

Guia bàsica de protecció de dades per als ens locals

Biblioteca de Catalunya. Dades CIP

Guia bàsica de protecció de dades per als ens locals

I. Autoritat Catalana de Protecció de Dades II. Catalunya. Generalitat

1. Protecció de dades – Dret i legislació – Catalunya

2. Administració local – Dret i legislació - Catalunya

342.738(467.1)(094.5)

Edició

© **Generalitat de Catalunya**

Autoritat Catalana de Protecció de Dades

Primera edició: març 2012

Coordinació de l'edició i composició: Entitat Autònoma del Diari Oficial i de Publicacions

Dipòsit legal: B-10450-2012

■ Índex

Presentació	5
1 Marc normatiu	7
2 Legitimitat del tractament	11
2.1 El principi de consentiment	13
2.1.1 El consentiment.....	13
2.1.2 Dades especialment protegides.....	15
2.1.3 Dades recollides per les policies locals.....	16
2.1.4 Dades relatives a menors d'edat.....	16
2.1.5 Revocació del consentiment	17
2.1.6 Tractament en supòsits de manca de consentiment.....	17
2.2 El principi de qualitat de les dades.....	19
2.2.1 Principi de proporcionalitat	19
2.2.2 Principi de finalitat	19
2.2.3 Principi d'exactitud	19
2.2.4 Conservació	19
2.2.5 Principi de lleialtat	20
3 Obligacions prèvies al tractament	21
3.1 La creació, la modificació i la supressió dels fitxers.....	23
3.1.1 Fitxers de titularitat pública.....	24
3.1.2 Fitxers de titularitat privada	26
3.2 La notificació dels fitxers o tractaments	26
3.3 La informació a la persona titular de les dades.....	27
4 Obligacions durant el tractament	28
4.1 El deure de secret	30
4.2 La comunicació de dades personals	30
4.2.1 Requisits.....	31
4.2.2 L'encarregat del tractament.....	33
4.2.3 Accés dels regidors a informació municipal	34
4.2.4 Accés d'altres àrees de l'ajuntament a informació municipal.....	35
4.2.5 Transferències internacionals de dades.....	36
4.3 Els drets d'habeas data	36
4.3.1 Dret d'accés	37
4.3.2 Dret de rectificació	38
4.3.3 Dret de cancel·lació.....	39
4.3.4 Dret d'oposició.....	39
4.3.5 Procediment per exercir els drets ARCO	40
4.3.6 Reclamació de tutela de drets.....	41
4.4 Mesures de seguretat	42
4.4.1 Implementació de les mesures de seguretat.....	42
4.4.2 Document de seguretat	45

5	El règim de responsabilitat	46
5.1	Tipus de responsabilitats.....	48
5.2	Potestat d'inspecció	49
5.3	Potestat d'immobilització de fitxers	49
5.4	Infraccions	50
5.5	Sancions.....	52
5.6	Procediment sancionador.....	53
6	Els codis tipus	55
7	L'Autoritat Catalana de Protecció de Dades.....	59
7.1	Naturalesa i objecte.....	61
7.2	Àmbit d'actuació	61
7.3	Organització	62
7.4	Funcions.....	62
	Abreviatures.....	65

■ Presentació



L'exercici de les funcions que tenen atribuïdes els ens locals comporta que hagin de tractar un gran volum d'informació de naturalesa diversa. Això implica, necessàriament, el tractament de dades de caràcter personal. Els ens locals no són els titulars d'aquesta informació, atès que els titulars són les persones físiques a les quals es refereix, però els correspon custodiar-la i tractar-la d'una forma diligent i amb respecte als drets de les persones.

Amb aquesta Guia es vol oferir una primera aproximació als principis, les garanties i les obligacions que han de tenir en compte els ens locals en la seva actuació, per tal d'ajustar-la al que estableix la normativa de protecció de dades de caràcter personal. Per això, s'hi han recollit els principis fonamentals i les obligacions més rellevants, fent referència tant a la normativa

aplicable en cada cas, com també a alguns exemples de les consultes que se'ns han plantejat amb més freqüència.

No es tracta, per tant, d'una anàlisi exhaustiva de les qüestions que s'hi recullen, atès que l'anàlisi més completa requerirà aprofundir en la normativa aplicable, en la jurisprudència recaiguda en aquesta matèria i en els criteris i recomanacions que ha anat formulant aquesta Autoritat. En aquest sentit, recordar que al web d'aquesta Autoritat (<http://www.apd.cat>), podreu trobar tant la normativa esmentada com les darreres resolucions dictades, com també els informes i els dictàmens emesos.

Esperem, doncs, que sigui una eina útil per a desenvolupar la vostra activitat i per a conèixer millor el dret fonamental a la protecció de les dades de caràcter personal.

Esther Mitjans Perelló
Directora de l'Autoritat Catalana
de Protecció de Dades

Barcelona, febrer de 2012

1 Marc normatiu

El tractament de la informació relativa a una persona física identificada o identificable requereix el compliment d'un seguit de principis i obligacions, establerts en diferents normes que cal tenir en compte

- Directiva 95/46/CE del Parlament Europeu i del Consell, de 24 d'octubre de 1995, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades.
- Directiva 2002/58/CE del Parlament Europeu i del Consell, de 12 de juliol de 2002, relativa al tractament de les dades personals i a la protecció de la intimitat en el sector de les comunicacions electròniques (Directiva sobre la privadesa i les comunicacions electròniques, ePrivacy), modificada per la Directiva 2009/136/CE del Parlament Europeu i del Consell, de 25 de novembre de 2009.
- Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.
- Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.
- Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades.
- Decret 48/2003, de 20 de febrer, pel qual s'aprova l'Estatut de l'Agència Catalana de Protecció de Dades.
- Instrucció 1/2009, de 10 de febrer, sobre el tractament de dades de caràcter personal mitjançant càmeres amb fins de videovigilància.

També convé tenir en compte les següents recomanacions publicades:

- Recomanació 1/2008 de l'Agència Catalana de Protecció de Dades, sobre la difusió d'informació que contingui dades de caràcter personal a través d'Internet.
- Recomanació 1/2010 de l'Agència Catalana de Protecció de Dades, sobre l'encarregat del tractament en la prestació de serveis per compte d'entitats del sector públic de Catalunya.
- Recomanació 1/2011 de l'Autoritat Catalana de Protecció de Dades, sobre la creació, modificació i supressió de fitxers de dades de caràcter personal de titularitat pública.

2 Legitimitat del tractament

**Els ens locals poden tractar les dades
personals que resultin adequades per
a l'exercici de les seves funcions**

2.1 El principi de consentiment

La LOPD reconeix i garanteix el dret de les persones físiques a protegir la seva informació personal. Les persones titulars de dades personals, com a persones directament afectades o interessades, tenen dret a saber si un ens local disposa d'aquestes dades, per quin motiu les té i per a què les vol utilitzar.

La informació referida a persones físiques pot ser de diversos tipus (numèrica, alfabètica, gràfica, fotogràfica, acústica) i pot referir-se a un tret físic de la persona, a la seva situació econòmica o social, als seus estudis o a la seva professió, a la seva salut, etc.

La informació pot permetre identificar directament una persona (quan disposem del nom i cognoms, d'una fotografia, del DNI...), o bé pot identificar-la indirectament (quan disposem d'una informació que no està vinculada a una persona concreta, però l'associem amb d'altres dades que sí que ens permeten identificar-la sense esforços desproporcionats).

La LOPD protegeix tota aquesta informació, llevat de les dades que no puguem relacionar amb una persona concreta sense esforços desproporcionats.

Tractar informació personal vol dir accedir a aquesta informació (ja sigui perquè el mateix ciutadà la dona a l'ens local o perquè aquest la rep de tercers persones), com també emmagatzemar-la, modificar-la, utilitzar-la, eliminar-la o comunicar-la a qualsevol persona física o jurídica, aliena a l'ens, que no sigui la mateixa persona interessada.

2.1.1 El consentiment

El consentiment és la peça angular en la protecció de dades. Constitueix el principi sobre el qual s'articula el poder de disposició i control de qualsevol persona sobre les seves dades. Així, quan una entitat vulgui desenvolupar una activitat que requereixi tractar dades de caràcter personal, ha de comptar amb el consentiment de la persona afectada o, a manca d'aquest, amb una llei que l'habiliti.

Tot i això, cal tenir en compte que la mateixa LOPD habilita les **administracions públiques**, i entre elles els ens locals, perquè recullin les dades necessàries per a exercir les seves funcions, en l'àmbit de les seves competències.

Consentiment

Qualsevol manifestació de la voluntat, lliure, inequívoca, específica i informada, mitjançant la qual la persona interessada consent el tractament de dades personals que la concerneixen.

D'acord amb la normativa de protecció de dades, el consentiment ha de ser:

- **Inequívoc:** la sol·licitud i l'atorgament del consentiment s'han de produir de forma clara.
- **Lliure:** la persona ha de disposar de la possibilitat de rebutjar lliurement que es tractin les seves dades.
- **Específic:** el consentiment es refereix a tractaments concrets i per a una finalitat determinada, explícita i legítima del responsable del tractament, sense que es puguin fer habilitacions genèriques.
- **Informat:** cal informar les persones afectades d'acord amb allò que estableix l'article 5 de la LOPD per tal que, amb antelació al tractament, en puguin conèixer l'existència i les finalitats.

El consentiment es pot obtenir de forma expressa o de forma tàcita, llevat que es tracti de dades especialment protegides, en què el consentiment ha de ser exprés.

Quan sigui admissible el consentiment tàcit, aquest es pot obtenir a través del mecanisme següent:

a) El responsable del tractament es pot adreçar a les persones afectades, informar-les en els termes de l'art. 5 LOPD i atorgar-los un termini de 30 dies per manifestar la seva negativa al tractament.

b) S'ha d'oferir a la persona interessada un mitjà senzill i gratuït per manifestar la seva negativa al tractament de les seves dades en el termini esmentat.

c) Si la persona interessada manifesta la seva negativa, el responsable del fitxer no pot tornar-li a demanar el consentiment respecte del mateix tractament i les mateixes finalitats, en el termini d'un any a comptar des de la data de la sol·licitud anterior.

d) Si la persona interessada no s'ha pronunciat en acabar el termini, s'entén que consent el tractament de les dades.

Responsable del fitxer o del tractament

Persona física o jurídica, de naturalesa pública o privada, o òrgan administratiu, que sol o conjuntament amb altres decideix sobre la finalitat, el contingut i l'ús del tractament, encara que no ho realitzi materialment. També poden ser responsables del fitxer o del tractament els ens sense personalitat jurídica que actuïn en el tràfic com a subjectes diferenciats.

◇ Com s'ha d'actuar en aquells supòsits de pèrdua de la documentació en la qual s'havia recollit el consentiment de la persona afectada per al tractament de les seves dades de caràcter personal?

L'entitat ha de tornar a demanar el consentiment per al tractament o comunicació de dades de caràcter personal, atès que li correspon la càrrega de provar-ne l'atorgament.

Normativa aplicable: art. 3.h), 5 i 6 LOPD; 5.1.d), 12 i 14 RLOPD.

■ 2.1.2 Dades especialment protegides

El règim general del consentiment es reforça en el cas del tractament de dades especialment protegides o sensibles. Cal diferenciar els supòsits següents:

a) Dades que revelen la **ideologia, l'afiliació sindical, la religió i les creences**: només es poden tractar amb el consentiment exprés i per escrit, amb l'advertiment a la persona interessada respecte del seu dret a no facilitar aquestes dades.

b) Dades que es refereixen a l'**origen racial, la salut i la vida sexual**: només es poden tractar quan, per raons d'interès general, així ho disposi una llei o la persona afectada hi consenti expressament.

c) Dades relatives a la **comissió d'infraccions penals i administratives**: la creació de fitxers per a recopilar aquestes dades només la poden dur a terme les administracions públiques competents, d'acord amb les normes reguladores respectives.

No obstant això, excepcionalment, les dades especialment protegides es poden tractar, sense consentiment, quan sigui necessari per a la prevenció o el diagnòstic mèdic, la prestació d'assistència sanitària o de tractaments mèdics, la gestió de serveis sanitaris, per part de professionals sanitaris o altres persones subjectes al secret professional, o per a la salvaguarda de l'interès vital de la persona afectada o d'una altra persona, en cas que la persona afectada estigui físicament o jurídicament incapacitada per donar el seu consentiment.

◇ **Es poden comunicar dades que formen part de la història clínica d'un pacient a un familiar sense el seu consentiment?**

Segons la Llei 21/2000, l'accés a l'historial clínic tan sols el pot demanar el pacient o el seu representant degudament acreditat, atès que es tracta d'un dret personalíssim. Només s'ha d'informar les persones vinculades al pacient en la mesura que aquest ho permeti expressament o tàcitament.

