

# Universitat de Barcelona: Taller de protecció de dades a l'àmbit de la Gestió Acadèmica



**Àlvar Sánchez**

**Curs de formació PAS (6 hores)**

**21 i 23 de novembre de 2012**

# Formació en protecció de dades a la UB

**Normativa General:** (4 hores) visió teòrica del dret a la protecció de dades amb les principals regulacions sobre protecció de dades. Marc jurídic comunitari, estatal i autonòmic.

**Mòdul 1:** (4 hores) primer contacte amb la pràctica del dret a la protecció de dades: dada de caràcter personal, consentiment, fitxer, tractament, etc. Procés de creació i inscripció dels fitxers de la UB. El Document de seguretat de nivell bàsic.

**Mòdul 2:** (4 hores) reforçar la visió pràctica del dret fonamental de protecció de dades a l'activitat universitària amb la resolució de casos pràctics. Propostes de clàusules en formularis, contractes, etc. Les activitats de publicitat i prospecció comercial. Els Documents de seguretat de nivell mitjà i alt.

**Mòdul 3:** (3 hores) establir els criteris tècnics de seguretat específics per a l'adequada utilització dels sistemes d'informació de la Universitat de Barcelona, fent èmfasi en la protecció de dades.

**Protecció de dades en àmbits específics:** (Octubre de 2011: 6 hores) aplicació de la normativa de PD a àmbits i/o sectors de la UB. De forma experimental s'ha començat amb el de Recursos Humans. Aquesta iniciativa ha tingut la seva continuïtat amb aquest taller sobre l'àmbit de la gestió acadèmica (novembre 2012).

# Agenda dels dos dies

1. El dret fonamental a la protecció de les dades de caràcter personal.
  - a) Significat d'aquest dret.
  - b) Repàs dels conceptes fonamentals: dada caràcter personal, fitxer, tractament de dades, recollida de dades, consentiment, cessió de dades, etc.,
  - c) Deure de secret
  - d) Drets dels afectats
  - e) Règim sancionador
  - f) Repartiment de competències entre les diferents autoritats de protecció de dades.
  - g) L'assignació de competències en la UB: el responsable del fitxer i el responsable de seguretat.
  
2. La gestió acadèmica i el dret fonamental a la protecció de les dades de caràcter personal.
  - a) Fitxers de la UB relacionats amb la gestió acadèmica.
  - b) La preinscripció universitària.
  - c) La matrícula universitària.
  - d) Transmissió intraadministrativa de dades.
  - e) Qualificacions acadèmiques.
  - f) Cessió de dades: a entitats del Grup UB, a les forces i cossos de seguretat, etc.
  - g) Transferències internacionals
  - h) Difusió de dades en Internet
  - i) Cancel·lació de dades.
  
3. Mesures de seguretat més significatives a l'àmbit dels fitxers de la gestió acadèmica
  - a) La seguretat i les mesures de seguretat.
  - b) Aplicació de les mesures de seguretat.

# **1. El dret fonamental a la protecció de les dades de caràcter personal**

# Significat del dret fonamental a la protecció de dades a l'ordenament jurídic espanyol

No existeix en la Constitució referència expressa a la protecció de dades. Ha estat el Tribunal Constitucional, en la sentència 292/2000, de 30 de novembre, fonament de dret 7, qui ha assenyalat que de l'article 18.4 de la CE (*"La llei limitarà l'ús de la informàtica per tal de garantir l'honor i la intimitat personal i familiar dels ciutadans i el ple exercici dels seus drets"*) es deriva un **dret fonamental a la protecció de dades de caràcter personal**, el contingut del qual consisteix en un **poder de disposició i de control** sobre les pròpies dades personals.

De **disposició** -tot i que amb les limitacions imposades per les lleis- per què les dades són titularitat de cada persona, que decideix que fa amb elles. De **control**, per què l'interessat té la facultat de saber a qui es faciliten, qui les utilitza i per a quines finalitats: **Informació i consentiment**.

La LORTAD de 1992 va ser la primera llei limitadora de l'ús de la informàtica. Es va fer a corre-cuita, degut a la incorporació de l'estat espanyol a l'espai Shengen (1991) que requeria disposar d'una llei de protecció de dades per a poder consultar el fitxer de cooperació policial del Sistema d'Informació de Shengen per tal de prevenir la criminalitat. Va estar vigent fins el 14 de gener de 2000.

La [Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal](#), és la disposició legislativa vigent, juntament amb el [RD 1720/2007, de 21 de desembre, pel qual s'aprova el reglament de desenvolupament de la LOPD](#). Aquesta llei obeeix també al mandat contingut a la Directiva 95/46/CE.

# Les dades de caràcter personal

**Dades personals ≠ dades de caràcter personal.** No obstant, en la pràctica, s'utilitzen indistintament.

**Definició:** Qualsevol informació referent a persones físiques identificades o identificables (art. 3 LOPD). És a dir, la informació pot permetre identificar directament una persona (quan disposem del nom i cognoms, de la seva fotografia, del DNI), o bé pot identificar-la indirectament mitjançant un número de telèfon, una matrícula d'un cotxe, una combinació de criteris significatius (edat, sexe, domicili, ocupació...) que faci possible la seva identificació. Així, un número de telèfon per si mateix no identifica a una persona però si truquem a aquest número podem saber a qui pertany, o també, mirant les pàgines blanques. El mateix succeeix amb una matrícula del cotxe ja que aquesta dada no mostra directament qui és el seu titular, però si es consulta al registre de vehicles podem saber-ho.

Les autoritats de protecció de dades han resolt en sentit positiu alguns dubtes sobre el caràcter de dada personal del [DNI o NIE](#), [adreça electrònica](#), [núm. telèfon mòbil](#), [matrícula de vehicles](#) o [l'adreça IP](#).

El RD 1720/2007, de 21 desembre RLOPD ha concretat aquesta informació en el sentit de que pot ser numèrica, alfabètica, gràfica, fotogràfica, acústica o de qualsevol altre tipus. A la vista d'aquesta definició, poden ser dades personals la veu, la imatge, l'empremta digital, el grup sanguini, l'iris, les dades biomètriques, les dades genètiques, etc.

# Tipus de dades de caràcter personal

Font: Formulari per a la notificació de fitxers de l'Autoritat Catalana de Protecció de Dades

- a) **Dades de caràcter identificatiu:** nom i cognoms, adreça postal i/o electrònica, número de telèfon, signatura o empremtes, imatge, veu, DNI, NIF o NIE, número SS o Mutualitat, número de registre personal, marques físiques, signatura electrònica.
- b) **Dades de característiques personals:** estat civil, dades familiars, data de naixement, lloc de naixement, edat, sexe, nacionalitat, característiques físiques, llengua.
- c) **Dades de circumstàncies socials:** allotjament o habitatge, propietats o possessions, aficions i estils de vida, clubs i associacions, llicències, permisos...
- d) **Dades acadèmiques i professionals:** formació i titulacions, historial acadèmic, experiència professional, col·legis o associacions professionals.
- e) **Dades d'ocupació laboral:** cos, escala, categoria, grau, llocs de treball, dades no econòmiques de nòmina, historial laboral.
- f) **Dades d'informació comercial:** activitats i negocis, llicències comercials, subscripcions a publicacions, creacions artístiques, científiques...
- g) **Dades econòmicofinanceres i d'assegurances:** ingressos, rendes, inversions, patrimoni, crèdits, préstecs, avals, dades bancàries, assegurances, dades de nòmina, impostos, deduccions, plans de pensió, jubilació, hipoteques, subsidis, beneficis, historial, crèdits, targetes de crèdit.
- h) **Dades de transaccions:** béns subministrats, béns rebuts, transaccions financeres, compensacions, indemnitzacions.

