Formació per a entitats

La llei de protecció de dades personals

La llei de protecció de dades personals

La **Llei orgànica 15/1999 de protecció de dades de caràcter personal (LOPD)** 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; garantir el dret a controlar què es fa amb les nostres dades, saber **qui té informació** sobre nosaltres, **quina informació té**, d'on l'ha obtingut, per a quina **finalitat** té les dades i si té intenció de **facilitar-les** a un tercer.

Qualsevol dada que pugui identificar una persona (nom, adreça, DNI...) o que la faci identificable (com per exemple una fotografia), està sotmesa a aquesta llei.

El consentiment de l'afectat/da (art. 5 LOPD) és imprescindible per al tractament de dades. **La informació personal no pertany a qui la gestiona sinó al titular de les dades**. En qualsevol document on recollim dades (formularis, fitxes d'inscripció, etc.) hi ha de constar el nom de l'entitat que recull les dades, quin tractament en farà, la possibilitat de cancel·lar-les i el procediment per fer-ho, tot atenent els drets **ARCO: drets d'Accés, Rectificació, Cancel·lació i Oposició**.

Per a tractar dades de persones físiques, cal que l'interessat hagi prestat el seu consentiment per a facilitar les seves dades, n'autoritzi el seu emmagatzematge i la seva utilització pel 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 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 acceptada per l'interessat.

Les dades referents a ideologia, afiliació sindical, religió o creences, requereixen un consentiment exprés per escrit. Així doncs, en aquests casos, no serà suficient un avís legal acceptat, sinó que haurem de dissenyar una butlleta específica per a formalitzar aquesta autorització (Amb l'excepció de fitxers de partits polítics, sindicats, esglésies, confessions o comunitats religioses).

També caldrà un consentiment exprés de l'afectat (o que una llei així ho disposi) per al tractament de dades de caràcter personal com són l'origen racial, dades referents a la salut o vida sexual.

A qui afecta aquesta normativa?

Les associacions estan obligades a mantenir actualitzat, entre d'altres documents, un llibre registre de socis i de voluntaris (article 313-3.2 del Llibre V del Codi Civil de Catalunya). Quan els beneficiaris són persones físiques, les dades d'aquests es veuen emparades per la normativa sobre protecció de dades de caràcter personal.

Aquesta normativa afecta a tota entitat que tracti dades personals, com ara un llistat de socis/es, voluntaris/es, clients/es, treballadors/es... però no només afecta a les entitats, sinó que també afecta a les empreses, comunitats de veïns, organismes públics, botigues, persones físiques... En definitiva, a tots aquells organismes que facin recollida i tractament de dades referents a les persones físiques.

Cal tenir present que aquesta normativa presenta algunes excepcions. En queden exemptes:

- Les dades referents a persones difuntes. Tot i que en aquest cas els familiars si que tenen dret a cancel·lació.
- Les dades de persones jurídiques (adreça, NIF, correu electrònic... d'una entitat).
- Les dades de les persones físiques que exerceixen un càrrec dins de l'entitat, com per exemple els seus representants (president, secretari, tresorer i vocals).
- Les dades relatives a empresaris individuals (telèfon, correu de contacte, adreça....).
- Els fitxers de persones físiques amb finalitats exclusivament personals (com per exemple la llista de contactes d'amistats).