En cas d'incapacitat del pacient, aquest ha de ser informat d'acord amb el seu grau de comprensió, sens perjudici d'haver d'informar també qui en té la representació.

Si el pacient, a criteri del metge responsable de l'assistència, no és competent per a entendre la informació, perquè es troba en un estat físic o psíquic que no li permet fer-se càrrec de la seva situació, se n'ha d'informar també els familiars o les persones que hi estan vinculades.

◇ **Pot una càmera de videovigilància enregistrar imatges que continguin dades especialment protegides, sense el consentiment de les persones afectades i sense una habilitació legal?**

No, excepte les captacions d'imatges de les persones en què, de forma merament accessòria, es puguin tractar trets físics, aparença, hàbits o comportaments.

Normativa aplicable: art. 7 i 8 LOPD; 3, 6 i 7 Llei 21/2000; 5.2 Instrucció 1/2009.

■ 2.1.3 Dades recollides per les policies locals

En relació amb les dades de caràcter personal recollides i tractades per les policies locals i la resta de Forces i Cossos de Seguretat amb finalitats policials, **no cal el consentiment** de la persona afectada en els supòsits i respecte de les categories de dades que siguin necessàries per a prevenir un perill real per a la seguretat pública o per a la repressió d'infraccions penals.

Respecte de les dades **especialment protegides**, les Forces i Cossos de Seguretat les poden recollir i tractar exclusivament en els supòsits en què sigui absolutament necessari per a una investigació concreta.

- Aquestes dades s'han d'**emmagatzemar** en fitxers específics establerts a aquest efecte, que s'han de classificar per categories d'acord amb el seu grau de fiabilitat. Així, no es pot atorgar el mateix grau de fiabilitat a meres sospites no contrastades, que a informacions relatives a una determinada imputació o sobre una persona que ha estat condemnada o absoluta.
- S'han de **cancel·lar** quan ja no siguin necessàries per a la finalitat per a la qual es van recollir.
- En aquells casos en què es pugui produir un perill per la defensa de l'Estat o la seguretat pública, la protecció dels drets i llibertats de tercers o les necessitats de les investigacions que estiguin obertes, es pot **denegar** l'accés, la rectificació o la cancel·lació de les dades.

◇ Les policies locals de Catalunya poden accedir a les gravacions de les càmeres de videovigilància d'una entitat?

Si és en el curs d'una investigació, la llei preveu que la policia pugui accedir a les gravacions.

Normativa aplicable: art. 22 LOPD; 9 LOVFC; 9 Decret 78/2010; 15 Decret 134/1999; 1 Ordre de 29 de juny de 2001; 5.1 i 18 Instrucció 1/2009.

■ 2.1.4 Dades relatives a menors d'edat

En cas de tractar dades de menors d'edat, cal tenir en compte:

- Si són **majors de catorze anys**, és suficient amb el seu consentiment, llevat dels casos en què la llei exigeixi l'assistència de les persones titulars de la pàtria potestat.
- Si són **menors de catorze anys**, sempre és necessari el consentiment dels pares o tutors.

No es poden obtenir a través d'un menor dades que permetin obtenir informació sobre la resta de membres del grup familiar o les seves característiques (activitat professional dels progenitors, informació econòmica...), sense consentiment de les altres persones afectades, llevat que es tracti de les dades referents a la identitat i l'adreça dels progenitors per tal de poder obtenir el seu consentiment.

La protecció dels menors es concreta també en l'exigència que la informació que se'ls proporciona sigui en un llenguatge fàcilment comprensible per a ells.

◇ **Pot un casal d'estiu municipal recollir la dada relativa a les adreces dels correus electrònics dels pares, a través dels menors d'edat que hi són inscrits, per tal de posar-s'hi en contacte?**

Com a norma general, cal comptar amb el consentiment dels pares per recollir la dada relativa al seu correu electrònic. Excepcionalment, pot facilitar-la directament el menor, en els casos en què sigui necessari completar la capacitat del menor d'edat a través dels seus progenitors, per tal que aquests puguin consentir el tractament de les dades del menor.

Normativa aplicable: art. 13 RLOPD.

■ 2.1.5 Revocació del consentiment

El consentiment atorgat per la persona afectada es pot **revocar** en qualsevol moment, sense efectes retroactius, sempre que hi hagi una causa justificada:

- El responsable del fitxer ha d'establir un mitjà senzill a través del qual la persona interessada pugui revocar el consentiment. El responsable del fitxer disposa d'un termini de 10 dies, des que rep la sol·licitud, per cessar en el tractament i, si escau, per cancel·lar les dades.
- La persona interessada pot sol·licitar al responsable del tractament la confirmació del cessament. Aquesta sol·licitud s'ha de respondre expressament.
- Si el responsable del tractament, amb caràcter previ a la revocació del consentiment, ha cedit dades a un tercer, ha de comunicar-li la revocació del consentiment dins el mateix termini de 10 dies, per tal que també cessi en el tractament i, si escau, cancel·li les dades.

Normativa aplicable: art. 6 LOPD; 12 i s. RLOPD.

■ 2.1.6 Tractament en supòsits de manca de consentiment

Malgrat el que acabem d'exposar, hi ha un seguit de supòsits regulats a la LOPD en els quals **no és necessari el consentiment** de la persona afectada, concretament quan:

- Així ho estableixi una norma amb rang de llei.
- Es recullin per a l'exercici de funcions pròpies de les **administracions públiques**, en l'àmbit de les seves competències.
- Es refereixin a les parts d'un contracte o precontracte d'una relació laboral, negocial o administrativa i siguin necessàries per mantenir-la o complir-la.

- El tractament de les dades tingui com a finalitat protegir un interès vital de la persona interessada.
- Les dades figurin en fonts accessibles al públic i el seu tractament sigui necessari per a satisfer l'interès legítim perseguit pel responsable del fitxer o pel tercer a qui es comuniquin les dades, sempre que no es vulnerin els drets i llibertats fonamentals de la persona interessada.

Fonts accessibles al públic

Fitxers que pot consultar qualsevol persona, sense que ho impedeixi una norma limitativa o sense altra exigència que, si escau, l'abonament d'una contraprestació. Només es consideren fonts d'accés públic el cens promocional, els diaris i els butlletins oficials, els mitjans de comunicació, les guies de serveis de comunicacions electròniques, en els termes que preveu la normativa específica, i les llistes de persones que pertanyen a grups de professionals que continguin únicament les dades de nom, títol, professió, activitat, grau acadèmic, direcció i indicació de la seva pertinença al grup.

◇ Es requereix el consentiment de les persones afectades perquè l'ajuntament pugui tractar les dades en un expedient iniciat d'ofici? I si el procediment s'ha iniciat a instància de part?

No és necessari el consentiment de la persona afectada en aquells tractaments de dades de caràcter personal que estiguin relacionats amb les funcions pròpies de les administracions públiques, en l'àmbit de les seves competències. Per tant sempre que aquesta informació s'obtingui en relació amb el desenvolupament de les seves competències, no cal el seu consentiment.

◇ La incorporació de dades al padró municipal requereix el consentiment de les persones afectades?

Les dades del padró constitueixen prova de la residència i el domicili habitual al municipi.

Existeix l'obligació de facilitar aquestes dades, fet que suposa una excepció legal al principi del consentiment. Aquesta obligació sempre ha d'estar vinculada amb la finalitat del padró.

◇ Cal demanar el consentiment dels treballadors d'un ens local per tractar les seves dades per mitjà de la lectura de l'empremta dactilar, amb la finalitat de control horari?

No, en la mesura que la recollida de dades personals dels treballadors públics es realitzi dins d'una relació jurídica laboral o administrativa i tingui com a finalitat el control, precisament, del seu compliment.

◇ Pot una empresa municipal tractar dades de caràcter personal recollides d'altres webs (números de telèfon, adreces electròniques personals, noms i cognoms...)?

No, llevat que es compti amb el consentiment de les persones afectades. El fet que les dades es trobin accessibles en un web no les converteix en fonts accessibles al públic.

Normativa aplicable: art. 3.j), 6.2 LOPD; 7, 10.3 i 12.1 RLOPD.

2.2 El principi de qualitat de les dades

És el segon dels principis cabdals pel que fa al dret fonamental a la protecció de dades. En realitat es tracta d'un principi que es desgrana en diversos principis que es regulen a la LOPD i al RLOPD.

2.2.1 Principi de proporcionalitat

Només es poden tractar les dades que siguin **adequades, pertinents i no excessives** en relació amb la finalitat del tractament.

2.2.2 Principi de finalitat

Les dades s'han de destinar a la finalitat determinada, explícita i legítima per a la qual es van recollir. És contrari a aquest principi qualsevol ús que se'n faci destinat a una finalitat incompatible amb aquella per a la qual s'hagin recollit. No és incompatible el tractament amb finalitats històriques, estadístiques o científiques.

2.2.3 Principi d'exactitud

Les dades han de ser exactes i posades al dia, per tal de reflectir la situació real de les persones afectades. Quan les dades siguin inexactes s'han de rectificar, no tan sols a petició de la persona afectada en exercici del seu **dret de rectificació**, sinó també d'ofici, en el mateix moment en què l'entitat responsable del tractament tingui coneixement de la inexactitud.

- Si les dades són o esdevenen inexactes, del tot o en part, o incompletes, s'han de **rectificar d'ofici**.
- Si les dades ja no són necessàries o pertinents d'acord amb la finalitat per a la qual es van recollir o enregistrar, s'han de **cancel·lar**.

2.2.4 Conservació

Les dades s'han de cancel·lar quan deixin de ser necessàries o pertinents. Només es poden conservar durant un període superior al necessari per a la finalitat per a la qual es van recollir si s'anonimitzen o es dissocia la informació que contenen, o si es volen conservar, amb l'autorització de l'Autoritat Catalana de Protecció de Dades, atesos els valors històrics, estadístics o científics d'acord amb la legislació específica.

No obstant això, les dades cancel·lades s'han de conservar, a disposició de les administracions públiques, jutges i tribunals, degudament bloquejades durant el transcurs del temps en què es pugui exigir algun tipus de responsabilitat derivada d'una relació o obligació jurídica, de l'execució d'un contracte o de l'aplicació de mesures precontractuals sol·licitades per la persona afectada. Transcorregut aquest termini, s'han de suprimir.

Ara bé, si les dades s'han obtingut per mitjans fraudulents, deslleials o il·lícits, s'han de destruir directament.

Per determinar el període de conservació dels documents cal tenir en compte les previsions sobre avaluació documental contingudes a la normativa d'arxius.

◊ **Es compleix amb l'obligació de cancel·lar les dades si la informació personal s'anonimitza o dissocia de forma irreversible?**

L'anonimització o dissociació d'una dada, de manera que no se'n pugui identificar el titular, compleix aquesta obligació de cancel·lació.

◊ **Durant quant de temps es poden conservar les imatges obtingudes a través d'un sistema de videovigilància?**

En els supòsits en què no es pugui assolir la finalitat perseguida sense emmagatzemar les imatges, el període de conservació no ha de ser superior al que resulti necessari per al compliment de la finalitat de vigilància per a la qual s'han recollit o enregistrat.

Amb caràcter general, es recomana no excedir el termini màxim d'un mes per cancel·lar les imatges.

■ 2.2.5 Principi de lleialtat

Qualsevol entitat que tracti dades personals ho ha de fer de manera **lleial, lícita** i sense emprar **mitjans fraudulents**.

Normativa aplicable: art. 3.f) i 4 LOPD; 9 LA; 5.1.e), 5.1.p), 8 i 157-158 RLOPD; 6, 7 i 8 Instrucció 1/2009; art. 10.2 LUMESPC.

3 Obligacions prèvies al tractament

**Abans d'iniciar la recollida de
les dades, cal disposar del fitxer
corresponent, notificar-lo a l'Autoritat
Catalana de Protecció de Dades i
informar les persones afectades**

La implementació de la normativa de protecció de dades exigeix a les entitats la definició d'un pla d'adequació, que permeti conèixer quina és la situació de tots els fitxers i tractaments de dades personals que es realitzen dins de l'entitat i l'anàlisi de com estan interconnectats. S'ha d'analitzar el "cicle de vida" o recorregut de les dades al llarg del seu tractament, a fi d'identificar:

- Quines dades personals s'han de recollir i per a quina finalitat.
- Com es recolliran (formularis, electrònicament, telefònicament...).
- Quins fitxers cal crear i, si escau, quins fitxers cal modificar o suprimir.
- Qui les tractarà (àrees, departaments, persones usuàries...).
- Com circularan dins l'entitat (en suport paper, telemàticament...).
- A qui es cediran o quines transferències internacionals es duran a terme.
- Com es conservaran i, si escau, com i quan es destruiran.