Però no totes les dades són iguals. Algunes són particularment delicades en pertànyer a l'esfera més íntima de la persona. Són dades especialment protegides: ideologia, afiliació sindical, religió, creences, origen racial, salut (informació genètica), vida sexual i infraccions penals o administratives.

# Què és un fitxer?

Els llistats amb dades de caràcter personal han existit des de sempre, encara que en format paper (per ex. cens de matriculats en una universitat medieval). El canvi que s'ha produït amb la informàtica és que s'ha multiplicat la possibilitat de realitzar tractaments automatitzats d'aquestes dades i que els arxius informàtics s'anomenen "bases de dades", que complementen els antics fitxers de paper. Tant per a la Directiva europea com per a la LOPD ambdós tipus de suport són fitxers: paper i informàtic.

**Definició LOPD:** Qualsevol conjunt organitzat de dades de caràcter personal que permeti l'accés a les dades d'acord amb uns criteris determinats, sigui quina sigui la forma o modalitat de la seva creació, emmagatzematge, organització i accés (art. 5 RLOPD).

Certament, un conjunt de dades organitzades constitueix un **únic fitxer** de protecció de dades, encara que físicament es trobin emmagatzemades en diferents tipus de suports o en diferents ubicacions geogràfiques. Així, a la nostra UB, per exemple, les dades personals dels estudiants es troben emmagatzemades en un fitxer gestionat amb un software denominat GIGA. També hi ha dades personals d'estudiants en diversos arxius i carpetes informàtiques i també en diverses carpetes i arxivadors que contenen documentació en format paper. Doncs bé, encara que físicament existeixi un fitxer automatitzat (arxius i aplicacions informàtiques) i un fitxer no automatitzat (carpetes i arxivadors, etc.), jurídicament es tracta d'un únic fitxer de caràcter mixt (parcialment automatitzat), que l'hem denominat Fitxer de Gestió Acadèmica. No s'ha de declarar dues vegades un fitxer pel simple fet d'estar en suport paper i en suport automatitzat, sinó que es tracta d'un fitxer parcialment automatitzat.

**Activitats personals i domèstiques:** La LOPD no és aplicable als fitxers ni als tractaments realitzats o mantinguts per persones físiques en l'exercici d'activitats exclusivament personals o domèstiques, sempre que la finalitat es limiti a aquests àmbits. Per exemple, no es podria fer, en superar l'àmbit personal o domèstic, la publicació d'una foto d'aquestes en Internet (art. 4.a) RLOPD).

**Director:** No cal crear un fitxer quan es limita a incorporar les dades de les persones físiques que presten serveis en empreses i administracions públiques consistents únicament en el nom i cognoms, les funcions o llocs exercits, així com l'adreça postal o electrònica, telèfon i número de fax professionals (art. 2.2 LOPD).



# Creació i notificació d'un fitxer

L'article 20 LOPD obliga a les AAPP a crear i publicar els fitxers al Registre de Protecció de Dades corresponent. Per a la creació, cal una Resolució del Rector/Acord del Consell de Govern, segons s'indiqui als Estatuts, i després la seva publicació al DOGC. L'Estatut de la UB atribueix aquesta funció al rector (art. 73 de l'Estatut de la UB).

Una vegada creat el fitxer i publicat al DOGC, tenim 30 dies per tal de fer la notificació al Registre de PD de Catalunya (Hi ha una aplicació informàtica per tal de fer-ho *on line*).

**NO ES PODEN RECOLLIR DADES SENSE TENIR EL FITXER CREAT I NOTIFICAT.** Art. 44.3a) LOPD. És infracció greu *“Crear fitxers de titularitat pública o iniciar la recollida de dades de caràcter personal per a aquests, sense autorització de disposició general, publicada en el “Butlletí Oficial de l'Estat” o diari oficial corresponent”*: ([PS 35/2012](#))

Durant el procés de creació del fitxer s'ha de comprovar que estigui elaborat el corresponent **Document de Seguretat**, amb les mesures de seguretat tècniques i organitzatives per tal de garantir la seguretat de les dades. L'ha de redactar (o encarregar) el responsable del fitxer.

# 36 Fitxers creats per la UB

## Resolució del rector de 17 de novembre de 2008 (DOGC de 24.12.2008)

- Personal
- Espai personal
- Gestió acadèmica
- Beques
- Mobilitat dels estudiants
- Bústia de consultes sobre activitats acadèmiques i formatives
- Feina UB
- Esports UB
- Activitats infantils i juvenils
- Gestió de la recerca
- Registre de becaris de recerca
- Centre de recursos per a l'aprenentatge i la investigació
- Serveis jurídics
- Gestió econòmica
- Antics UB
- Síndic de greuges
- Registre general

## Resolució del rector de 18 de maig de 2009 (DOGC de 15.06.2009)

- Projectes de recerca, desenvolupament i innovació amb dades personals de nivell bàsic
- Projectes de recerca, desenvolupament i innovació amb dades personals de nivell mitjà
- Projectes de recerca, desenvolupament i innovació, amb dades personals de **nivell alt**
- Seminaris, Jornades i Congressos
- Projectes institucionals
- Gestió de correccions i traduccions
- Activitats i cursos de l'ICE
- Formadors de l'ICE
- Col·legis Majors
- Prevenció de riscos laborals, vigilància de salut i prestació sanitària-assistencial (**nivell alt**)

## Resolució del rector de 28 de maig de 2010 (DOGC de 26.07.2010)

- Videovigilància de la UB
- Difusió d'oferta formativa
- Concursos, premis i altres activitats de foment

## Resolució del rector de 22 de març de 2011 (DOGC de 06.04.2011)

- Fons documental
- Fons d'acció social (**nivell alt**)
- Integració dels estudiants amb necessitats especial (**nivell alt**)
- Col·laboradors de programes d'integració

## Resolució del rector de 12 d'abril de 2012 (DOGC de 08.05.2012)

- Formadors
- Protecció radiològica (**nivell alt**)

# Dret d'informació en la recollida de dades

**Els interessats, als que es sol·licitin dades personals, han de ser informats de manera expressa, precisa i inequívoca de:** (art 5.1 LOPD)

- a) L'existència d'un fitxer, la finalitat de la recollida de les dades i els destinataris de la informació.
- b) Del caràcter obligatori o facultatiu de la resposta a les preguntes que els siguin plantejades.
- c) De les conseqüències de l'obtenció de les dades o de la negativa a subministrar-les.
- d) De la possibilitat d'exercir els drets ARCO.
- e) De la identitat i adreça del responsable.

Els apartats b) c) no caldran si del contingut de la informació ja es dedueix. Forma de recollir les dades: formularis, web, telèfon, entrevista, etc. Sempre s'ha de **guardar l'acreditació** de que s'ha informat a l'interessat.

Les dades de caràcter personal facilitades seran incorporades al fitxer **XXXX**\_titularitat de la Universitat de Barcelona, les finalitats principals del qual són: **YYYY**. L'òrgan responsable del fitxer és la Secretaria General. En qualsevol cas, podeu exercir els drets d'accés, rectificació, cancel·lació i oposició mitjançant una comunicació escrita, adjuntant fotocòpia del DNI o altre document identificatiu, dirigida a la Secretaria General de la Universitat de Barcelona, Gran Via de les Corts Catalanes 585, 08007 Barcelona, o mitjançant correu electrònic a la següent adreça: [secretaria.general@ub.edu](mailto:secretaria.general@ub.edu).