Mots clau

- **Dada:** tota informació que identifica o permet identificar una persona física (nom, cognoms, DNI, adreça postal, e-mail, telèfon, imatge, veu, número de compte bancari...). Noteu que les dades referents a entitats (persones jurídiques) no estan subjectes a aquesta normativa.
- **Tractament de les dades:** procediments tècnics de caràcter automatitzat o no, per a la recollida, gravació, modificació, cancel·lació, cessió i consultes de les dades.
- **Fitxer:** conjunt organitzat de dades de caràcter personal, ja sigui automatitzat, en suport paper o parcialment automatitzat.
- **Afectat o interessat:** persona física titular de les dades que siguin objecte del tractament.
- **Responsable del fitxer**: persona física o jurídica de naturalesa pública o privada a qui pertany el fitxer, amb independència que executi o no materialment el tractament.
- **Sistema de Tractament**: qualsevol forma o modalitat que permeti l'ús i gestió de les dades, des que es registren fins que s'eliminen.
- **Encarregat de Tractament**: pot ser el responsable del fitxer o qualsevol altra persona física o jurídica de naturalesa privada o pública que tracti per encàrrec del responsable les dades de caràcter personal dels fitxers. Alhora, aquest encarregat de tractament pot fer-ho sol o conjuntament i en cada cas tots els agents implicats estan obligats a seguir la normativa de confidencialitat.
- **Usuari**: qualsevol persona que tingui accés a les dades personals que componen un o més fitxers del responsable.
- **Responsable de Seguretat**: persona o persones físiques o jurídiques que tenen la funció de vetllar pel compliment, aplicació i manteniment del document de seguretat.
- **Document de seguretat**: recull de normativa i processos per a l'aplicació dels aspectes regulats en matèria de protecció de dades que tot Responsable de Fitxer ha de tenir obligatòriament.
- **Comunicació de dades**: qualsevol cessió de les dades personals del responsable del fitxer a tercers.

Quins tipus de dades hi ha?

Hi ha tres nivells de seguretat, que s'apliquen en funció de les dades que contingui el fitxer.

- **Nivell de seguretat baix:** nom, cognoms, adreça postal, adreça electrònica, telèfon, DNI...

Per a aquest tipus de dades caldrà garantir un document de seguretat, informar de les funcions i obligacions del personal que les gestiona, portar un registre d'incidències, garantir una identificació i autenticació de les dades, establir un control d'accés a aquestes dades i disposar de còpies de recolzament i recuperació d'aquestes.

- **Nivell de seguretat mitjà:** Totes aquelles dades que puguin determinar el nivell socioeconòmic o un perfil que pugui avaluar determinats aspectes de les persones (Currículums, targetes de fidelització de clients, etc).

Les dades que requereixen un nivell de seguretat mitjà, **a part de les característiques del primer nivell**, també hauran de tenir assignat un responsable de seguretat d'aquesta informació, han de passar una auditoria, un registre d'entrada i sortida de suports, un control d'accés físic...

- **Nivell de seguretat alt:** Dades relatives a salut, religió, vida sexual, ideologia o dades relacionades amb violència de gènere.

Les dades que requereixin un nivell de seguretat alt, **a part de les condicions anteriors** necessiten registre d'accessos, xifratge d'equips i dispositius, control de còpia o reproducció...

En cas de tenir dades que requereixen **nivells diferents** de seguretat, serà convenient tenir **registres separats.** Per exemple: si es fan unes colònies, a més de les dades de Nivell de protecció 1 que ja tenim dels nens i nenes (Nom, cognoms, DNI....) necessitarem dades de salut (al·lèrgies, malalties...), per això haurem de fer un registre diferent amb un nivell de protecció 2, que contingui aquestes noves dades i que garanteixi el seu nivell de seguretat. Caldrà generar un document signat pel tutor legal de l'infant, on constin aquestes noves dades aportades i què es farà amb elles un cop acabades les colònies (arxivar, destruir, retornar...).

+informació sobre obligacions de seguretat en funció de cada nivell
https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_SEGURIDAD_2010.pdf

Per a complir la normativa...

S'han de garantir els drets d'informació de l'interessat. Aquests drets consisteixen en:

- Comunicar l'existència d'un fitxer on hi constaran les seves dades.
- Informar del tractament que se'n farà (la finalitat de recollir-les) i dels destinataris a qui es farà arribar aquesta informació.
- Informar a l'interessat sobre la llibertat a l'hora de cedir aquestes dades i les conseqüències de la seva negativa (per exemple: un soci no està obligat a informar de la seva adreça, però en cas contrari haurà d'assumir les conseqüències de no rebre les informacions que l'associació envia per correu postal).
- Garantir la possibilitat per part de l'afectat d'exercir els drets ARCO. Al mateix temps, també, evitar l'alteració, pèrdua, tractament o accés no autoritzat.