3.1 La creació, la modificació i la supressió dels fitxers

Quan l'exercici de les funcions pròpies d'un ens local comporti la recollida i el tractament posterior de dades de caràcter personal, independentment que el tractament s'hagi de realitzar de forma automatitzada o no, cal **crear** un o diversos fitxers amb caràcter previ a l'inici del tractament.

Fitxer

Qualsevol conjunt organitzat de dades de caràcter personal que permeti l'accés a les dades d'acord amb criteris determinats, sigui quina sigui la forma o la modalitat de creació, emmagatzematge, organització i accés.

Amb el pas del temps, és possible que determinades circumstàncies obliguin a **modificar** el contingut dels fitxers. Pot ser necessari modificar un fitxer perquè canvia el responsable, o perquè se n'amplien els usos, o perquè cal fer un tractament de dades que no s'havia previst inicialment i que pot comportar, a més, un canvi en el nivell de mesures de seguretat que cal aplicar al fitxer. Qualsevol canvi que afecti, substancialment, el tractament de dades configurat inicialment amb la creació del fitxer fa necessària la modificació d'aquest fitxer.

Finalment, és possible que determinats fitxers s'hagin de **suprimir**. Per exemple, perquè l'ens local deixa de prestar un servei determinat i, en conseqüència, ja no és pertinent tractar determinades dades personals, o perquè les dades que es tractaven en un fitxer passen a formar part d'un altre fitxer, dins el mateix ens local. En aquest cas, cal preveure el destí que tindran les dades i valorar si s'ha de derogar la disposició o acord de creació corresponent, que hagi pogut quedar sense contingut.

Segons quina sigui la naturalesa, pública o privada, de l'entitat responsable del fitxer, els fitxers poden ser de titularitat pública (ens locals, consorcis, organismes autònoms locals, etc...) o privada (societats privades municipals, fundacions, etc...).

◊ Qui és el responsable dels fitxers en el si d'un ens local?

Normalment és l'òrgan administratiu que tracti la informació i tingui competències en la matèria i que tingui capacitat de decidir sobre el contingut, la finalitat i l'ús del tractament de dades que es realitzi. Estarà determinat per l'ordenança municipal o per la disposició que el creï.

Normativa aplicable: art. 3.d), 20 i 25, 44.3.a) LOPD; 5.1.m), n) i q), 52 i s. RLOPD; 9 Instrucció 1/2009; Recomanació 1/2011.

3.1.1 Fitxers de titularitat pública

Fitxer de titularitat pública

Fitxers els responsables dels quals siguin òrgans constitucionals o amb rellevància constitucional de l'Estat o les institucions autonòmiques amb funcions anàlogues a aquests òrgans, les administracions públiques territorials, així com les entitats o organismes que hi estan vinculats o en depenen i les corporacions de dret públic, sempre que, en aquest darrer cas, estiguin vinculats a l'exercici de les potestats de dret públic que els atribueix la seva normativa específica.

Els fitxers de titularitat pública s'han de crear, modificar o suprimir mitjançant una **disposició de caràcter general**, és a dir, una disposició dictada en exercici de la potestat normativa que correspon als ens locals. Aquesta disposició s'ha d'aprovar i publicar amb caràcter previ a l'inici del tractament de les dades.

Instrument d'aprovació:

- En el cas dels ens locals i els ens públics vinculats o que en depenen, els fitxers es poden aprovar per **ordenança o reglament del ple de la corporació**. En el cas de l'ajuntament de Barcelona també es poden aprovar, d'acord amb el seu règim especial, per decret de l'Alcaldia o de la Junta de Govern Local.
- Si es tracta dels fitxers d'un Grup municipal, es poden aprovar per acord del Grup.
- Quan es tracti de consorcis:
 - Si depenen d'un determinat ens local, es poden aprovar per ordenança o reglament de l'ens local.
 - Si la representació de la Generalitat en els seus òrgans de govern és majoritària, es poden aprovar mitjançant ordre del conseller corresponent o decret del Govern de la Generalitat.
 - Si no hi ha una relació de dependència respecte de cap ens local determinat, ni de la Generalitat, es poden aprovar per acord de l'òrgan superior del consorci.

Contingut:

Els articles 20 de la LOPD i 54 del RLOPD exigeixen que la disposició general o acord de **creació** de nous fitxers faci referència a:

- a) La denominació del fitxer o tractament.
- b) La finalitat i els usos previstos.

- c) Les persones o els col·lectius afectats.
- d) El procediment de recollida de les dades personals.
- e) La procedència de les dades personals.
- f) L'estructura del fitxer:
 - Tipologia de les dades, amb descripció detallada de les dades identificatives i, si escau, de les dades especialment protegides, i de les restants categories de dades.
 - El sistema de tractament utilitzat en la seva organització.
- g) Les cessions de dades personals previstes.
- h) Les transferències internacionals de dades personals previstes amb indicació, si escau, dels països de destí de les dades.
 - i) L'òrgan o els òrgans responsables del fitxer.
 - j) Els serveis o les unitats davant les quals es poden exercir els drets d'accés, rectificació, cancel·lació i oposició.
 - k) El nivell de seguretat exigible.

Durant la fase d'elaboració de la disposició, els ens locals poden sol·licitar un informe potestatiu a l'Autoritat Catalana de Protecció de Dades. Es recomana adjuntar, a la sol·licitud de l'informe, una còpia de la memòria de l'expedient. En el cas que es creïn fitxers de videovigilància, la memòria ha d'incloure la informació requerida a l'article 10 de la Instrucció 1/2009.

Pel que fa a la disposició o l'acord de **modificació** del fitxer, s'ha d'indicar en cada cas quins dels anteriors apartats es veuen afectats per la modificació. Es recomana reproduir, a continuació, novament el fitxer sencer amb les modificacions incorporades, per tal de facilitar-ne la recerca a qualsevol persona interessada.

La disposició o l'acord de **supressió** s'ha de fer ressò del destí de les dades o, si escau, de les previsions que s'adoptin per a destruir-les.

Les disposicions o acords de creació, de modificació i de supressió de fitxers s'han de publicar al BOP, i també s'ha incloure una referència al DOGC.

En relació amb la creació, la modificació i la supressió de fitxers, consulteu també la Recomanació 1/2011, de l'Autoritat Catalana de Protecció de Dades sobre la creació, modificació i supressió de fitxers de dades de caràcter personal de titularitat pública.

◊ **Es pot afegir una nova finalitat a un fitxer existent?**

Sí, però només si es tracta d'una finalitat compatible amb la que ja tenia el fitxer. En qualsevol cas cal modificar el fitxer i, si escau, informar-ne les persones afectades.

Normativa aplicable: art. 20.1, 20.3 i 25 LOPD; 49 LRBRL; 39 Llei 13/2008; 5.n) i D.F 3a LACPD; 26 i 27 Llei 22/98; 61 i s. Llei 26/2010; 60 i s. ROAS; 52 i s. RLOPD; 178 TRLMRLC; 9 i 10 Instrucció 1/2009; Recomanació 1/2011.

3.1.2 Fitxers de titularitat privada

Fitxer de titularitat privada

Fitxers els responsables dels quals siguin persones, empreses o entitats de dret privat, amb independència de qui tingui la titularitat del seu capital o de la procedència dels seus recursos econòmics, així com els fitxers els responsables dels quals siguin corporacions de dret públic no vinculats a l'exercici de les potestats de dret públic que els atribueix la seva normativa específica.

En la **creació** de fitxers de titularitat privada, com el cas de les societats municipals o altres ens dependents que siguin de dret privat, hi ha llibertat de forma. A diferència dels fitxers de titularitat pública, no es requereix l'aprovació de cap disposició. N'hi ha prou amb la voluntat del responsable del fitxer (és a dir, la decisió conforme es volen crear uns fitxers destinats a una finalitat concreta, quan sigui necessari per assolir l'activitat o l'objecte legítim de l'entitat titular), i la notificació al Registre de Protecció de Dades de Catalunya.

◇ Es pot incloure un fitxer de titularitat privada dins d'una disposició de creació de fitxers de titularitat pública?

Sí, és possible. Això, però, no alterarà la seva naturalesa privada i condicionarà la seva futura modificació i supressió, atès que també s'haurà de fer mitjançant una disposició general.

Normativa aplicable: art. 25 LOPD; 5.1.I), 55 i s. RLOPD.

3.2 La notificació dels fitxers o tractaments

La creació o, si escau, la modificació o la supressió dels fitxers s'ha de **notificar** al Registre de Protecció de Dades de Catalunya de l'Autoritat Catalana de Protecció de Dades. Un cop inscrits, l'Autoritat en dona trasllat al Registre General de Protecció de Dades de l'Agència Espanyola de Protecció de Dades.

- El termini per presentar les sol·licituds d'inscripció és de 30 dies des de la seva publicació.
- Els fitxers **s'inscriuran** un cop verificat el compliment dels requisits legalment establerts a la LOPD i el RLOPD.
- Transcorregut un mes des de la presentació de la sol·licitud d'inscripció, sense que s'hagi resolt, s'entendrà inscrit el fitxer a tots els efectes.

La inscripció dels fitxers ha d'estar permanentment **actualitzada**. Qualsevol modificació que afecti el seu contingut s'ha de notificar a l'Autoritat Catalana de Protecció de Dades.

◇ A qui correspon notificar la creació, la modificació o la supressió del fitxer?

Al responsable del fitxer.

◇ **A quin registre ha de notificar els seus fitxers una empresa privada que disposi d'una concessió pública?**

Sempre que els fitxers estiguin directament vinculats a la prestació del servei objecte de la concessió, es trobaran dins l'àmbit d'actuació de l'Autoritat Catalana de Protecció de Dades i, per tant, s'han de notificar al Registre de Protecció de Dades de Catalunya.

◇ **On s'ha de fer la notificació en el cas que es vulguin modificar o suprimir uns fitxers prèviament inscrits al Registre General de Protecció de Dades de l'Agència Espanyola de Protecció de Dades, però que ara es trobin dins l'àmbit d'actuació de l'Autoritat Catalana de Protecció de Dades?**

Tant les modificacions com les supressions dels fitxers inscrits al Registre General de Protecció de Dades que es trobin dins l'àmbit d'actuació de l'Autoritat Catalana de Protecció de Dades s'han de tramitar davant el Registre de Protecció de Dades de Catalunya.

Normativa aplicable: art. 26 LOPD; 5.i) LACPD; 55 i s. 130 i 131 RLOPD; 11 Instrucció 1/2009; Recomanació 1/2011; Res. APDCAT 04.04.2011.

3.3

La informació a la persona titular de les dades

Per poder iniciar el procediment de recollida de les dades, i amb independència que sigui necessari el consentiment o es compti amb habilitació legal, el responsable del tractament ha de garantir el dret d'informació a cadascuna de les persones afectades. La seva omissió pot comportar un vici del consentiment.

Correspon al responsable del fitxer o tractament poder acreditar el compliment d'aquesta obligació.

Les persones titulars de les dades han de ser informades prèviament de forma **expressa, precisa i inequívoca** sobre:

- a) L'existència d'un fitxer o un tractament de dades de caràcter personal, la finalitat de la recollida de les dades i els destinataris de la informació.
- b) El caràcter obligatori o facultatiu de la resposta a les preguntes que els siguin plantejades.
- c) Les conseqüències de l'obtenció de les dades o de la negativa a subministrar-les.
- d) La possibilitat d'exercir els drets d'accés, rectificació, cancel·lació i oposició.
- e) La identitat i la direcció del responsable del tractament o, si escau, del seu representant.

(No és necessari donar la informació dels apartats b), c) i d) si es dedueix clarament de la naturalesa de les dades o de les circumstàncies concurrents)

Quan s'utilitzin formularis o impresos per recollir les dades, aquests han d'incorporar, de forma clara i llegible, les advertències anteriors, amb independència que sigui o no necessari recollir el consentiment.

També es pot donar compliment a aquest deure d'altres maneres, com ara missatges pregravats, comunicacions per escrit, cartells, etc. que siguin aptes per a que el ciutadà tingui ple coneixement d'aquesta informació, d'acord amb el mitjà emprat per a la recollida.

Si les dades no es recullen directament del seu titular, sinó que les cedeix o comunica una tercera persona, se l'ha d'informar, dins dels tres mesos següents al moment de rebre les dades, de manera **expressa, precisa i inequívoca** sobre:

- a) El contingut del tractament.
- b) La procedència de les dades.
- c) L'existència d'un fitxer o un tractament de dades de caràcter personal, de la finalitat de la recollida de les dades i dels destinataris de la informació.
- d) La possibilitat d'exercir els drets d'accés, rectificació, cancel·lació i oposició.
- e) La identitat i la direcció del responsable del tractament o, si escau, del seu representant.