# El consentiment per a la recollida de les dades. Regla general i excepcions

El principi general és la necessitat de comptar amb el consentiment per a poder tractar dades de caràcter personal o una llei que l'habiliti. No obstant, en el nostre àmbit la LOPD excepciona aquest requisit quan:

- a) Les dades de caràcter personal es recullen per a l'exercici de les **funcions pròpies** de les administracions públiques en **l'àmbit de les seves competències**, *“que els atribueixi una norma amb rang de llei o una norma de dret comunitari”* ha afegit el reglament (art. 10.3.a).
- b) Les sol·liciti el responsable del tractament en ocasió de la subscripció d'un contracte o precontracte o de l'existència d'una relació comercial, laboral o administrativa de la qual sigui part l'afectat i siguin necessaris per al seu manteniment o compliment (doncs, si ja es va donar el consentiment per a la formalització del contracte laboral o de la relació administrativa, és raonable que no es torni a exigir aquest consentiment per a tractar les dades pel manteniment o compliment d'aquesta relació). Les dades que facin referència a l'origen racial, la **salut** i a la vida sexual només poden ser recollides quan així ho disposi una llei o l'afectat consenti **expressament**. Per a les dades que revelin la ideologia, la religió, les creences o **l'afiliació sindical**, cal el consentiment **explícit i per escrit** dels afectats. A més, en aquest darrer cas, quan es recullen aquestes dades cal advertir a la persona interessada que no té l'obligació de facilitar-les.
- c) Les dades figurin en fonts accessibles al públic. **Només** tenen el caràcter de fonts accessibles al públic:
  - El cens promocional, regulat conforme al que disposa la Llei orgànica 15/1999, de 13 de desembre
  - Les guies de serveis de comunicacions electròniques, en els termes que preveu la seva normativa específica.
  - Les llistes de persones pertanyents a grups de professionals que continguin únicament les dades del nom, títol, professió, activitat, grau acadèmic, adreça professional i indicació de la seva pertinença al grup. L'adreça professional pot incloure les dades del domicili postal complet, número telefònic, número de fax i adreça electrònica. En el cas dels col·legis professionals, es poden indicar com a dades de pertinença al grup les de número de col·legiat, data d'incorporació i situació d'exercici professional.
  - Els diaris i butlletins oficials.
  - Els mitjans de comunicació social.

El consentiment s'entén donat quan voluntàriament l'afectat omple un formulari o imprès.

# Aplicació del principi de qualitat de les dades en la recollida de les dades

Les dades que es recullin han de ser:

- a) **adequades, pertinents i no excessives** en relació amb les finalitats a obtenir,
- b) no recollides per mitjans fraudulents, deslleials o il·lícits.
- c) exactes i **posades al dia** per tal de reflectir la situació real,
- d) tractades de manera **lleial i lícita** respecte l'interessat,
- e) recollides per a **finalitats determinades, explícites i legítimes** i no tractades posteriorment de manera incompatible amb aquestes finalitats,
- f) **cancel·lades** quan hagin deixat de ser necessàries per a la finalitat per a la qual es van recollir (tret que hi hagi una previsió legal que exigeixi conservar-les). A la universitat, difícilment es pot dur a terme, per la legislació de patrimoni històric.

# Cessió o comunicació de dades. Necessitat de consentiment

La cessió és el tractament de dades que suposa la seva revelació a una persona diferent de l'interessat o afectat. La revelació es refereix tant el lliurament, comunicació, consulta, interconnexió, transferència, difusió o qualsevol altra forma que faciliti l'accés a les dades d'un fitxer a un tercer, diferent del titular del fitxer.

La cessió implica una important pèrdua de control sobre les dades personals, atès que aquestes passen a entitats o persones diferents d'aquelles a qui, en un principi, s'han facilitat les dades. Per això, l'art. 11 LOPD requereix, com a principi general, el consentiment previ de l'interessat, encara que hi ha excepcions.

De tots els tractaments, la cessió requereix unes condicions específiques para poder atorgar el consentiment. D'acord amb l'article 11.1 LOPD, cal:

- a) conèixer la finalitat concreta a que es destinaran les dades (art. 11.3),
- b) saber el tipus d'activitat del receptor de les dades o el sector al que pertany (art. 11.3),
- c) determinar, de les dades que conté el fitxer, quines es pretenen cedir,
- d) que la cessió tingui per objecte el compliment de finalitats directament relacionades amb les funcions legítimes del cedent i del cessionari (art. 11.1)

# La difusió (cessió) de dades en Internet

La difusió de dades, en un mitjà com Internet, està considerada com una cessió de dades de caràcter personal on una pluralitat indeterminada de persones pot accedir a les mateixes.

Internet no és una Font accessible al públic. En conseqüència, no es poden recollir, per exemple, adreces electròniques, encara que estiguin en Internet: directoris, pàgines web, fòrums, etc. i elaborar una base de dades.

Hi ha una recomanació de l'APDCAT sobre *“la difusió de d'informació que contingui dades de caràcter personal a través d'Internet”*

- a) Compte amb el que es penja en Internet!
- b) Limitació temporal: la difusió de les dades de caràcter personal s'ha de limitar temporalment al període necessari per assolir la finalitat que justifiqui la seva publicació.
- c) Informació actualitzada: s'ha de mantenir al dia la informació que tenim penjada a la xarxa. És important evitar la difusió de dades de caràcter personal desactualitzades.

L'aplicació de tot l'anterior ha de comportar una **revisió periòdica** dels continguts de les seues electròniques i les pàgines web, per tal de cessar la difusió en el cas que ja hagi esdevingut innecessària. Exemple: [relació de persones que van complir 25 anys a la UB l'any 2008](#).

# Excepcions del consentiment per a la cessió

- a) Quan la cessió està autoritzada per una llei.
- b) Quan la cessió respongui a la lliure i legítima acceptació d'una **relació jurídica el desenvolupament, el compliment i el control de la qual** que impliqui la cessió. Ex. un conveni de pràctiques (relació jurídica: Universitat i estudiant, mentre que la cessió de dades es fa a l'empresa o institució). Curs de formació a impartir per l'Escola d'Administració Pública però que es gestiona des de la universitat (relació jurídica: empleat públic i universitat, mentre que la cessió es a fa a l'Escola d'A. P. Altres exemples: cessió a entitats bancàries per a la facturació dels productes o serveis que hem contractat amb un tercer, empreses de missatgeria per a l'enviament contractat. Exemple: [“Exigimos un referéndum”](#)
- c) Quan tingui com a destinatari el Defensor del Poble o figures similars autonòmiques, el Ministeri Fiscal, jutges o tribunals. Tribunal de Comptes o figures similars autonòmiques.
- d) Entre les Administracions públiques
  - Quan la comunicació es porti a terme per a l'exercici de competències idèntiques (ex. cessió de dades entre universitats per al trasllat d'un expedient) o de competències diferents que versin sobre la mateixa matèria (ex, dades cedides periòdicament per una universitat pública a la conselleria d'educació corresponent).
  - Quan les dades personals hagin estat recollides o elaborades per una administració pública amb destinació a una altra administració pública. (Així, Dades dels alumnes preinscrits, registre d'entrada d'un document en una AAPP diferent, etc.).
  - Quan l'objecte de la cessió sigui el tractament de les dades amb finalitats històriques, estadístiques o **científiques**. (Llei 16/1985, del patrimoni històric espanyol i llei 9/1993, del patrimoni cultural català, Llei 12/1989, de 9 de maig, reguladora de la funció estadística pública i llei 23/1998, d'estadística de Catalunya, Llei 14/2011, d'1 de juny, de la Ciència, la Tecnologia i la Innovació).



# Contracte d'encarregat del tractament

La UB encarrega una prestació de serveis a un tercer, però per dur-la a terme cal facilitar-li determinades dades de caràcter personal d'alguns dels seus fitxers. Ex. carnet Som UB, contracte amb empresa per a la destrucció de documents, contractes de prestació de serveis en *cloud computing*, etc.

Regulació: **art. 12 LOPD** i arts. 20 a 22 del RD 1720/2007, de 21 de desembre.

