de-proteccio-de-dades
- http://xarxanet.org/juridic/noticies/cronica-xerrada-lopd
- http://apdcat.gencat.cat/ca/documentacio/RGPD/novetats/

Recordeu que des del **Centre de Recursos per a les Associacions Juvenils de Barcelona** podeu demanar una assessoria legal, fiscal, comptable totalment gratuïta.
Cal sol·licitar hora prèvia omplint el formulari o trucant al **93 265 52 17.**

Aquest document té una finalitat merament divulgativa en relació a determinats aspectes de la normativa sobre protecció de dades. En aquest sentit, el present document comprèn informació i comentaris de caràcter general i no constitueixen un assessorament jurídic de cap tipus.

El present document ha sigut actualitzat en data 26/06/2018 i el CRAJ no assumeix cap compromís d'actualització o revisió del seu contingut ni de la exactitud, veracitat o correcció de la informació compresa.