(La informació dels apartats c), d) i e) només s'ha de facilitar si no s'ha informat la persona titular anteriorment)

Excepcions al deure d'informació:

- Quan el compliment del deure d'informació afecti la defensa nacional, la seguretat pública o la persecució d'infraccions penals, no és obligatori el compliment del deure d'informació.
- Si les dades no es recullen directament del seu titular, en els supòsits següents:
 - a) Quan una llei prevegi expressament la comunicació.
 - b) Quan el titular ja n'hagi estat informat amb anterioritat.
 - c) Quan el tractament tingui finalitats històriques, estadístiques o científiques.
 - d) Quan resulti impossible o exigeixi esforços desproporcionats, amb autorització de l'Autoritat Catalana de Protecció de Dades.
 - e) Quan les dades procedeixin de fonts accessibles al públic i es destinin a l'activitat de publicitat o prospecció comercial.

◊ **Quan no és necessari el consentiment, cal informar igualment?**

Sí. El deure d'informació s'ha de complir en tots els casos, llevat que concorri alguna de les excepcions descrites.

◊ **Quines mesures es requereixen per complir amb el deure d'informació, en els supòsits de sistemes de videovigilància?**

Les persones responsables del tractament d'imatges a través de càmeres fixes han d'informar de forma clara i permanent sobre l'existència de les càmeres, encara que les imatges no s'enregistren, mitjançant la col·locació dels cartells informatius que siguin necessaris per garantir-ne el coneixement, d'acord amb els requisits de l'article 12 de la Instrucció 1/2009.

Normativa aplicable: art. 5, 24 LOPD; 5.p) LACPD; 13.3 RLOPD; 12 Instrucció 1/2009.

4 Obligacions durant el tractament de les dades

Els principis i les obligacions i les garanties previstes per la normativa de protecció de dades s'han de tenir en compte no només en el moment de la recollida de les dades, sinó també durant qualsevol fase del tractament

La persona afectada disposa d'una sèrie de garanties encaminades a assegurar l'adequació del tractament de les seves dades personals a la normativa vigent, que són d'aplicació durant la recollida, l'emmagatzematge, la utilització o la comunicació de les dades de caràcter personal i fins i tot després que finalitzi la relació jurídica. Aquestes garanties són:

- El deure de secret.
- Els drets d'accés, rectificació, cancel·lació i oposició.
- La implementació de mesures de seguretat.

4.1 El deure de secret

El responsable del fitxer i totes les persones que intervinguin en qualsevol de les fases del tractament de dades de caràcter personal estan obligades a guardar secret professional respecte d'aquestes dades.

Aquesta obligació subsisteix fins i tot després de la finalització de les seves relacions amb el responsable.

Per tal de garantir el compliment d'aquest deure, és recomanable incorporar i definir aquesta obligació en els contractes laborals, en els protocols interns i en les regulacions específiques que recullen els drets i les obligacions de les parts en una relació jurídica que comporti el tractament de dades de caràcter personal.

Normativa aplicable: art. 10 LOPD; 83 i 123 RLOPD; 164.6 TRLMRLC.

4.2 La comunicació de dades personals

Tot i la vigència del deure de secret, hi ha determinats supòsits en què l'exercici de les competències de l'ens local o d'altres administracions o entitats públiques pot comportar la necessitat de comunicar determinades dades a terceres persones o entitats. En aquests casos, cal subjectar-se al règim de cessions o comunicacions previst a la LOPD.

Cessió o comunicació de dades personals

Tota revelació de dades personals feta a una persona diferent a la persona afectada.

■ 4.2.1 Requisites:

Per tal que una cessió o comunicació sigui legítima, ha de complir amb **dos requisits**:

- Que respongui al compliment de les **finalitats** directament relacionades amb les funcions legítimes del cedent i del cessionari.
- Que s'hagi obtingut el **previ consentiment** de la persona afectada o que concorri alguna de les circumstàncies següents:
 - a) Estigui autoritzada per una llei.
 - b) Es tracti de dades recollides de fonts accessibles al públic.
 - c) Respongui a la lliure i legítima acceptació d'una relació jurídica que impliqui necessàriament la comunicació.
 - d) El destinatari sigui el Defensor del Poble, el Ministeri Fiscal i els jutges o tribunals o els tribunals de comptes i les institucions autonòmiques anàlogues, en l'exercici de les seves funcions.
 - e) En dades relatives a la salut, en casos d'urgència o per elaborar estudis epidemiològics.

La comunicació de dades **entre administracions públiques** està específicament regulada a la LOPD, que preveu la possibilitat de cedir dades a una altra administració pública sense disposar del consentiment de les persones afectades quan:

- Es comuniquin per a l'exercici de les mateixes competències.
- Es comuniquin per a l'exercici de competències que versin sobre la mateixa matèria.
- La comunicació tingui per objecte el tractament de les dades amb finalitats històriques, científiques o estadístiques.
- Una administració pública les obtingui o elabori amb destinació a una altra administració.

◇ **Es poden cedir dades del padró municipal a persones físiques o jurídiques de naturalesa privada diferents de la persona afectada?**

Com que les persones físiques o jurídiques de naturalesa privada no són administracions públiques, no escau cedir-les, atès que resulta contrari a les previsions de la LOPD, la LRBRL i el TRLMRLC, llevat que es compti amb el consentiment de les persones afectades o d'algun supòsit previst a la legislació vigent.

◇ **Pot un ajuntament comunicar individualment als seus ciutadans les dades que consten al padró municipal d'habitants, a través de consultes telefòniques?**

Sí, quan es tracti de la persona titular de les dades, sempre que s'estableixin mecanismes per assegurar que la persona que sol·licita la informació realment ho sigui.

◇ **Es poden utilitzar les dades del padró municipal per a proposar a tots els veïns la possibilitat d'inscriure's en un nou registre de l'ajuntament, per poder rebre informació de caràcter municipal?**

Sí, és possible accedir a les dades del nom i el domicili dels veïns del municipi que consten al padró municipal, atès que es tracta de dades necessàries per a l'exercici de les pròpies competències en què la dada relativa al domicili és una dada rellevant, tal com requereix la LRBRL i el TRLMRLC.

◇ **És conforme a les previsions de la LOPD la publicació de les dades de persones presumptament infractores en matèria de trànsit en un diari oficial?**

La publicació de dades de persones presumptament infractores en matèria de trànsit a les quals no s'hagi pogut practicar la notificació personal constitueix una comunicació de dades personals a efectes de la LOPD. Aquesta comunicació troba habilitació a l'article 59.5 de la LRJPAC, mentre no entri en vigor el nou sistema de notificacions electròniques i el tauler electrònic d'edictes de sancions de trànsit.

Pot resultar adequat a la LOPD publicar les dades relatives al nom i cognoms de la persona infractora i, si escau, amb les quatre darreres xifres del número de DNI, juntament amb una identificació del número d'expedient i una referència succinta al tràmit que es notifica.

◇ **La difusió d'informació que contingui dades personals a les seues electròniques o pàgines web dels ens locals, es troba sotmesa a la normativa sobre protecció de dades?**

Sí. La difusió, entesa com la comunicació d'informació que conté dades personals a través d'Internet, intranet o extranet, adreçada a una pluralitat indeterminada de destinataris, s'ha de considerar com a cessió o comunicació de dades als efectes de la LOPD i, per tant, està sotmesa a aquesta normativa.

◇ **Pot un ajuntament difondre, en la seva pàgina web, les dades personals contingudes en les actes de les sessions del ple?**

Quan les actes inclouen dades personals, la seva difusió constitueix un tractament de dades sotmès a la LOPD. D'acord amb l'article 10.2 de la LUMESPC, es poden difondre sense comptar amb el consentiment de la persona interessada les dades referents a actes debatuts al ple de la corporació o a disposicions objecte de publicació en el butlletí oficial corresponent, tenint en compte els principis i garanties que estableix la normativa de protecció de dades i la de protecció del dret a l'honor i la intimitat. En la resta de supòsits, sens perjudici del que disposin altres lleis, la publicació únicament és possible si es compta amb el consentiment o les dades no es poden, en cap cas, vincular amb la persona interessada.

◇ **S'adequa a la LOPD la possibilitat que un ciutadà consulti les seves dades corresponents al cens electoral a través de la pàgina web de l'ajuntament?**

Sí, si l'accés es limita a les pròpies dades. No constitueix una cessió de dades, atès que el ciutadà que accedeix a la web i sol·licita la informació només rep la corresponent a la seva persona. Per tant, es pot consultar sempre que s'implantin les mesures de seguretat adients per comprovar la identitat de qui fa la consulta.

◇ **Pot un ajuntament remetre periòdicament a la Generalitat una relació dels veïns que tinguin deutes pendents amb la tresoreria municipal, per tal que els sigui denegada qualsevol subvenció que sol·licitin?**

No, perquè es tracta de finalitats diferents. No obstant això, es poden comunicar, a petició de l'ens requeridor, si la persona afectada ho ha autoritzat o ho ha declarat en una declaració responsable.

Normativa aplicable: art. 3.i), 11, 21 i 27 LOPD; 5.1.c) ,10 RLOPD; Recomanació 1/2008; 69 i s. LRBRL; 154 i s. TRLMRLC; 35 Llei 26/2010.

■ 4.2.2 L'encarregat del tractament

No es considera comunicació de dades l'accés d'un tercer a les dades de caràcter personal, quan aquest accés sigui necessari per a la prestació d'un servei al responsable del tractament.

Aquesta prestació ha d'estar regulada per un contracte o acord d'encàrrec, per escrit o en alguna altra forma que permeti acreditar-ne la celebració i contingut, el qual ha d'establir:

- a) Que únicament tractarà les dades conforme a les instruccions del responsable del tractament.
- b) Que no utilitzarà les dades amb una finalitat diferent de la predeterminada en el contracte.
- c) Que no comunicarà les dades, ni tan sols per a la seva conservació, a tercers persones.
- d) Les mesures de seguretat.

Encarregat del tractament

Persona física o jurídica, pública o privada, o òrgan administratiu que, sol o conjuntament amb altres, tracti dades personals per compte del responsable del tractament o del responsable del fitxer, com a conseqüència de l'existència d'una relació jurídica que l'hi vincula i delimita l'àmbit de la seva actuació per a la prestació d'un servei. També poden ser encarregats del tractament els ens sense personalitat jurídica que actuïn en el tràfic com a subjectes diferenciats.

En els contractes sotmesos a la legislació de contractes del sector públic, l'acord o contracte d'encàrrec ha de constar necessàriament **per escrit**.

En el cas que l'encarregat del tractament **incompleixi** alguna d'aquestes obligacions, es considerarà com a responsable del tractament i li seran imputables, personalment, les infraccions que hagi comès.

Un cop complerta la prestació contractual, les dades s'han de **destruir o restituir** al responsable del tractament o a l'encarregat que hagi designat.

- En els casos en què hi hagi una previsió legal que n'exigeixi la conservació, s'han de restituir al responsable garantint-ne la conservació.

- L'encarregat pot conservar les dades, degudament bloquejades, per atendre possibles responsabilitats.

Per a l'anàlisi d'aquesta figura amb més detall, ens remetem a la Recomanació 1/2010.

◊ **Qui és el responsable del fitxer que conté les dades relatives a la recaptació dels tributs locals, quan aquesta funció la duu a terme una entitat col·laboradora per compte d'un ajuntament?**

El responsable del fitxer és l'ajuntament corresponent, mentre que el recaptador és un encarregat del tractament, sempre que se subscrigui el corresponent contracte o acord d'encàrrec, d'acord amb l'article 12 de la LOPD.

◊ **Pot un ajuntament comunicar les dades relatives a la titularitat dels béns immobles situats en el terme municipal a una empresa concessionària del servei de subministrament d'aigua potable?**

Sí, sempre que se subscrigui el corresponent contracte o acord d'encàrrec, d'acord amb l'article 12 de la LOPD.

◊ **Per tal que un ens instrumental tracti dades per compte d'un ajuntament, n'hi ha prou que aquest li doni certes indicacions o instruccions?**

No. Quan l'ens instrumental accedeix, per compte de l'ajuntament, a dades personals que es tracten sota la responsabilitat de l'ajuntament, ha de fer-ho a través del corresponent contracte, conveni o acord, en els termes de l'article 12 de la LOPD.

Normativa aplicable: art. 3.g), 9 i 12 LOPD; D.A. 26 TRLCSP; 20 i s. 82 RLOPD; Recomanació 1/2010.

■ 4.2.3 Accés dels regidors a informació municipal

L'accés a informació municipal que conté dades personals per part dels regidors no és pròpiament un supòsit de cessió o comunicació de dades, en els termes de l'article 3.i) de la LOPD, atès que un regidor, que és part integrant del consistori, no pot ser considerat com un tercer aliè a la relació que s'estableix entre l'ajuntament i la persona titular de les dades personals.

La normativa aplicable atorga als regidors municipals un dret d'accés específic a la informació de l'ajuntament, per a l'exercici de les funcions que els corresponen.