La realització de tractaments per compte de tercers ha d'estar regulada en un [contracte](#) diferent al contracte principal, que ha de constar per escrit, i s'ha d'establir de manera expressa que l'encarregat del tractament només ha de tractar les dades d'acord amb les instruccions del responsable del tractament, que no les pot aplicar ni utilitzar amb una finalitat diferent de la que figuri en el contracte esmentat, ni comunicar-les a altres persones, ni tan sols per conservar-les. El contracte també ha d'estipular les mesures de seguretat a què es refereix l'article 9 LOPD que l'encarregat del tractament està obligat a implementar. L'Autoritat de PD també accepta una clàusula específica dins del contracte principal adjudicat, o en el plec de clàusules administratives particulars, o bé al plec de prescripcions tècniques.

Una vegada complerta la prestació contractual, les dades de caràcter personal han de ser destruïdes o tornades al responsable del tractament, i també qualsevol suport o document en què consti alguna dada de caràcter personal objecte del tractament.

En cas que l'encarregat del tractament destini les dades a una altra finalitat, les comuniqui o les utilitzi incomplint les estipulacions del contracte, també ha de ser considerat responsable del tractament, i ha de respondre de les infraccions en què hagi incorregut.

# El deure de secret

L'article 10 LOPD estableix que *“El responsable del fitxer i els qui intervinguin en qualsevol fase del tractament de les dades de caràcter personal estan obligats al secret professional respecte dels mateixos i al deure de guardar-los, obligacions que subsistiran fins i tot després de finalitzar les seves respectives relacions amb el titular del fitxer o, si escau, amb el responsable del mateix”*. La vulneració del deure de guardar secret sobre les dades de caràcter personal especialment protegides pot ser constitutiu de una sanció molt greu en els termes de l'article 44.4.g) de la LOPD.

Es recomana la inclusió de clàusules específiques en aquesta matèria en els **contractes laborals** que subscriuguin les administracions públiques en el seu àmbit d'actuació amb empleats públics.

També es pot incloure en el **Manual d'acollida**.

# Dret d'accés

El Dret d'accés és el dret de tota persona a obtenir gratuïtament informació sobre les seves dades que són objecte de tractament, les finalitats del tractament que s'estigui realitzant, així com la informació sobre l'origen de les dades i les cessions o comunicacions realitzades o previstes.

Per raons de complexitat especial, es pot sol·licitar de l'afectat que especifiqui els fitxers respecte dels quals vulgui exercir el dret, si bé se li ha de facilitar la relació de tots els fitxers.

La sol·licitud es presenta davant el responsable del fitxer i s'ha d'adjuntar fotocòpia del DNI o del passaport. Termini per a resoldre: un mes des de la sol·licitud.

L'afectat pot optar per rebre la informació a través dels següents sistemes de consulta: visualització en pantalla, la indicació de les dades que són objecte del tractament mitjançant escrit, còpia o fotocòpia remesa per correu, telecòpia, correu electrònic o altres sistemes de comunicació electrònica, qualsevol altre que sigui adequat.

No es pot exercir una altra vegada quan el dret ja s'ha exercit en els dotze mesos anteriors a la sol·licitud, llevat que s'acrediti un interès legítim.

# Dret de rectificació i cancel·lació

El **dret de rectificació** és el dret de l'afectat per a que es modifiquin les dades que siguin inexactes o incompletes. S'han d'especificar les dades que es pretén rectificar i corregir.

Les dades seran **cancel·lades** quan hagin deixat de ser necessàries o pertinents per a la finalitat per a la qual van ser recavades. No es poden cancel·lar les dades mentre són necessàries per a l'activitat universitària o hagin de ser conservades per motius legals (recursos judicials, valor històric, científic, etc). S'han de conservar les dades durant els terminis previstos en les legislacions aplicables o, en el seu cas, en les relacions contractuals entre el responsable del tractament i l'interessat. Cancel·lació de dades a la guia telefònica, fotografia quan ja no és membre de la plantilla, etc. El **dret de cancel·lació** dóna lloc a que se suprimeixin les dades que siguin inadequades o excessives. La cancel·lació donarà lloc al **bloqueig** de les dades, conservant-se únicament a la disposició de les Administracions Públiques, Jutges i Tribunals, per a l'atenció de les possibles responsabilitats nascudes del tractament, durant el termini de prescripció d'aquestes. Complert el citat termini s'haurà de procedir a la supressió (art. 16.3 LOPD).

Si les dades rectificades o cancel·lades haguessin estat comunicades prèviament, el responsable del tractament haurà de notificar la rectificació o cancel·lació efectuada a qui s'hagin comunicat, en el cas que es mantingui el tractament per aquest últim, que haurà de procedir també a la cancel·lació (art. 16.4).

La resolució s'ha de fer en 10 dies des de la recepció de la sol·licitud.

# Dret d'oposició

Quan hem donat el nostre consentiment, el podem revocar en qualsevol moment. No obstant, quan el consentiment no ha estat necessari, per exemple, si utilitzem dades d'una font accessible al públic, o la publicació de notificacions de denúncies als diaris oficials per no haver estat possible practicar la notificació, pot entrar en marxa el dret d'oposició.

És el dret per tal que no es porti a terme el tractament de les pròpies dades o se cessi en aquest tractament, quan no ha estat necessari el seu consentiment per al tractament i una llei no disposi el contrari.

Es sol·licita l'exclusió del tractament de les dades relatives a l'afectat.

Termini per a resoldre: 10 dies.

# Infraccions i sancions

Article 44 de la LOPD: Tipus d'infraccions (lleus, greus i molt greus).

Article 46 de la LOPD: Sancions.

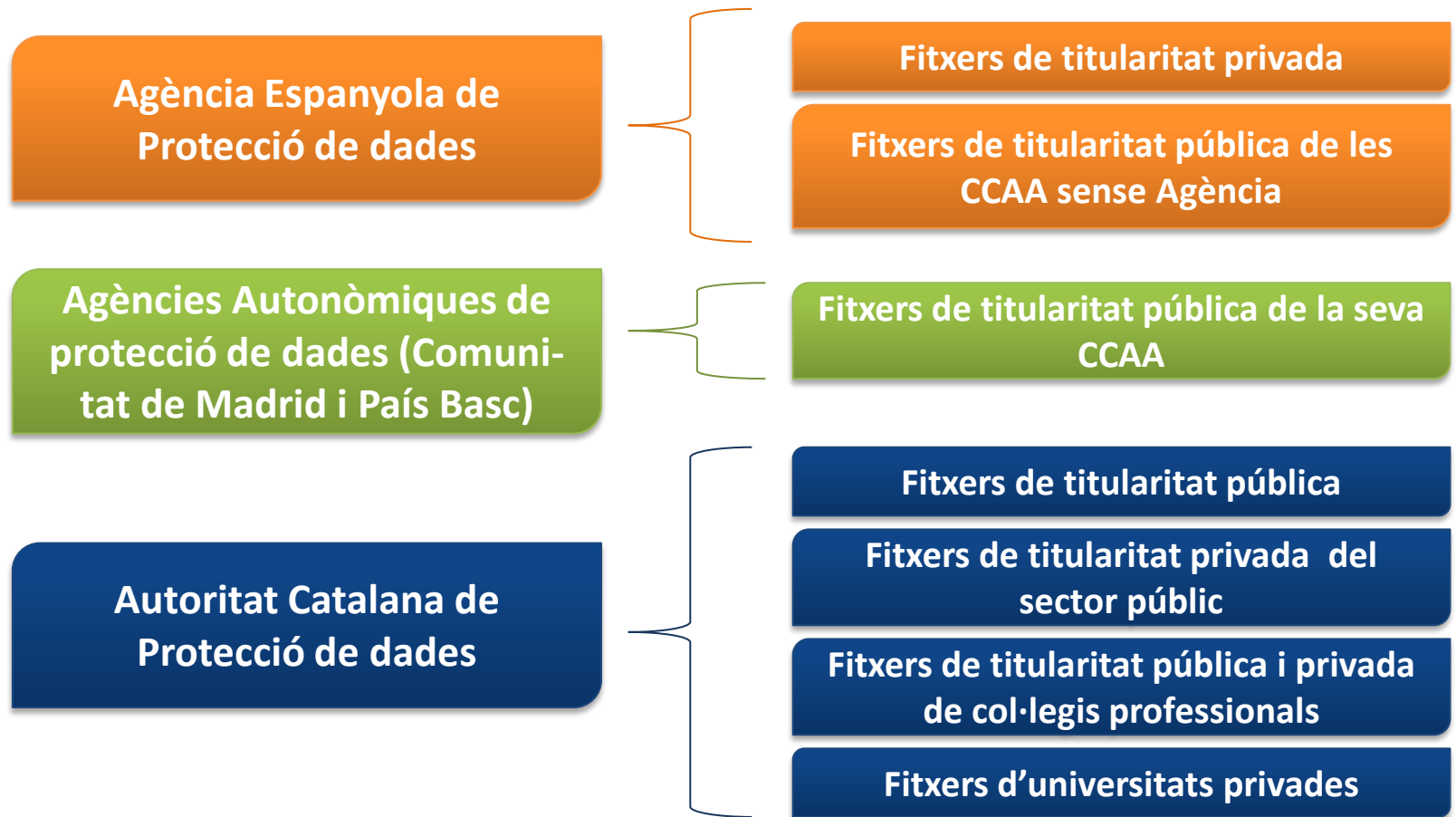
- a) Infraccions lleus: multa de 900 a 40.000 euros.
- b) Infraccions greus: multa de 40.001 a 300.000 euros.
- c) Infraccions molt greus: multa de 300.001 a 600.000 euros