Drets ARCO

Dret d'Accés: el dret d'Accés reconeix als ciutadans la potestat de defensar la seva privacitat controlant per si mateixos l'ús que es fa de les seves dades personals.

Drets de Rectificació i Cancel·lació: quan les dades personals d'un ciutadà resultaren ser incompletes, inexactes, excessives o inadequades aquest pot requerir al responsable del fitxer la seva rectificació o cancel·lació.

Dret d'Oposició: bàsicament consisteix en el dret dels titulars de les dades per dirigir-se al responsable del fitxer perquè deixi de tractar les seves dades sense el seu consentiment per a fins de publicitat o prospecció comercial.

Per aplicar la llei correctament, s'han de realitzar els següents passos:

1. Identificació de les dades: Cal comprovar quin tipus de dades contenen els nostres fitxers i conèixer a quin nivell de protecció s'adeqüen. També és pertinent considerar l'opció de fer divisió entre un o més fitxers segons el nivell de protecció que requereixen les dades.

2. Elaborar un document de seguretat: És un document intern on es descriuen les mesures de seguretat aplicades a cada fitxer. És de compliment obligatori per tot el personal i s'ha de mantenir actualitzat, afegint les modificacions pertinents en cas que el nivell de protecció de les dades hagi de canviar. El document ha de contenir:

- L'àmbit d'aplicació d'aquestes mesures de seguretat
- Normes, procediments, regles que s'han de seguir en el tractament de les dades.
- Funcions i obligacions del personal: Identificació del responsable de seguretat, encarregats del tractament, usuaris del fitxer...
- Estructura dels fitxers i descripció dels sistemes que el contenen.
- Mecanismes de notificació, gestió i resposta davant de possibles incidències.
- Còpies de seguretat i recuperació de dades.
- Mètodes de conservació i actualització del document.

Al web de L'AEPD hi podeu consultar un model de Document de Seguretat en format editable.
https://www.agpd.es/portalwebAGPD/canalresponsable/guia_documento/index-idca-idphp.php

3. Inscriure els fitxers a Agència Espanyola de Protecció de Dades (AEPD): Notificar a l'AEPD quin o quins tipus de fitxer gestionem i quin tractament tenen les dades que contenen. El que comuniquem a l'Agència Espanyola de Protecció de Dades és el **tipus de dades** de les quals es disposa, no el contingut explicit de les dades.

Inscripció de fitxers a la web de l'AEPD
http://sedeagpd.gob.es/sede-electronica-web/vistas/formNOTA/servicioNOTA.jsf

4. Confeccionar les clàusules: fitxa de soci, formularis de tallers, cursos, conferències, taules rodones, inscripcions per sortides d'un dia...

Model de clàusula informativa:
D'acord amb l'article 5 de la Llei Orgànica 15/1999 de Protecció de Dades (LOPD) us informem que les vostres dades s'inclouen en el fitxer "(nom del fitxer)", el responsable del qual és (nom de l'empresa o professional). Les vostres dades seran tractades amb l'única finalitat de (definir la finalitat). En qualsevol cas, podeu exercir els vostres drets d'accés, rectificació, cancel·lació i oposició mitjançant una comunicació escrita, a la qual heu d'adjuntar una fotocòpia del DNI, adreçada a (adreça postal de l'empresa o professional).

5. Crear un document de confidencialitat dels treballadors/es: Aquest document ha de garantir que els responsables de gestionar aquesta informació estan al corrent de la confidencialitat d'aquestes dades.

6. **Comunicació i cessió de dades personals a tercers**
Una altra obligació fonamental per al responsable del fitxer la trobem en la cessió i comunicació de dades, que també ha de tenir el coneixement i consentiment de l'afectat. Aquesta obligació adquireix especial rellevància en el context actual de subcontractació de serveis per part de les entitats.

Podria ser que la dada fos recollida per un responsable del fitxer i que després fos cedida a un tercer per a un tractament específic. Per exemple, les dades d'uns treballadors passades al servei contractat d'assessoria laboral, sense coneixement ni consentiment dels afectats, podrien ser posteriorment utilitzades per enviar-los publicitat comercial de serveis.