La concurrència d'aquest dret específic amb el dret a la protecció de dades personals requereix ponderar si l'accés a informació per part dels regidors és necessari per desenvolupar les funcions que tenen atribuïdes. Això fa especialment rellevant l'aplicació del principi de qualitat.

Quan els regidors accedeixen a dades personals incloses en la informació municipal, queden subjectes als principis i obligacions de la LOPD, entre d'altres el deure de secret.

◊ **Poden els regidors de l'oposició accedir a informació municipal?**

Sí. La normativa aplicable atorga a tots els membres de les corporacions locals, independentment que formin part del govern municipal o de l'oposició, el dret a obtenir de l'alcalde o alcaldessa, o del president o presidenta, o de la comissió de govern, els antecedents, dades o informacions en poder dels serveis de la corporació que resultin necessaris per desenvolupar les funcions que cada regidor tingui encomanades.

◊ **Poden els regidors accedir a les dades de caràcter personal del padró municipal d'habitants? Poden accedir-hi per a qualsevol finalitat?**

Els regidors, com a membres de la corporació, poden accedir a les dades dels fitxers d'aquesta, entre els quals el fitxer del padró municipal d'habitants, sense previ consentiment dels afectats, sempre que sigui necessari pel desenvolupament de les funcions que els atribueix la legislació de règim local.

Els regidors no poden accedir a la informació per a l'exercici de finalitats no relacionades amb l'exercici de les seves funcions, com podrien ser, entre d'altres, les pròpies de l'activitat política del partit al qual pertanyen.

◊ **Els regidors han de justificar el motiu de la seva petició d'accés a informació municipal?**

Com es desprèn de la LRBRL i de la jurisprudència del Tribunal Suprem, als regidors no se'ls exigeix que expliquin o fonamentin la finalitat de la seva petició d'accés a la informació, que s'entén implícita en l'exercici de les seves funcions. No obstant això, quan la petició pugui entrar en conflicte amb altres drets, atès que l'ajuntament ha de fer una ponderació en què s'han de tenir en compte la finalitat, les circumstàncies del cas, les dades personals afectades, etc., és convenient i recomanable que els regidors concretin la finalitat de la seva petició.

Normativa aplicable: art. 4 i 10 LOPD; 19.1, 77 LRBRL; 164 TRLMRLC.

■ **4.2.4 Accés d'altres àrees de l'ajuntament a informació municipal**

Els òrgans o les àrees de l'ajuntament formen part de l'administració municipal, que actua sota una personalitat jurídica única. Per tant, les informacions que circulin entre aquests diferents òrgans no tenen, des del punt de vista de la normativa de protecció de dades, la consideració de comunicació. Tot això sens perjudici que la utilització de les dades per part d'altres òrgans o àrees, diferents a aquelles que les van recollir, està sotmesa al principi de finalitat.

■ 4.2.5 Transferències internacionals de dades

Són transferències internacionals de dades totes les comunicacions de dades amb un destinatari situat fora del territori de l'espai econòmic europeu.

Aquest tipus de comunicacions requereixen que la legislació del país destinatari proporcioni un nivell adequat de protecció. Altrament, és necessari obtenir autorització del director o directora de l'Agència Espanyola de Protecció de Dades.

No obstant això, la normativa estableix una sèrie de supòsits en què es permet la transferència internacional de dades sense necessitat d'autorització:

- a) Quan resulti de l'aplicació d'un tractat o conveni del qual Espanya en sigui membre.
- b) Quan tingui per objecte donar o sol·licitar auxili judicial internacional.
- c) Quan sigui necessària per al diagnòstic o l'assistència sanitària.
- d) Quan faci referència a transferències dineràries.
- e) Quan la persona afectada hagi donat el seu consentiment inequívoc.
- f) Quan sigui necessari per executar un contracte entre la persona afectada i el responsable del fitxer, o entre aquest últim i un tercer quan sigui en interès de la persona afectada.
- g) Quan sigui necessària o legalment exigida per a salvaguardar un interès públic.
- h) Quan es requereixi per a l'exercici d'un dret dins d'un procediment judicial.
- i) Quan la petició l'efectuï una persona amb un interès legítim des d'un Registre públic.

Normativa aplicable: art. 20.2.e), 33 i 34 LOPD; 54.1.e), 65 i s. 137 i s. RLOPD.

4.3 Els drets d'habeas data

Les persones titulars de les dades, com a part del seu dret a l'autodeterminació informativa, disposen dels drets d'accés, rectificació, cancel·lació i oposició. Aquests drets, coneguts com drets d'habeas data o amb l'acrònim de drets ARCO, es caracteritzen per ser:

a) **Personalíssims:** només els pot exercir la persona titular de les dades, llevat dels supòsits següents:

- Quan la persona afectada es trobi en situació d'incapacitat o minoria d'edat, que l'impossibiliti l'exercici d'aquests drets, els pot exercir el representant legal.
- Quan s'actui mitjançant un representant voluntari:

Si es tracta de fitxers privats, cal aportar còpia del DNI o equivalent i de la representació conferida. La utilització de signatura electrònica identificativa

de la persona afectada exigeix de la presentació de les fotocòpies del DNI o document equivalent.

Si es tracta de fitxers de les administracions públiques, s'ha d'acreditar la representació per qualsevol mitjà vàlid en dret, que en deixi constància fidedigna, o mitjançant la compareixença personal de la persona afectada.

b) **Independents:** en cap cas l'exercici d'un d'aquests drets constitueix un requisit previ per a l'exercici d'un altre.

c) **Gratuits:** l'exercici d'aquests drets s'ha de poder fer per un mitjà senzill i no pot suposar un ingrés addicional per al responsable del tractament.

L'exercici dels drets ARCO pot veure's modulats per motius de seguretat pública o relatius a l'hisenda pública, en els casos previstos legalment.

Normativa aplicable: art. 15-18 i 22-23 LOPD.

■ 4.3.1 Dret d'accés

Mitjançant aquest dret, la persona afectada té dret a conèixer:

- Les dades de caràcter personal que siguin objecte de tractament.
- La finalitat del tractament.
- L'origen d'aquestes dades.
- Les comunicacions que s'han fet o que s'han previst fer.

El dret es pot exercir en relació amb dades concretes, dades incloses en un determinat fitxer o la totalitat de les seves dades sotmeses a tractament.

- En casos d'especial complexitat, el responsable del fitxer pot facilitar a la persona afectada una llista dels seus fitxers i demanar-li que especifiqui respecte de quins pretén exercir el seu dret.
- El responsable del fitxer disposa de 30 dies a partir de la recepció de la sol·licitud, per notificar la resposta a la persona afectada. Si la resolució és estimatòria, cal fer efectiu l'accés en el termini de 10 dies.
- El responsable del fitxer pot denegar l'accés, en els casos en què ja s'hagi exercit el mateix dret en els dotze mesos anteriors a la sol·licitud, llevat que la persona interessada acrediti un interès legítim que ho justifiqui.

La persona afectada pot demanar que el dret d'accés es faci efectiu a través dels **sistemes de consulta** següents:

- Visualització en pantalla.
- Escrit, còpia o fotocòpia, per correu certificat o ordinari.
- Correu electrònic o altres sistemes de comunicació electrònica.
- Qualsevol altre sistema que sigui adequat a les característiques del fitxer.
- Si el responsable ofereix un determinat sistema per fer efectiu el dret d'accés i la persona afectada el rebutja, el responsable no ha de respondre dels riscos que per a la seguretat de la informació es puguin derivar de l'elecció.

- Si la persona afectada exigeix que el dret d'accés es materialitzi mitjançant un procediment que implica un cost desproporcionat respecte de l'ofert pel responsable, amb els mateixos efectes i garantint la mateixa seguretat, les despeses derivades de la seva elecció aniran a càrrec de la persona afectada.

◊ **És possible denegar l'exercici del dret d'accés per la dificultat o l'elevat cost que pugui suposar a l'entitat local?**

No, atès que la LOPD preveu que les dades de caràcter personal s'han d'emmagatzemar de forma que permetin l'exercici del dret d'accés, excepte un cop hagin estat legalment cancel·lades. Ara bé, aquest dret només es podrà exercir en intervals no inferiors de 12 mesos, excepte que s'acrediti un interès legítim que ho justifiqui.

◊ **Poden els hereus exercir el dret d'accés?**

Atès que la mort extingeix la personalitat civil, els hereus no poden exercir el dret d'accés de l'article 15 de la LOPD, sens perjudici que altres normes sí que els puguin reconèixer el dret a accedir a determinada informació.

Normativa aplicable: art. 15 LOPD; 9.2 LOVFC; 2.4 i 27 i s. RLOPD; 9.1 Decret 78/2010; 15 Decret 134/1999; 13 Instrucció 1/2009.

■ 4.3.2 Dret de rectificació

Mitjançant aquest dret, la persona afectada pot demanar al responsable del fitxer que rectifiqui les dades que siguin inexactes o incompletes. La sol·licitud ha d'indicar la dada o les dades errònies i la correcció corresponent i ha d'anar acompanyada de la documentació que ho justifica.

- El responsable del fitxer ha de resoldre sobre la sol·licitud de rectificació en el termini de 10 dies des de la seva recepció.
- Si les dades rectificades s'han cedit prèviament, el responsable del fitxer ha de notificar al destinatari les rectificacions efectuades en un termini de 10 dies des de la resolució, per tal que també les rectifiqui, també en un termini de 10 dies.
- No es pot fer efectiu el dret de rectificació quan ho impedeixi una llei o una norma de dret comunitari d'aplicació directa.
- No es pot fer efectiu el dret de rectificació quan una llei o norma de dret comunitari d'aplicació directa impedeixin revelar l'existència del tractament.

◊ **Es pot exercir el dret de rectificació respecte de dades que constin als fitxers de la hisenda municipal?**

Sí, es pot exercir. No obstant això, es pot denegar en aquells casos en què l'exercici del dret de rectificació pugui obstaculitzar les actuacions administratives destinades a assegurar el compliment de les obligacions tributàries i, en tot cas, quan la persona afectada sigui objecte d'actuacions inspectores.

Pel que fa a les dades relatives al domicili fiscal, no es poden modificar llevat que aquest no coincideixi amb el domicili fiscal declarat per la persona afectada, atès el que disposa l'article 48 de la Llei General Tributària.

Normativa aplicable: art. 16, 23.2 LOPD; 31 i s. RLOPD; 14 Instrucció 1/2009.

■ 4.3.3 Dret de cancel·lació

Mitjançant aquest dret, la persona afectada pot demanar al responsable del fitxer que supprimeixi les dades que siguin inadequades o excessives. La sol·licitud ha d'indicar les dades a què es refereix i ha d'anar acompanyada de la documentació que ho justifica.

- El responsable del fitxer ha de resoldre sobre la sol·licitud de cancel·lació, en el termini de 10 dies des de la seva recepció.
- Si les dades rectificades s'han cedit prèviament, el responsable del fitxer ha de notificar al destinatari les rectificacions efectuades en un termini de 10 dies des de la resolució, per tal que també les cancel·li, també en un termini de 10 dies.
- No es poden cancel·lar les dades:
 - Quan s'hagin de conservar durant un període de temps per motius legals o contractuals.
 - Quan ho impedeixi una llei o norma de dret comunitari d'aplicació directa.
 - Quan una llei o norma de dret comunitari d'aplicació directa impedeixin al responsable revelar el tractament de les dades a què es refereix la cancel·lació.

La cancel·lació de les dades dóna lloc al bloqueig. El **bloqueig** implica que les dades es poden conservar exclusivament a disposició de les administracions públiques, els jutjats i els tribunals, per atendre les possibles responsabilitats nascudes del tractament, mentre no hagin prescrit aquestes responsabilitats. Un cop transcorregut aquest termini es poden suprimir les dades.

Bloqueig

Identificació i reserva de les dades personals, amb la finalitat d'impedir-ne el tractament excepte per posar-les a disposició de les administracions públiques, jutges i tribunals, per a atendre les possibles responsabilitats nascudes del tractament i només durant el termini de prescripció de les responsabilitats esmentades.

◇ Poden els hereus exercir el dret de cancel·lació?

Les persones vinculades al difunt, per raons familiars o anàlogues, poden notificar l'òbit al responsable del tractament i sol·licitar la cancel·lació de les dades.

Normativa aplicable: art. 16 LOPD; 9.2 LOVFC; 2.4 i 31 i s. RLOPD; 9.2 Decret 78/2010; 15 Decret 134/1999; 15 Instrucció 1/2009.

■ 4.3.4 Dret d'oposició

L'exercici d'aquest dret per part de les persones afectades impedeix a les entitats tractar les seves dades personals o, si el tractament s'hagués iniciat anteriorment, obliga a cessar-ne el tractament, en algun dels supòsits següents:

- Quan, en tractaments per als quals no sigui necessari el consentiment de la persona afectada, hi hagi un motiu legítim i fundat referit a la seva situació personal concreta que ho justifiqui, sempre que una llei no disposi el contrari.