A les Administracions públiques no hi ha sancions econòmiques, sinó que es requereix al responsable del fitxer per tal que adopti les mesures d'ordre intern que impedeixin que en el futur es produeixi una nova infracció del mateix tipus. Si el requeriment no és atès, l'Autoritat pot immobilitzar el fitxer. També, el/la directora/a de l'Autoritat pot proposar la iniciació d'actuacions disciplinàries a les persones responsables.

El responsable del fitxer ha de comunicar a l'Autoritat les resolucions adoptades. El director o la directora de l'Autoritat de PD ha de comunicar al Síndic de Greuges de Catalunya les actuacions que faci i les resolucions adoptades.

Decret 278/1993, de 9 de novembre, sobre el procediment sancionador d'aplicació als àmbits de competència de la Generalitat, segons el previst a la DT 2a de la Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades.

# Agències/Autoritat de Protecció de dades



# Assignació de competències en matèria de PD a la UB

**Rector:** decideix la **creació**, modificació, i supressió dels fitxers. També designa al responsable dels fitxers de la UB cada vegada que se'n creen de nous.

**Responsable dels fitxers:** És la persona física o jurídica, pública o privada, o òrgan administratiu, que sol o conjuntament amb altres decideix sobre la finalitat, el contingut i l'ús del tractament de les dades personals que conté el fitxer, encara que no ho faci materialment. En la UB, és el secretari general (òrgan unipersonal). Sobre el responsable del fitxer recauen les principals obligacions establertes per la LOPD i li correspon vetllar pel compliment de la normativa en PD.

El responsable dels fitxers ha de **notificar** els fitxers, oferir el dret d'informació en la recollida de dades, assegurar-se que es compleix amb el principi de qualitat, obtenir el consentiment quan calgui, autoritzar les cessions de dades, garantir els deures de secret i de seguretat, garantir l'exercici dels drets ARCO, assegurar-se que es compleix el disposat per l'art. 12 LOPD i resta de normativa aplicable, nomenar al responsable de seguretat (a proposta del gerent).

**Comissió de Seguretat de la LOPD:** té assignades les funcions de Responsable de Seguretat de la LOPD de tots els fitxers de titularitat de la UB (designació de 15 de Juliol de 2010). Aquesta comissió està integrada per:

- a) El Secretari General, que exerceix la presidència.
- b) Director/a de l'Àrea de Serveis Comuns i Grup UB.
- c) Director/a de l'Àrea TIC.
- d) Director/a de l'Àrea de Recursos Humans.
- e) Vocal de Secretaria General.



## **2. La gestió acadèmica i el dret fonamental a la protecció de les dades de caràcter personal**

# Fitxer de Gestió Acadèmica

**Nom del fitxer:** [Gestió Acadèmica](#)

**Finalitat i usos previstos:** Accés a la universitat. Preinscripció. Admissió, matrícula, avaluació i gestió de l'expedient acadèmic. Convalidacions. Informació. Anàlisi de l'evolució i el rendiment dels estudiants. Acreditació d'estudis realitzats. Registre i expedició de títols. Estudis per a estrangers. Assegurança escolar. Emissió del carnet. Elaboració del cens electoral. Màsters oficials. Postgraus propis.

**Persones o col·lectius afectats:** Sol·licitants d'accés a la Universitat de Barcelona i estudiants matriculats.

**Sistema de tractament utilitzat en la seva organització:** automatitzat i no automatitzat

**Procedència de les dades:** Del propi interessat o del seu representant legal i/o d'administracions públiques.

**Procediment de recollida de les dades:** Formularis. Transmissió electrònica.

**Estructura bàsica del fitxer i tipus de dades:** Dades de caràcter identificatiu (DNI/NIF o NIE, número de la Seguretat Social/mutualitat, nom i cognoms, adreça postal electrònica, telèfon, signatures i fotografia). Dades de característiques personals (estat civil, edat, dades familiars, data i lloc de naixement, sexe, nacionalitat, llengua materna, passaport i permís de residència). Dades de circumstàncies socials (característiques d'allotjament o habitatge). Dades acadèmiques i professionals (formació, titulacions, historial acadèmic i experiència professional). Dades econòmico-financeres i d'assegurances (dades bancàries i assegurances).

**Cessions de dades i transferències internacionals previstes:** Únicament es preveu cedir-les a tercers qual la cessió estigui autoritzada per una llei (Tresoreria General de la Seguretat Social), a altres administracions públiques per a l'exercici de competències iguals o que versin sobre les mateixes matèries (Generalitat de Catalunya, Ministeri competent, Consejo de Universidades), i quan sigui necessari per desenvolupar la relació jurídica amb la persona interessada (entitats bancàries per tal de gestionar el cobrament de la matrícula, Agència de Gestió d'Ajuts Universitaris i de Recerca). Amb el consentiment previ dels alumnes, es podran cedir les dades a entitats vinculades a la Universitat o que prestin serveis educatius (cursos, beques, avantatges per a estudiants). No es preveuen transferències internacionals.

**Persona jurídica responsable del fitxer:** Universitat de Barcelona

**Unitat per exercir els drets d'accés, rectificació, cancel·lació i oposició:** Secretaria General de la Universitat de Barcelona, Gran Via de les Corts Catalanes, 585, 08007-Barcelona.

**Mesures de seguretat:** Nivell bàsic.

# Fitxer de Beques

**Nom del fitxer:** [Beques](#)

**Finalitat i usos previstos:** Gestió administrativa per a la sol·licitud i tramitació dels programes de beques per a estudiants de la Universitat de Barcelona i centres adscrits.

**Persones o col·lectius afectats:** Estudiants que sol·licitin les beques i ajuts.

**Sistema de tractament utilitzat en la seva organització:** automatitzat i no automatitzat

**Procedència de les dades:** Del propi interessat o del seu representant legal i/o d'administracions públiques i entitats privades.

**Procediment de recollida de les dades:** Entrevistes. Formularis. Transmissió electrònica.

**Estructura bàsica del fitxer i tipus de dades:** Dades de salut (grau d'incapacitat o la simple declaració de la condició de discapacitat o invalidesa de l'estudiant). Dades de caràcter identificatiu (DNI/NIF, nom i cognoms, adreça postal i electrònica, telèfon, signatura i NIUB o número d'identificació de l'estudiant). Dades de característiques personals (estat civil, dades familiars, data i lloc de naixement, nacionalitat, edat i sexe). Dades de circumstàncies socials (propietats o possessions). Dades acadèmiques i professionals (formació, titulacions, historial acadèmic). Dades d'ocupació laboral (situació d'atur).