En qualsevol comunicació o cessió de dades, per a tractament o no, hi ha d'haver un contracte entre el responsable del fitxer i aquest tercer encarregat del tractament on s'estableixin quines són les finalitats del tractament i on l'encarregat del tractament es comprometi a complir amb la normativa vigent en matèria de protecció de dades. Resulta doncs una garantia força important per a l'afectat i en e**l recull de processos sancionadors de l'Agència Espanyola trobem importants sancions econòmiques per cessió il·legal de dades**. L'article 9 de la LOPD estableix que el responsable del fitxer i en el seu cas l'encarregat del tractament seran els responsables d'aplicar les mesures de seguretat en les dades.

7. Adaptar el web i el correu electrònic de l'entitat: Incloent-hi un avís legal i especificant la política de privacitat que s'aplica en aquest espai web.

- **Adaptar el Web a la llei de protecció de dades**
  A la pàgina web hi han de constar les dades identificatives de l'entitat: el nom de l'entitat i un mitjà de contacte: telèfon, correu electrònic, etc.

  També hi haurà de constar un avís legal on s'especifiquin les condicions d'ús del web i la política de privacitat que exerceix. A més, si el web inclou algun formulari, hi ha d'haver una clàusula que especifiqui la finalitat del recull de les dades i el tractament que se'ls hi donarà.

- Les dades que es tracten via e-mail
  Els correus que envieu a més d'un destinatari, s'han d'enviar sempre mitjançant CCO (còpia oculta) de tal manera que la resta de receptors del missatge no tinguin accés a les dades de contacte dels altres receptors.

  En els correus massius que s'envien a destinataris que us van facilitar les seves dades de contacte, és adient afegir- hi també l'avís legal on s'especifiquin tots els aspectes referents al compliment dels drets ARCO (Accés, Rectificació, Cancel·lació i Oposició) dels quals

disposen els propietaris de les dades. Aquest avís legal pot seguir un model estàndard ja predeterminat que contingui les explicacions pertinents del tractament d'aquestes dades.

Classificació de les infraccions

L'incompliment de la Llei de protecció de dades es classifica en tres tipus d'infraccions:

- **Infracció lleu**: No sol·licitar la inscripció del fitxer, incompliment del deure d'informació a l'interessat o transmissió de dades sense complir el que disposa la llei. Aquests supòsits comporten una sanció de 900 a 40.000 euros.

- **Infracció greu**: Tractar dades sense consentiment, impediment per exercir els drets d'accés, oposició, rectificació i cancel·lació (Drets ARCO) o mantenir fitxers sense les condicions de seguretat apropiades. Aquests supòsits comporten una sanció de 40.000 a 300.000 euros.

- **Infracció molt greu**: Recollida de dades de manera fraudulenta, no cessar en el tractament il·lícit de dades previ requeriment de l'Agència de Protecció de Dades, **transferència de dades de caràcter personal a països que no proporcionin un nivell equiparable de protecció**. Aquests supòsits comporten una sanció de 300.000 a 600.000 euros.

La Normativa Aplicable

- La Llei de Protecció de dades actualment està sotmesa a la següent normativa:
- Llei Orgànica 15/1999, del 13 de desembre, de Protecció de Dades de Caràcter Personal (LOPD).
- Reial Decret 1720/2007, de 21 de desembre, de desenvolupament de la Llei Orgànica de Protecció de Dades.
- Llei 34/2002, de l'11 de juliol, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSIce).

Cal tenir present que aquesta normativa s'aplica a les dades referents a persones físiques. Pel que fa a les dades de persones jurídiques (entitats) la normativa de protecció de dades és més laxa.

Webs d'interès

Agència Espanyola de Protecció de Dades (901100099 / 912663517)
https://www.agpd.es/portalwebAGPD/index-idca-idphp.php

Guia de seguretat
www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_SEGURIDAD_2010. pdf

Autoritat Catalana de Protecció de Dades www.apd.cat