- Quan es tracti de fitxers destinats a activitats publicitàries i de prospecció comercial.
- Quan el tractament tingui com a finalitat l'adopció d'una decisió amb efectes jurídics referida a la persona afectada, basada únicament en un tractament automatitzat.

El responsable del fitxer ha de resoldre sobre la sol·licitud d'oposició en el termini de 10 dies des de la seva recepció.

◊ **Pot un veí demanar que el seu nom, o altres dades personals, no apareguin en un llistat que l'ajuntament ha d'exposar públicament per mandat legal?**

En els casos en què no es requereix el consentiment de la persona per tractar determinades dades, com podria ser l'exposició pública d'una llista de persones que els ajuntaments han d'exposar per mandat legal, la persona titular de les dades pot exercir el seu dret d'oposició per tal que, per motius justificats relatius a la seva situació personal (com per exemple motius relatius a la seguretat o la integritat física), les seves dades personals no es difonguin.

Normativa aplicable: art. 6.4 LOPD; 34 i s. 50 RLOPD; 9.3 Decret 78/2010; 16 Instrucció 1/2009.

■ 4.3.5 Procediment per exercir els drets ARCO

El **procediment** que s'ha de seguir per exercir els drets ARCO és el següent:

a) Sol·licitud de la persona afectada adreçada al responsable del fitxer o, si escau, a l'encarregat del tractament (el responsable del tractament pot demanar l'esmena de la sol·licitud, en el cas que no es compleixin els requisits establerts a l'article. 25.1.a) del RLOPD).

- Convé fer-ho amb un mitjà que permeti acreditar la recepció de la sol·licitud.
- Quan l'entitat responsable disposi d'un servei d'atenció al públic o d'exercici de reclamacions, la persona afectada s'hi pot adreçar per tal d'exercir els seus drets ARCO.
- Els drets es poden exercir també davant l'encarregat del tractament. En aquest cas, l'encarregat ha de traslladar la sol·licitud al responsable del fitxer perquè la resolgui, excepte en els casos en què el contracte d'encarregat del tractament l'habiliti a resoldre les sol·licituds per compte del responsable.

b) El responsable del fitxer ha de contestar la sol·licitud, amb independència que en el fitxer hi figurin o no dades personals de qui ha presentat la sol·licitud, dins del termini establert:

Dret d'accés: 30 dies

Resta de drets: 10 dies

El responsable del fitxer ha de formar els membres de la seva organització perquè puguin informar del procediment d'exercici dels drets ARCO i, si escau, tramitar-los de forma diligent.

◇ **Cal atendre la sol·licitud de les persones afectades que no hagin emprat el mitjà establert pel responsable?**

Sí, sempre que s'hagi utilitzat un mitjà que permeti acreditar l'enviament i la recepció de la sol·licitud en els termes de l'article 25.1 RLOPD.

◇ **Cal respondre la sol·licitud quan ja s'hagin destruït les dades?**

Sí, les sol·licituds d'exercici dels drets sempre s'han de respondre de forma expressa i dins el termini establert.

Normativa aplicable: art. 17 LOPD; 25, 44, 50, 117 i s. RLOPD; 17 Instrucció 1/2009.

■ 4.3.6 Reclamació de tutela de drets

La tutela de drets s'exerceix mitjançant un procediment que es tramita davant l'Autoritat Catalana de Protecció de Dades i que s'inicia a instància de la persona afectada:

- Per exercir els seus drets el ciutadà s'ha d'adreçar al responsable del fitxer. En el cas que no es doni resposta a aquesta petició dins del termini legalment establert, o es denegui l'exercici d'un d'aquests drets, pot adreçar-se a l'Autoritat Catalana de Protecció de Dades mitjançant una reclamació de tutela de drets.
- L'Autoritat trasllada la reclamació al responsable del fitxer i, una vegada rebudes les al·legacions dins del termini legalment establert i practicades totes les proves, ha de dictar i notificar una resolució que resolgui sobre la reclamació, en el termini de sis mesos des de la data d'entrada de la reclamació. Si no es resol dins d'aquest termini, la reclamació de tutela es considera desestimada per silenci administratiu.
- Quan la resolució de la reclamació sigui estimatòria, s'ha de requerir el responsable del fitxer per a què, en el termini dels 10 dies següents a la notificació, faci efectiu l'exercici del dret reclamat.

Normativa aplicable: art. 18 LOPD; 5.b) i 16 LACPD; 117 i s. RLOPD.

4.4 Mesures de seguretat

4.4.1 Implementació de les mesures de seguretat

Un tractament correcte de les dades personals requereix que responsables i encarregats del tractament implementin una sèrie de mesures de seguretat, adequades a les diferents tipologies de dades que es tracten.

Correspon al **responsable** del fitxer i, si escau, al responsable del tractament, adoptar les mesures necessàries en cada cas, tenint en compte l'estat de la tecnologia, la naturalesa de les dades emmagatzemades, el sistema de tractament emprat (automatitzat o no) i els riscos als quals estiguin exposats, ja siguin provinents de l'acció humana o del medi físic o natural. Quan hi ha un **encarregat del tractament**, li són d'aplicació les mateixes obligacions relatives a les mesures de seguretat que al responsable, d'acord amb el que s'estableixi en el contracte d'encàrrec del tractament.

Les mesures de seguretat poden ser tant de caràcter tècnic com organitzatiu i estan destinades a evitar l'alteració, la pèrdua o l'accés a les dades de caràcter personal per part de tercers no autoritzats.

El RLOPD estableix les mesures necessàries d'acord amb el tipus de dades tractades i el suport en el qual estiguin emmagatzemades. Les mesures de seguretat es **classifiquen en tres nivells de seguretat** que tenen la condició de mínims exigibles:

- **Bàsic:** les han d'adoptar tots els fitxers o tractaments de dades personals.
- **Mitjà:** s'apliquen, juntament amb les de nivell bàsic, als fitxers o tractaments que tinguin per objecte dades relatives a:
 - a) La comissió d'infraccions administratives o penals.
 - b) Informació sobre la solvència patrimonial i crèdit que tractin entitats que presten aquests serveis.
 - c) L'exercici de potestats tributàries per part d'administracions tributàries.
 - d) La prestació de serveis financers per entitats financeres.
 - e) L'exercici de competències de les entitats gestores de la seguretat social i mútues d'accidents de treball i malalties professionals.
 - f) L'avaluació de la personalitat o el comportament dels individus.

Els fitxers dels operadors de serveis de comunicacions electròniques disponibles al públic o xarxes públiques de comunicacions electròniques, que continguin dades relatives al trànsit i la localització, han d'adoptar mesures de nivell mitjà a més de la implantació d'un registre d'accessos.

- **Alt:** S'apliquen, juntament amb les de nivell bàsic i mitjà, als fitxers o tractaments que continguin dades relatives a:
 - a) Ideologia, afiliació sindical, religió, creences, origen racial, salut o vida sexual.
 - b) Recollides per a finalitats policials, sense el consentiment de les persones afectades.
 - c) Actes de violència de gènere.

La determinació del nivell de seguretat aplicable dependrà de les dades que es recullin en cada cas. **A títol orientatiu**, alguns dels fitxers més característics dels ens locals podrien tenir assignat el nivell de seguretat següent:

Fitxers	Nivell de seguretat
Padró municipal	Bàsic
Registre municipal d'interessos	Mitjà
Recursos humans	Mitjà
Infraccions administratives	Mitjà
Hisenda Pública	Mitjà
Policial	Alt
Registre entrada i sortida de documents	Alt

◊ **Quin nivell de seguretat requereixen les dades relatives a l'afiliació sindical, quan es recullin exclusivament per fer una transferència de les quotes sindicals al sindicat corresponent?**

Bàsic o mitjà, d'acord amb la resta de dades que contingui el fitxer. D'acord amb l'art. 81.5.a) RLOPD no és exigible aplicar mesures de nivell alt a les dades que, tot i tenir assignat en principi aquest nivell, s'utilitzin amb l'única finalitat de fer una transferència dinerària a les entitats de què els afectats siguin associats o membres.

◊ **Quin nivell de seguretat requereixen les dades relatives a la condició de discapacitat o invalidesa de la persona afectada o al grau de la discapacitat?**

Bàsic o mitjà, d'acord amb la resta de dades que contingui el fitxer, sempre que la dada es tracti per al compliment d'un deure públic. D'acord amb l'art. 81.6) RLOPD, no és exigible aplicar mesures de nivell alt als fitxers o tractaments que continguin dades relatives a la salut, referents exclusivament al grau de discapacitat o la simple declaració de la condició de discapacitat o invalidesa de la persona afectada, amb motiu del compliment de deures públics.

◊ **Com s'apliquen les mesures de seguretat en els fitxers de videovigilància?**

De conformitat amb l'art. 20.2 de la Instrucció 1/2009, els fitxers de videovigilància requereixen, amb caràcter general, el nivell de seguretat bàsic, sens perjudici que en determinats supòsits puguin ser d'aplicació mesures de seguretat de nivell mitjà o alt.

A les imatges, i si escau, la veu, obtingudes o tractades mitjançant sistemes digitals, se'ls ha d'aplicar les mesures de seguretat previstes a la LOPD per als tractaments automatitzats, mentre que a les que no emprin tecnologia digital, o que posteriorment a la captació s'incorporin a suports que no es basin en la tecnologia digital, se'ls ha d'aplicar les mesures de seguretat previstes per als fitxers no automatitzats.

◊ **Amb relació als fitxers de videovigilància, en quins casos s'han de fer còpies de seguretat?**

Si les dades es guarden per un període superior a una setmana, cal fer còpies de seguretat setmanalment, segons disposa l'article 21.4.e) de la Instrucció 1/2009.

Normativa aplicable: art. 9,12 i 20.2.h) LOPD; 54.1.h), 79 i s. 89 i s. 105 i s. RLOPD; 19, 20 i 21 Instrucció 1/2009.

Fitxers i tractaments automatitzats			
Mesures	Nivell bàsic	Nivell mitjà	Nivell alt
Funcions i obligacions del personal	Art. 89	Art. 89	Art. 89
Registre d'incidències	Art. 90	Art. 100	Art. 100
Control d'accés	Art. 91	Art. 99	Art. 99
Gestió de suports i documents	Art. 92	Art. 97	Art. 101
Identificació i autenticació	Art. 93	Art. 98	Art. 98
Còpies de seguretat i recuperació	Art. 94	Art. 94	Art. 102
Responsable de seguretat		Art. 95	Art. 95
Auditoria		Art. 96	Art. 96
Control d'accés físic		Art. 99	Art. 99
Registre d'accessos			Art. 103
Telecomunicacions			Art.104

Normativa aplicable: art. 89 i s. RLOPD.

Fitxers i tractaments no automatitzats			
Mesures	Nivell bàsic	Nivell mitjà	Nivell alt
Criteris d'arxiu	Art. 106	Art. 106	Art. 106
Dispositius d'emmagatzematge	Art. 107	Art. 107	Art. 107
Custòdia dels suports	Art. 108	Art. 108	Art. 108
Responsable de seguretat		Art. 109	Art. 109
Auditoria		Art. 110	Art. 110
Emmagatzematge de la informació			Art. 111
Còpia o reproducció			Art. 112
Accés a la documentació			Art. 113
Trasllat de documentació			Art. 114

Normativa aplicable: art. 106 i s. RLOPD.

■ 4.4.2 Document de seguretat

El responsable del fitxer o tractament ha d'elaborar un **document de seguretat**, que ha de recollir les mesures d'índole tècnica i organitzativa que el responsable del fitxer i/o l'encarregat del tractament, si escau, han d'implementar sobre els fitxers que contenen dades personals.

El document de seguretat s'ha de mantenir **actualitzat** en tot moment i ha de ser objecte de revisió sempre que es produeixin canvis rellevants que puguin repercutir en el compliment de les mesures de seguretat implementades.

El document de seguretat ha de tenir el contingut mínim que detalla l'article 88.3 del RLOPD:

- a) Àmbit d'aplicació del document, amb especificació detallada dels recursos protegits.
- b) Mesures, normes, procediments d'actuació, regles i estàndards encaminats a garantir el nivell de seguretat exigit al RLOPD.
- c) Funcions i obligacions del personal, en relació amb el tractament de les dades de caràcter personal incloses en els fitxers.
- d) Estructura dels fitxers amb dades de caràcter personal i descripció dels sistemes d'informació que els tracten.
- e) Procediment de notificació, gestió i resposta davant les incidències.
- f) Procediments de realització de còpies de seguretat i de recuperació de les dades en els fitxers o tractaments automatitzats.
- g) Mesures que calgui adoptar per al transport de suports i documents, així com per destruir els documents i els suports o, si s'escau, reutilitzar-los.