**Cessions de dades i transferències internacionals previstes:** Ministeri en raó de la competència sobre la matèria, Consejo de Universidades, Generalitat de Catalunya, Agència de Gestió d'Ajuts Universitaris i de Recerca (AGAUR). No es preveuen transferències internacionals.

**Persona jurídica responsable del fitxer:** Universitat de Barcelona.

**Unitat per exercir els drets d'accés, rectificació, cancel·lació i oposició:** Secretaria General de la Universitat de Barcelona, Gran Via de les Corts Catalanes, 585, 08007-Barcelona.

**Mesures de seguretat:** Nivell bàsic.

# Fitxer de Mobilitat dels estudiants

**Nom del fitxer:** [Mobilitat dels estudiants](#)

**Finalitat i usos previstos:** Gestió de programes de mobilitat i intercanvi d'estudiants. Emissió del carnet de la UB. Estadístiques internes. Arxiu.

**Persones o col·lectius afectats:** Estudiants propis o d'altres universitats que participen en programes de mobilitat i intercanvi.

**Sistema de tractament utilitzat en la seva organització:** automatitzat i no automatitzat

**Procedència de les dades:** Del propi interessat o del seu representant legal i/o d'administracions públiques.

**Procediment de recollida de les dades:** Formularis. Transmissió electrònica.

**Estructura bàsica del fitxer i tipus de dades:** Dades de caràcter identificatiu (DNI/NIF o NIE, nom i cognoms, adreça postal i electrònica, telèfon, número d'identificació de l'estudiant, passaport, fotografia). Dades de característiques personals (data i lloc de naixement, sexe, nacionalitat, llengua materna i coneixement d'idiomes). Dades acadèmiques i professionals (formació i titulacions, historial acadèmic, nom i adreça electrònica del tutor, i crèdits superats). Dades econòmico-financeres i d'assegurances (dades bancàries).

**Cessions de dades i transferències internacionals previstes:** Únicament es preveu cedir-les a tercers quan sigui necessari per desenvolupar la relació jurídica amb la persona interessada (universitats que han subscrit un conveni bilateral amb la UB). Amb el consentiment previ dels alumnes, es podran cedir les dades a entitats vinculades a la Universitat o que prestin serveis educatius (cursos, beques, avantatges per a estudiants). Únicament es preveu transferir-les quan sigui necessari per la celebració o execució d'un contracte celebrat o per celebrar, en interès de l'afectat, pel responsable del fitxer i un tercer (art. 34 LOPD). Universitats que han subscrit un conveni bilateral amb la UB

**Persona jurídica responsable del fitxer:** Universitat de Barcelona

**Unitat per exercir els drets d'accés, rectificació, cancel·lació i oposició:** Secretaria General de la Universitat de Barcelona, Gran Via de les Corts Catalanes, 585, 08007-Barcelona.

**Mesures de seguretat:** Nivell bàsic.

# Fitxer de Bústia de consultes sobre activitats acadèmiques i formatives

**Nom del fitxer:** [Bústia de consultes sobre activitats acadèmiques i formatives](#)

**Finalitat i usos previstos:** Respondre a les consultes formulades per aquelles persones interessades en obtenir informació en relació amb les activitats acadèmiques i formatives de la Universitat de Barcelona.

**Persones o col·lectius afectats:** Sol·licitants d'informació i estudiants matriculats.

**Sistema de tractament utilitzat en la seva organització:** automatitzat.

**Procedència de les dades:** Del propi interessat o del seu representant legal.

**Procediment de recollida de les dades:** Formularis. Transmissió electrònica.

**Estructura bàsica del fitxer i tipus de dades:** Dades de caràcter identificatiu (nom i cognoms, adreça electrònica). Dades de característiques personals (data i lloc de naixement, sexe, nacionalitat). Dades acadèmiques i professionals (formació i titulacions).

**Cessions de dades i transferències internacionals previstes:** Amb el consentiment previ dels sol·licitants, es podran cedir les dades a entitats vinculades a la Universitat o que prestin serveis educatius (cursos, beques, avantatges per a estudiants). No es preveuen transferències internacionals.

**Persona jurídica responsable del fitxer:** Universitat de Barcelona

**Unitat per exercir els drets d'accés, rectificació, cancel·lació i oposició:** Secretaria General de la Universitat de Barcelona, Gran Via de les Corts Catalanes, 585, 08007-Barcelona.

**Mesures de seguretat:** Nivell bàsic.

# Fitxer de Difusió d'oferta formativa

**Nom del fitxer:** [Difusió d'oferta formativa](#)

**Finalitat i usos previstos:** fitxer “Difusió d’oferta formativa”, que té com a finalitat la difusió d’informació de l’oferta de postgraus, màsters oficials, doctorats, títols propis i formació continuada organitzats per la UB.

**Origen de les dades, col·lectius sobre el qual es pretén obtenir les dades o que està obligat a subministrar-les i procediment de recollida:** proporcionades pel propi interessat o pel seu representant legal i de fons accessibles al públic, a través de formularis o per transmissió electrònica. El col·lectiu del qual es pretén obtenir les dades son totes aquelles persones que desitgin rebre informació sobre l’oferta formativa.

**Estructura del fitxer i sistema de tractament emprat:** el fitxer de difusió d’oferta formativa, d’estructura automatitzada i no automatitzada, conté dades de caràcter identificatiu, de característiques personals i acadèmiques i professionals.

**Comunicacions de dades previstes:** les estipulades en la llei.

**Transferències internacionals de dades previstes:** no se’n preveuen.

**Òrgan administratiu responsable del fitxer:** Secretaria General.

**Òrgan administratiu davant del qual s’han d’exercir els drets d’accés, rectificació, cancel·lació i oposició:** Secretaria General de la Universitat de Barcelona, Gran Via de les Corts Catalanes, 585, 08007-Barcelona.

**Nivell de seguretat exigible:** bàsic.

# Fitxer de Projectes institucionals

**Nom del fitxer:** [Projectes institucionals](#)

**Finalitat i usos previstos:** Organització i gestió de cursos d'estiu i d'altres projectes.

**Persones o col·lectius afectats:** Persones que tinguin relació amb aquests cursos.

**Sistema de tractament utilitzat en la seva organització:** automatitzat i no automatitzat

**Procedència de les dades:** Del propi interessat o del seu representant legal.

**Procediment de recollida de les dades:** Entrevistes. Formularis. Transmissió electrònica.

**Estructura bàsica del fitxer i tipus de dades:** Dades de caràcter identificatiu (DNI/NIF o NIE, nom i cognoms, adreça postal i electrònica, telèfon, signatura electrònica i NIUB o número d'identificació de l'estudiant). Dades de característiques personals (data de naixement i nacionalitat). Dades d'ocupació laboral (ocupació).

**Cessions de dades i transferències internacionals previstes:** No estan previstes.

**Persona jurídica responsable del fitxer:** Universitat de Barcelona

**Unitat per exercir els drets d'accés, rectificació, cancel·lació i oposició:** Secretaria General de la Universitat de Barcelona, Gran Via de les Corts Catalanes, 585, 08007-Barcelona.

**Mesures de seguretat:** Nivell bàsic.

# Es pot crear un fitxer de Directori d'alumnes?

[Resolució APDCAT PS 26/2011](#): La persona denunciant exposava que a través de l'apartat "Directori d'alumnes", ubicat a l'apartat "Estudiants UAB" del web de l'UAB es podia accedir per Internet a les següents dades de caràcter personal dels estudiants d'aquesta universitat: nom i cognoms, facultat o escola i l'adreça de correu electrònic institucional.