◇ **Tractant-se d'un fitxer públic, cal tenir en compte també la normativa d'arxius?**

Sí. En el document de seguretat cal indicar el criteri d'arxiu emprat, amb subjecció als criteris continguts en la normativa d'arxius.

Normativa aplicable: art. 88 RLOPD; 22 Instrucció 1/2009.

5 El règim de responsabilitat

L'incompliment de la normativa de protecció de dades pot donar lloc a un seguit de responsabilitats, a les quals el responsable i l'encarregat del tractament han de fer front

Sens perjudici de les responsabilitats que es puguin derivar de la vulneració d'altres drets, com ara el dret a l'honor, a la intimitat i a la pròpia imatge, la vulneració del dret a la protecció de dades genera responsabilitats que es poden exigir mitjançant denúncia davant l'Autoritat Catalana de Protecció de Dades, quan els fets siguin constitutius d'alguna de les infraccions tipificades a la LOPD o mitjançant una reclamació de responsabilitat pels danys i perjudicis soferts.

5.1 Tipus de responsabilitats

Les responsabilitats derivades d'un tractament il·lícit de les dades personals poden ser de diferents tipus:

Responsabilitat patrimonial: Si les persones titulars de les dades personals pateixen algun dany o alguna lesió en els seus drets o interessos, a conseqüència de la vulneració del que disposa la normativa de protecció de dades, tenen dret a ser indemnitzats. La responsabilitat patrimonial per vulneració de la LOPD pot reclamar-se en via administrativa, d'acord amb la legislació reguladora del règim de responsabilitat patrimonial de les administracions públiques, quan el perjudici provingui de fitxers o tractaments de titularitat pública, o bé davant els tribunals ordinaris, en relació amb fitxers o tractaments de titularitat privada.

Responsabilitat penal: El Codi Penal tipifica com a delictes contra la intimitat el descobriment i la revelació de secrets. Es tipifiquen, entre d'altres, l'apoderament, la utilització o la modificació, així com la difusió o cessió, sense consentiment i en perjudici de terceres persones, de dades reservades de caràcter personal o familiar, que es trobin en fitxers o suports informàtics, electrònics o telemàtics, o en arxius o registres, tant públics com privats.

Responsabilitat administrativa: Els responsables dels fitxers i els encarregats del tractament, tant de titularitat pública com privada, estan subjectes al règim sancionador de la LOPD. L'Autoritat Catalana de Protecció de Dades aplica aquest règim sancionador, en relació amb fitxers de titularitat pública i privada, dins el seu àmbit competencial.

◇ Les persones interessades poden reclamar una indemnització pels danys o les lesions sofertes com a conseqüència de l'incompliment de la normativa de protecció de dades?

Sí. Tractant-se d'un fitxer de titularitat pública, poden exercir una acció de reclamació de responsabilitat, d'acord amb la legislació reguladora del règim de responsabilitat patrimonial de les administracions públiques, davant de l'ens local responsable i, si escau, davant de la jurisdicció contenciosa administrativa.

Normativa aplicable: art. 19 LOPD; 139 i s. LRJPAC; 1902 CC; 197 i s. C.P.

5.2 Potestat d'inspecció

En el marc d'un procediment sancionador o abans d'iniciar-lo, l'Autoritat pot inspeccionar, si ho considera necessari, els fitxers i tractaments de dades personals, a fi d'obtenir totes les informacions necessàries per verificar el compliment de la normativa en matèria de protecció de dades. En concret, l'Autoritat pot sol·licitar la presentació o la tramesa de documents i de dades o examinar-los en el lloc on estiguin dipositats. També pot inspeccionar els equips físics i lògics utilitzats, per a la qual cosa pot accedir als locals on estiguin instal·lats.

Els funcionaris que exerceixen la funció inspectora tenen la consideració d'autoritat pública, estan vinculats pel deure de secret en les seves actuacions i han de comptar amb l'auxili, preferent i urgent, de les entitats inspeccionades.

Els fets constatats pels funcionaris de l'Autoritat, i formalitzats en document públic, tenen valor provatori, sens perjudici de les altres proves que puguin aportar les persones interessades.

Normativa aplicable: art. 40 LOPD; art. 5.j) i 19 LACPD.

5.3 Potestat d'immobilització de fitxers

En supòsits d'infracció greu o molt greu, en cas d'utilització o de comunicació il·lícita de dades personals en què s'atempti greument contra els drets fonamentals i les llibertats públiques dels ciutadans o se n'impedeixi l'exercici, l'Autoritat pot exigir als responsables dels fitxers el cessament de la utilització o la comunicació il·lícita de dades personals. Si no s'atén el requeriment, es poden immobilitzar els fitxers per tal de restaurar els drets de les persones afectades. La immobilització resta sense efecte si en el termini de 15 dies no s'acorda la incoació d'un procediment sancionador i no es ratifica la mesura.

Normativa aplicable: art. 49 LOPD; 25 LACPD.

5.4 Infraccions

L'article 44 de la LOPD tipifica les infraccions en què poden incórrer els responsables dels fitxers i els encarregats del tractament, que poden ser **lleus**, **greus** i **molt greus**:

Lleus	Greus	Molt greus
No trametre a l'APDCAT les notificacions previstes a la LOPD o al RLOPD (44.2.a)	Crear fitxers de titularitat pública o iniciar la recollida de dades sense autorització de disposició general publicada al DOGC o BOP corresponent (44.3.a)	Recollir dades de manera enganyosa o fraudulenta (44.4.a)
No sol·licitar la inscripció del fitxer al Registre de Protecció de Dades de Catalunya (44.2.b)	Tractar dades sense tenir el consentiment de la persona afectada, quan sigui necessari segons la LOPD i el RLOPD (44.3.b)	Tractar o cedir les dades especialment protegides dels apartats 2, 3 i 5 de l'article 7 LOPD, excepte en els supòsits que la LOPD ho autoritzi, o violentar la prohibició de l'article 7.4 LOPD (44.4 b)
Incomplir amb el deure d'informació a la persona afectada sobre el tractament de les seves dades personals, quan les dades es recullin de la mateixa persona interessada (44.2.c)	Tractar dades o utilitzar-les posteriorment amb conculcació dels principis i garanties establertes a l'art. 4 LOPD i al RLOPD, excepte que sigui constitutiu d'infracció molt greu (44.3.c)	No cessar en el tractament il·lícit de dades quan hi hagi un requeriment previ del director/a de l'APDCAT (44.4.c)
Transmetre dades a un encarregat del tractament sense complir amb els deures formals de l'art. 12 LOPD (44.2.d)	Vulnerar el deure de guardar secret sobre el tractament de les dades a què es refereix l'art. 10 LOPD (44.3 d)	Transferir dades a països que no proporcionin un nivell de protecció equiparable sense autorització del director/a de l'AEPD, excepte que no sigui necessària segons la LOPD o RLOPD (44.4.d)
	<p>Impedir o obstaculitzar l'exercici dels drets ARCO (44.3 e)</p> <p>Incomplir el deure d'informació a la persona afectada sobre el tractament de les seves dades, quan no s'hagin aconseguit de la mateixa persona interessada (44.3.f)</p> <p>Incomplir la resta de deures de notificació o requeriment de la persona afectada imposats per la LOPD i el RLOPD (44.3.g)</p>	

Lleus	Greus	Molt greus
	Mantenir els fitxers, locals, programes o equips que continguin dades sense les degudes condicions de seguretat que determina el RLOPD (44.3.h)	
	No atendre requeriments o advertències de l'APDCAT o no proporcionar-li tots els documents o informació que sol·liciti (44.3.i)	
	Obstruir l'exercici de la funció inspectora (44.3.j)	
	Comunicar o cedir les dades sense comptar amb legitimitat per a això, d'acord amb la LOPD i el RLOPD, llevat que sigui constitutiva d'infracció molt greu (44.3.k)	

La prescripció:

Les infraccions previstes a la LOPD prescriuen en els terminis següents:

- a) Infraccions **molt greus**: tres anys.
- b) Infraccions **greus**: dos anys.
- c) Infraccions **lleus**: un any.

El termini de prescripció de les infraccions comença a comptar el dia en què s'hagi comès la infracció. S'interromp per la iniciació del procediment sancionador amb coneixement de la persona interessada, i es reprèn si l'expedient està paralitzat durant més de sis mesos per causa no imputable al presumpte infractor.

Normativa aplicable: art. 44, 46 i 47 LOPD.

5.5 Sancions

Pel que fa a les infraccions comeses en relació amb els fitxers de **titularitat privada** o amb informació que hauria d'estar inclosa en fitxers d'aquesta naturalesa, la comissió d'una infracció tipificada a la LOPD comporta, juntament amb el requeriment d'adopció de les mesures correctores escaients, la imposició de la sanció corresponent:

- a) Infraccions **lleus**: multa de 900 a 40.000 €
- b) Infraccions **greus**: multa de 40.001 a 300.000 €
- c) Infraccions **molt greus**: multa de 300.001 a 600.000 €

De forma excepcional, en supòsits en què no hi hagi reincidència i sempre que concorrin determinades circumstàncies, l'Autoritat pot formular una advertència i imposar al responsable l'adopció de determinades mesures correctores, en lloc d'obrir un procediment sancionador.

Pel que fa a les infraccions comeses en relació amb fitxers de **titularitat pública**, no comporten la imposició de cap tipus de sanció. En aquest cas, l'Autoritat dicta una resolució en què declara la infracció i estableix les mesures que cal adoptar perquè cessin o es corregeixin els efectes de la infracció. En aquest cas, l'Autoritat també pot proposar la iniciació d'actuacions disciplinàries, si són procedents.

Les sancions previstes a la LOPD prescriuen en els terminis següents:

- a) Sancions per infraccions **molt greus**: tres anys.
- b) Sancions per infraccions **greus**: dos anys.
- c) Sancions per infraccions **lleus**: un any.

El còmput del termini de prescripció de les sancions comença l'endemà del dia en què adquireix fermesa la resolució per la qual s'imposa la sanció. S'interromp per la iniciació del procediment d'execució amb coneixement de la persona interessada, i es reprèn si el procediment d'execució està paralitzat durant més de sis mesos per una causa no imputable a l'infractor.

Normativa aplicable: art. 37.g), 45-47 LOPD; 5.k), 18, 21-24 LACPD.

5.6 Procediment sancionador

L'Autoritat Catalana de Protecció de Dades, en la tramitació dels procediments sancionadors i també en els procediments de declaració d'infraccions comeses en relació amb fitxers de titularitat pública, ha de seguir el procediment sancionador aplicable als àmbits de competència de la Generalitat.

Actuacions prèvies: Amb caràcter previ a la iniciació del procediment, es poden dur a terme actuacions prèvies per determinar si es donen circumstàncies que la justifiquin.

Si de les actuacions prèvies no se'n deriven fets susceptibles de motivar la imputació de cap infracció, es dicta resolució d'arxiu. Si hi ha indicis susceptibles de motivar la imputació d'una infracció, es dicta acord d'inici del procediment sancionador o de declaració d'infracció.

Iniciació: El procediment sancionador s'inicia d'ofici, per denúncia o com a conseqüència d'informacions conegudes directament per l'Autoritat.

Notificació i publicació de la resolució: en el cas d'infraccions comeses amb relació a fitxers de titularitat pública, la resolució s'ha de notificar a la persona responsable del fitxer o del tractament, a l'encarregat del tractament, si escau, a l'òrgan del qual depenguin i a les persones afectades, si n'hi ha.

En el cas d'infraccions comeses amb relació a fitxers de titularitat privada, es notifica a la persona responsable del fitxer o del tractament, a l'encarregat del tractament, si escau, i a les persones afectades, si n'hi ha.

La persona denunciant té dret a que li comuniquin les actuacions que es deriven de la denúncia, sens perjudici dels drets que pugui tenir com a persona interessada.

Un cop notificada les persones interessades, la resolució sancionadora es comunica al Síndic de Greuges i es fa pública al web de l'Autoritat, prèvia anonimització de les dades de caràcter personal, llevat que no tingui cap interès doctrinal o que, malgrat l'anonimització, sigui aconsellable per causes justificades evitar-ne la publicitat per impedir que determinades persones resultin recognoscibles.

Règim de recursos: les resolucions sancionadores i de declaració d'infracció de l'Autoritat exhaureixen la via administrativa i són susceptibles de recurs de reposició o directament recurs contenciós administratiu.

Normativa aplicable: art. 37.g), 43, 46 i 48 LOPD; 3.c), 5.k), 17, 18, 19, 21 i s. LA-CPD; Decret 278/1993.