La finalitat que va al·legar la universitat era "*facilitar les gestions acadèmiques per part del professorat de la UAB i del personal de les àrees i les unitats de gestió acadèmica de la Universitat, de manera que es garanteixi un sistema àgil d'interlocució amb els estudiants per allò que necessiti un contacte i un traspàs àgil d'informació més directe i exclusiu.*"

Doncs bé, a criteri d'aquesta Autoritat resultava excessiva la difusió a través d'Internet de les dades de caràcter personal de tots alumnes, sense cap tipus de restricció, atès que la finalitat de l'esmentat directori s'emmarcava dins l'àmbit de la comunitat universitària. En conseqüència, la UAB es va comprometre a mantenir aquest Directori però només "*accessible de manera exclusiva a la intranet, prèvia identificació per part d'aquelles persones que, **per raó del seu càrrec**, han d'accedir a aquelles dades.*" Per tant, s'havia de valorar quins usuaris havien de tenir accés a aquests recursos en funció de les tasques encomanades, circumstància que no es va complir en aquest cas, ja que hi podia accedir qualsevol persona a través d'Internet.



# La preinscripció universitària

Per accedir al primer curs d'un estudi de grau de qualsevol de les set universitats públiques de Catalunya i de la Universitat de Vic cal fer la preinscripció universitària. Aquesta preinscripció s'ha de formalitzar per Internet a l'adreça <https://acesnet.gencat.cat>. L'estudiant s'ha de registrar obtenint així una contrasenya que permetrà accedir als serveis del portal, una vegada identificat amb el DNI amb lletra (nacionalitat espanyola) o el NIE (amb permís de residència) o el passaport (resta d'alumnes). En el moment de formalitzar la preinscripció universitària, l'estudiant pot sol·licitar fins a 8 preferències, les quals han d'estar ordenades segons el grau d'interès. En el moment del registre, a l'estudiant se li mostra la següent clàusula a la pantalla,

## Informació sobre protecció de dades de caràcter personal

Segons la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, us informem que les vostres dades personals formaran part del tractament "Procés de preinscripció universitària" responsabilitat de la Secretaria General del Consell Interuniversitari de Catalunya, amb domicili a l'Avinguda de la Catedral, 6-8, 08002 Barcelona. **La seva finalitat és recollir i gestionar les dades de caràcter personal de l'alumnat que vol matricular-se, durant l'any lectiu, a les universitats que participen en el procés de la preinscripció universitària. Podeu exercir els vostres drets de l'afectat mitjançant escrit dirigit a la Secretaria General del Consell Interuniversitari de Catalunya, Avinguda de la Catedral, 6-8, 08002 Barcelona.**

**Accepto la política de protecció de dades**

L'Oficina d'Orientació per a l'Accés a la Universitat de la Generalitat de Catalunya gestiona els processos relatius a la preinscripció a la universitat, com a resultat de l'encàrrec de gestió al Consell Interuniversitari de Catalunya (art. 134 de la LUC de 2003). Aquesta Oficina trametrà a la universitat, mitjançant correu electrònic (amb clau d'accés), les dades dels alumnes admesos als centres pel procés de preinscripció universitària. L'habilitació legal es troba a l'article 21.2 LOPD "En tot cas, poden ser objecte de comunicació les dades de caràcter personal que una administració pública obtingui o elabori amb destinació a una altra". O també l'excepció prevista a l'article 11.2 c) LOPD.

# Matrícula: clàusules d'informació i cessió

Les dades de caràcter personal facilitades seran incorporades al fitxer «[Gestió Acadèmica](#)», les finalitats principals del qual són l'accés a la Universitat i la gestió acadèmica-administrativa. La Universitat de Barcelona té la titularitat d'aquest fitxer i la Secretaria General n'és l'òrgan responsable. D'altra banda, les vostres dades seran utilitzades per remetre-us **informació\*** sobre l'oferta de serveis. En qualsevol cas, podeu exercir els drets d'accés, rectificació, cancel·lació i oposició mitjançant una comunicació escrita —a la qual cal que adjunteu una fotocòpia del DNI o d'un altre document identificatiu— adreçada a la Secretaria General de la Universitat de Barcelona, Gran Via de les Corts Catalanes, 585, 08007 Barcelona, o enviant un missatge electrònic a l'adreça següent: [secretaria.general@ub.edu](mailto:secretaria.general@ub.edu).

¿Doneu el vostre consentiment perquè les dades corresponents a nom, cognoms, telèfon i adreces postal i electrònica es puguin cedir a tercers per a l'oferiment de serveis? En cas que doneu aquest consentiment, el podeu revocar en qualsevol moment Sí  No

*(\*) Informació i publicitat no és el mateix. Quan la informació institucional es troba barrejada amb informació publicitària deixa de ser institucional als efectes de la LOPD.*

# Peculiaritats d'algunes dades de caràcter personal dels estudiants

## 1) L'adreça electrònica institucional

L'adreça electrònica que la universitat facilita als estudiants també és una dada de caràcter personal\_([Resolució APDCAT PS 26/2011](#)):

El correu electrònic és una eina d'intercomunicació entre persones i no s'ha d'utilitzar com a eina de difusió d'informació, ja que per a aquest propòsit existeixen altres canals més adequats i efectius.

## 2) La fotografia

Consulta plantejada per una universitat madrilenya relativa a la realització de fotografies digitals per a la seva incorporació a l'expedient acadèmic. Resposta de l'Agència de protecció de dades de la Comunitat de Madrid, de maig de 2004:

*"Des de la perspectiva del principi de qualitat de les dades, s'entén que l'aportació i incorporació a l'expedient acadèmic de cada alumne matriculat de la seva fotografia, és una dada necessària per a la seva identificació que possibilitarà i facilitarà la gestió administrativa universitària, per exemple, per a la confecció del carnet universitari, per a la identificació posterior per cada professor, etc., considerant, per tant, legítim la seva obtenció i tractament.*

*Partint, per tant, de considerar la fotografia de cada alumne com una dada necessària i adequada per a la gestió administrativa derivada de la seva permanència a la Universitat, el fet que en l'actualitat es pretengui procedir a la seva digitalització, sota la protecció de dades no varia gens la legitimitat del tractament, ja que la protecció no varia per trobar en suport paper o en suport digital, sinó que la variació del suport que permetrà és la incorporació a la relació administrativa de les noves tècniques informàtiques"*

## 3) La condició de ser estudiant d'una facultat o escola

La dada consistent en el fet de formar part de la comunitat universitària com a estudiants d'una determinada facultat o escola, també és una dada de caràcter personal per que es pot inferir els estudis que es cursen ([Resolució APDCAT PS 26/2011](#))

# L'excepció del consentiment per a la recollida de dades dels estudiants

**Resposta a una consulta d'una universitat madrilenya, de 9 maig de 2004 (Agència de la Comunitat de Madrid)**

*"En el caso planteado, nos encontramos ante una relación de carácter administrativo existente entre los alumnos matriculados y la Universidad, que tiene como finalidad legítima la obtención del correspondiente título universitario, para lo que es necesario el tratamiento y gestión de determinados datos personales de los propios alumnos. Dicha relación administrativa implica que el consentimiento para el tratamiento de los datos de los alumnos **va implícito desde el momento en que se inicia la relación a través de la matrícula**, y ello porque la propia LOPD así lo excepciona en su artículo 6.2, al establecer que no será preciso el consentimiento del afectado para el tratamiento de sus datos, cuando dicho tratamiento se refiera a las partes de un contrato o precontrato, de una **relación** negocial, laboral o **administrativa** y el tratamiento sea necesario para su mantenimiento o cumplimiento".*

Si el tractament es fa amb una finalitat diferent, com pot ser la remissió **d'enviaments de publicitat**, no estaria emparat per aquesta excepció i requerirà el consentiment. L'art. 15 del RLOPD regula la sol·licitud del consentiment en el marc d'una relació contractual per a fins relacionats directament amb la mateixa. S'haurà de permetre a l'afectat que manifesti expressament la seva negativa al tractament. S'entendrà, quan es permeti la marcació d'una casella clarament visible i que no es trobi marcada.