6 Els codis tipus

**L'adopció de mesures proactives,
com ara l'aprovació de codis tipus,
facilita el compliment de la normativa
de protecció de dades i millora la
confiança dels ciutadans
en el tractament que tindran les seves
dades per part de les administracions
públiques**

El compliment dels principis, les obligacions i les garanties establertes en matèria de protecció de dades requereix adaptar les previsions establertes de forma general a la normativa, a les característiques i a les necessitats de cada tipus d'entitat. Això es pot fer mitjançant els codis tipus. Aquest mecanisme d'autoregulació, promogut pels mateixos ens locals o per entitats que els agrupin, establirà la forma com es compliran els principis, les obligacions i les garanties establertes a la normativa, com també els compromisos addicionals que es considerin necessaris per a una millor garantia dels drets dels ciutadans.

Els codis tipus són **acords sectorials**, **convenis administratius** o **decisions d'empresa**, mitjançant els quals els responsables dels tractaments poden establir, entre d'altres aspectes, les condicions d'organització, el règim de funcionament, els procediments aplicables, les normes de seguretat, les obligacions de les persones afectades i les garanties per exercir els seus drets en matèria de protecció de dades.

El seu objectiu és **adequar** les previsions establertes tant a la LOPD com al RLOPD, als tractaments que efectuïn les entitats durant l'exercici de la seva activitat, per harmonitzar els tractaments a través de regles, protocols o estàndards, facilitar l'exercici dels drets dels afectats i afavorir el compliment de la normativa.

Tenen caràcter de codis deontològics o de bona pràctica professional i són vinculants per a qui s'hi adhereixi de forma voluntària.

- Els **ens locals** poden adoptar codis tipus, d'acord amb allò establert a les normes que els siguin aplicables.

Han d'incloure **procediments de supervisió**, per tal de garantir el compliment de les obligacions assumides pels adherits, i establir un **règim sancionador** que sigui adequat, eficaç i dissuasori.

Per tal que tinguin la consideració de codis tipus, aquests acords o convenis s'han de **dipositar i inscriure** al Registre de Protecció de Dades de Catalunya.

Un cop inscrits, les entitats estan obligades a:

- Mantenir accessible al públic informació actualitzada sobre les entitats promotores, els adherits, els procediments d'adhesió, el contingut i els procediments de garantia del seu compliment.
- Fer una memòria anual relativa, entre d'altres aspectes, a la difusió del codi, la promoció de la seva adhesió i les actuacions de verificació del seu compliment.
- Avaluar-ne periòdicament l'eficàcia.

Normativa aplicable: art. 32 LOPD; 71 i s. 145 i s. RLOPD; 11.2.b) LACPD.

7 L'Autoritat Catalana de Protecció de Dades

**L' Autoritat Catalana de Protecció
de Dades és l'autoritat de control
competent pel que fa als fitxers i
tractaments de dades de caràcter
personal duts a terme pels ens locals
de Catalunya i els ens que
en depenen**

7.1 Naturalesa i objecte

L'Autoritat Catalana de Protecció de Dades, entitat successora de l'Agència Catalana de Protecció de Dades, és un organisme independent que té per objecte garantir, en l'àmbit de les competències de la Generalitat, els drets a la protecció de dades personals i d'accés a la informació que hi està vinculada.

Es regula per la Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades i el Decret 48/2003, de 20 de febrer, pel qual s'aprova l'Estatut de l'Agència Catalana de Protecció de Dades, vigent en tot allò que no s'oposi a la llei esmentada.

Es configura com una institució de dret públic, amb personalitat jurídica pròpia i plena capacitat d'obrar per al compliment dels seus fins, amb plena autonomia orgànica i funcional, que actua amb objectivitat i plena independència de les administracions públiques en l'exercici de les seves funcions.

Normativa aplicable: art. 1 i 2 LACPD.

7.2 Àmbit d'actuació

L'àmbit d'actuació de l'Autoritat comprèn els fitxers i els tractaments que duen a terme:

- Les institucions públiques de Catalunya.
- L'Administració de la Generalitat.
- Els ens locals.
- Les entitats autònomes, els consorcis i les altres entitats de dret públic vinculades a l'Administració de la Generalitat o als ens locals, o que en depenen.
- Les entitats de dret privat que compleixin, com a mínim, un dels tres requisits següents amb relació a la Generalitat o als ens locals, o que en depenen:
 - Que el seu capital pertanyi majoritàriament als dits ens públics.
 - Que els seus ingressos pressupostaris provenguin majoritàriament dels dits ens públics.
 - Que en els seus òrgans directius els membres designats pels dits ens públics siguin la majoria.
- Les altres entitats de dret privat que presten serveis públics per mitjà de qualsevol forma de gestió directa o indirecta, si es tracta de fitxers i tractaments vinculats a la prestació d'aquests serveis.
- Les universitats públiques i privades que integren el sistema universitari català, i els ens que en depenen.
- Les persones físiques o jurídiques que compleixen funcions públiques amb relació a matèries que són competència de la Generalitat o dels ens locals, si

es tracta de fitxers o tractaments destinats a l'exercici d'aquestes funcions i el tractament es duu a terme a Catalunya.

- Les corporacions de dret públic que compleixen les seves funcions exclusivament en l'àmbit territorial de Catalunya als efectes del que estableix la LA-CPD.

Normativa aplicable: art. 156 EAC; 3 LACPD.

7.3 Organització

L'Autoritat disposa de dos òrgans:

- El/la **director/a**, que dirigeix la institució i n'exerceix la representació.
- El **Consell Assessor de Protecció de Dades**, òrgan d'assessorament i participació de l'Autoritat, constituït per representants de les diferents institucions incloses dins el seu àmbit d'actuació, entre els quals hi ha dos representants dels ens locals de Catalunya, designats pel Consell de Governos Locals.

Normativa aplicable: art. 6 i s. LACPD; 13 i s. Decret 48/2003.

7.4 Funcions

L'Autoritat duu a terme, entre d'altres, les funcions següents:

- **Atenció al públic i consultoria** en relació amb les sol·licituds d'informació, queixes o consultes sobre els serveis de l'Autoritat i sobre l'aplicació de la legislació de protecció de dades de caràcter personal, que pugui formular qual-sevol ciutadà o el personal de les entitats sotmeses a l'àmbit d'actuació de l'Autoritat.

Es pot contactar amb aquest servei a través de:

- Telèfon: 902 011 710 (de 9 a 14 h, de dilluns a divendres laborables).
- Per correu electrònic: consultes.apdcat@gencat.cat.
- Per correu postal: carrer de la Llacuna, 166, 7a planta, 08018 Barcelona.
- Per fax: 93 552 78 30.
- Presencialment: de 9 a 14 h, de dilluns a divendres laborables.
- **Difusió** del dret a la protecció de dades de caràcter personal a través de publicacions, conferències, cursos, seminaris i altres iniciatives. A aquests efectes, l'Autoritat disposa d'una llista de distribució sobre les seves iniciatives, la inscripció a la qual es pot sol·licitar enviant un correu electrònic adreçat a consultes.apdcat@gencat.cat.

- **Registre:** a través del Registre de Protecció de Dades de Catalunya, en el qual són objecte d'inscripció:
 - a) Els fitxers de dades personals, de titularitat pública o privada, inclosos dins l'àmbit d'actuació de l'Autoritat.
 - b) Els codis tipus formulats per les entitats incloses dins l'àmbit d'actuació de l'Autoritat.
- **Elaboració d'informes,** sobre els projectes de disposicions de caràcter general de creació, modificació o supressió de fitxers i sobre disposicions que tinguin impacte en matèria de protecció de dades de caràcter personal. En el cas dels ens locals aquests informes són potestatus.
- **Elaboració de dictàmens** en relació amb les consultes que formulin els representants de les entitats del seu àmbit d'actuació.
- **Elaboració de recomanacions i instruccions,** per tal d'adequar els fitxers i els tractaments de dades als principis i a les garanties que estableix la legislació vigent de protecció de dades.
- **Tutela** dels drets ARCO, mitjançant un procediment de reclamació adreçat a fer efectius i restablir de forma immediata aquests drets dels ciutadans.
- **Funcions de control,** integrades per:
 - a) Els plans d'auditoria, com a sistema de control preventiu per verificar el compliment de la normativa i recomanar o requerir els responsables dels fitxers i tractaments que adoptin les mesures correctores adequades.
 - b) La potestat d'inspecció, per la qual l'Autoritat pot inspeccionar els fitxers i els tractaments de dades personals, per tal d'obtenir les informacions necessàries per a desenvolupar la seva activitat.
 - c) L'aplicació del règim sancionador previst a la LOPD respecte dels responsables dels fitxers i dels tractaments inclosos dins l'àmbit d'actuació de l'Autoritat, i dels encarregats dels tractaments corresponents.
 - d) Els requeriments d'adequació a la legalitat, en cas d'infraccions greus o molt greus, per exigir el cessament de la utilització o la comunicació il·lícita de dades personals i, si escau, la potestat d'immobilització de fitxers, en cas d'incompliment dels requeriments d'adequació.
- **Atorgar autoritzacions,** per a l'exempció del deure d'informació en la recollida de les dades o per al manteniment íntegre de determinades dades, i altres que estableixi la normativa, excepte les relatives a transferències internacionals de dades, competència del director de l'Agència Espanyola de Protecció de Dades.

Normativa aplicable: art. 5 i 15 i s. LACPD.

Abreviatures

EAC: Estatut d'Autonomia de Catalunya.

CC: Codi Civil

CP: Codi Penal, aprovat per la Llei orgànica 10/1995, de 23 de novembre.

LOPD: Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.

LOVFC: Llei orgànica 4/1997, de 4 d'agost, per la qual es regula la utilització de videocàmeres per les forces i cossos de seguretat en llocs públics.

LRBRL: Llei 7/1985, de 2 d'abril, reguladora de les bases del règim local.

LRJPAC: Llei 30/1992, de 26 de novembre, de règim jurídic de les administracions públiques i del procediment administratiu comú.

Llei 22/1998: Llei 22/1998, de 30 de desembre, de la Carta municipal de Barcelona.

Llei 21/2000: Llei 21/2000, de 29 de desembre, sobre els drets d'informació concernent la salut i l'autonomia del pacient, i la documentació clínica.

LA: Llei 10/2001, de 13 de juliol, d'arxius i documents.

TRLCSP: Text refós de la Llei de contractes del sector públic, aprovat pel Reial decret legislatiu 3/2011, de 14 de novembre.

Llei 13/2008: Llei 13/2008, de 5 de novembre, de la presidència de la Generalitat i del Govern.

Llei 26/2010: Llei 26/2010, del 3 d'agost, de règim jurídic i de procediment de les administracions públiques de Catalunya.

LUMESPC: Llei 29/2010, del 3 d'agost, de l'ús dels mitjans electrònics al sector públic de Catalunya.

LACPD: Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades.

TRLMRLC: Decret legislatiu 2/2003, de 28 d'abril, pel qual s'aprova el Text refós de la Llei municipal i de règim local de Catalunya.

RLOPD: Reglament de desplegament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, aprovat pel Reial decret 1720/2007, de 21 de desembre.

ROAS: Reglament d'obres, activitats i serveis dels ens locals, aprovat pel Decret 179/1995, de 13 de juny.

Decret 278/1993: Decret 278/1993, de 9 de novembre, sobre el procediment sancionador d'aplicació als àmbits de competència de la Generalitat.

Decret 134/1999: Decret 134/1999, de 18 de maig, de regulació de la videovigilància per part de la policia de la Generalitat i de les policies locals de Catalunya.

Decret 48/2003: Decret 48/2003, de 20 de febrer, pel qual s'aprova l'estatut de l'Agència Catalana de Protecció de Dades.

Decret 78/2010: Decret 78/2010, de 22 de juny, sobre la instal·lació de dispositius de videovigilància a les dependències policials de la Generalitat.

Ordre de 29 de juny de 2001: Ordre de 29 de juny de 2001, de regulació dels mitjans pels quals s'informa de l'existència de videocàmeres fixes instal·lades per la policia de la Generalitat i les policies locals de Catalunya en llocs públics.

Instrucció 1/2009: Instrucció 1/2009, de 10 de febrer, de l'Agència Catalana de Protecció de Dades, sobre el tractament de dades de caràcter personal mitjançant càmeres amb fins de videovigilància.

Recomanació 1/2008: Recomanació 1/2008 de l'Agència Catalana de Protecció de Dades sobre la difusió d'informació que contingui dades de caràcter personal a través d'Internet.

Recomanació 1/2010: Recomanació 1/2010 de l'Agència Catalana de Protecció de Dades sobre l'encarregat del tractament en la prestació de serveis per compte d'entitats del sector públic de Catalunya.

Recomanació 1/2011: Recomanació 1/2011 de l'Autoritat Catalana de Protecció de Dades sobre la creació, modificació i supressió de fitxers de dades de caràcter personal de titularitat pública.

Res. 04.04.2011 APDCAT: Resolució de 4 d'abril de 2011, per la qual s'aprova la modificació dels suports normalitzats per formalitzar les inscripcions dels fitxers al Registre de Protecció de Dades de Catalunya (DOGC núm. 5859, de 14.04.2011).