# Transmissió intraadministrativa de dades

Ni la LOPD ni el seu reglament tracten d'una forma directa de la transmissió intraadministrativa, és a dir, entre diversos òrgans o unitats de la mateixa administració pública.

Si d'acord amb la normativa de protecció de dades es considera comunicació tota revelació de dades realitzada a una **persona diferent** de la persona interessada, les transmissions de dades entre òrgans o unitats que formen part d'una mateixa administració, és a dir, d'una mateixa persona jurídica, no es consideren una comunicació de dades a efectes de comunicar les dades, sempre que es doni el **principi de finalitat**.

Si la transmissió entre òrgans diferents de la mateixa administració pública no respon a la mateixa finalitat estarem davant d'una cessió de dades i caldrà obtenir el consentiment de l'afectat ([AVPD CN11-031](#)).

El fet que una unitat administrativa gestioni o tracti dades personals, no vol dir que totes les persones d'aquesta unitat puguin accedir a totes les dades. Segons l'article 91 del RLOPD,

1. Els usuaris han de tenir accés només als recursos que necessitin per a l'exercici de les seves funcions.
2. El responsable del fitxer s'ha d'encarregar que hi hagi una relació actualitzada d'usuaris i perfils d'usuaris, i els accessos autoritzats per a cadascun d'ells.
3. El responsable del fitxer ha d'establir mecanismes per evitar que un usuari pugui accedir a recursos amb drets diferents dels autoritzats.

# Cessió o comunicació a entitats del grup UB

Un ens instrumental és una entitat, pública o privada, creada per l'Administració principal per tal de servir com instrument d'actuació. L'anomenada “*administració instrumental*” inclou un conjunt molt divers d'entitats que poden estar dotades de personalitat jurídica, patrimoni i pressupost propis, i poden tenir una denominació, naturalesa, tipologia i règim jurídic molt divers entre sí, i no es pot generalitzar respecte el tractament legal que reben.

[Informe Jurídic 0494/2008](#): És criteri uniforme de l'AEPD que l'existència d'un grup d'empreses no afecta per a que cadascuna de les societats integrades en el mateix no mantingui diferenciada i plena la seva personalitat jurídica. A tots els efectes jurídics, la circumstància que una societat estigui participada per una altra, no afecta el fet que ambdues siguin diferents persones, de manera que la comunicació de dades es produeix entre dues persones diferents, sense que hi hagi una previsió legal que flexibilitzi els requisits per a la legitimitat de la cessió. Aquest criteri ha estat ratificat per la Sentència de la Secció Novena de la Sala Contenciosa Administrativa del Tribunal Superior de Justícia de Madrid, de 16 d'octubre de 2000, quan en el seu fonament de dret quart assenyala que, *"Qualsevol empresa és lliure de constituir una entitat en qualsevol de les formes societàries que el dret mercantil regula. Així mateix, les empreses poden unir-se a través de les diferents formes regulades en dret: fusió, absorció, etc. Però, per descomptat, el que no es possible és que hi hagi dues societats anònimes i, com a tals, independents i amb personalitat jurídica autònoma i que pel fet que una sigui propietat de l'altra, el particular que contracta amb la primera pugui veure's perjudicat, precisament, per l'estructura empresarial que la societat ha triat. Si la recurrent ha preferit constituir dues societats i treballar amb elles de manera independent, beneficiant-se així del manteniment de dues persones jurídiques diferents, ha de ser posteriorment coherent amb aquesta decisió"*

[Informe CNS 17/2010 de l'Autoritat Catalana de PD](#). L'ens instrumental ha de ser considerat un “tercer” aliè a la Administració pública i al titular de les dades, i per tant cal sotmetre aquesta comunicació al règim de la cessió de dades establert en la LOPD (articles 11 i 21).

# Qualificacions acadèmiques

LOU 2007. Disposició addicional vint-i-unena. *Protecció de dades de caràcter personal*

3. *No és necessari el consentiment dels estudiants per a la publicació dels resultats de les proves relacionades amb l'avaluació dels seus coneixements i competències, ni dels actes que siguin necessaris per a l'adequada realització i seguiment de l'avaluació.* En algunes universitats estrangeres no es poden fer públiques les qualificacions (Regne Unit, França, EEUU,..).

A la UB, abans de la normativa de 2012, quan es publicaven llistes amb notes, l'estudiant havia de ser identificat només amb el NIUB: art. 18.3 Normes reguladores de l'avaluació i la qualificació dels aprenentatges de 2006 "*La informació pública sobre els resultats s'ha de fer mitjançant una llista en que l'estudiant s'identifiqui només amb el NIUB (número d'identificació que es proporciona a cada estudiant en el moment d'ingressar a la universitat)*"

A partir del curs 2012-2013, la Normativa reguladora dels plans docents de les assignatures i de l'avaluació i la qualificació dels aprenentatges (Aprovada per Consell de Govern en data 8 de maig de 2012), assenjala a l'article 18.4 que: "*La informació pública sobre el resultat de les avaluacions, siguin parcials o finals, té lloc mitjançant els mecanismes establerts amb aquesta finalitat. El professorat pot fer la difusió de les qualificacions de manera virtual, a través de les aplicacions institucionals establertes a aquest efecte*", per afegir posteriorment a l'Annex, que "*La publicació de les qualificacions virtuals es fa a través de l'espai específic de l'assignatura al Campus Virtual (o a l'espai que el substitueixi en el futur) o a través de l'expedient acadèmic de l'estudiant (Món UB), al qual es pot accedir, de manera individual i privada, telemàticament*"

A la vista d'aquesta nova normativa interna, s'ha d'entendre que a la UB ja no es publiquen llistes amb les qualificacions dels alumnes, sinó que aquests accedeixen a aquestes de forma individual i telemàtica (Món UB i Campus virtual).

# Pot un professor accedir a l'expedient acadèmic d'un alumne?

## Opinió de l'Agència de protecció de dades de la Comunitat de Madrid:

*"En la mesura que un professor té una relació directa amb cada un dels seus alumnes tindrà legitimitat per accedir als expedients acadèmics de cada un d'ells, sempre que aquest accés tingui una finalitat acadèmica i per tant compatible amb les finalitats declarades del fitxer. No obstant això, cal assenyalar que l'accés dels professors al Fitxer Expedients d'Alumnes o Gestió Acadèmica no hauria de ser indiscriminat, sinó que cada professor hauria de tenir accés només a les dades dels seus alumnes d'aquest any acadèmic, doncs no estaria justificada la finalitat l'accés a les dades de la resta dels alumnes. En conseqüència, el responsable del fitxer ha d'establir els controls d'accés necessaris per complir amb aquesta mesura, tenint en consideració el que preveu l'article 91 del Reial Decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la LOPD"*



# Poden els pares tenir accés a les qualificacions acadèmiques dels estudiants majors d'edat?

## [Opinió de l'Agència de Protecció de Dades de la Comunitat de Madrid](#)

El punt de partida és la previsió recollida a l'art. 39.3 Constitució Espanyola, que imposa als pares el deure assistència en tots els ordres als fills, dintre o fora del matrimoni, durant la seva minoria d'edat i en els casos en els quals legalment procedeixi. En aquest sentit, l'art. 143 Codi Civil obliga als pares a prestar als seus fills aliment en tota l'extensió que assenyalava l'art. 142, que estableix que: "*Els aliments comprenen també l'educació i instrucció de l'alimentat mentre sigui menor d'edat i fins i tot després, quan no hagi acabat a seva formació per causa que no li sigui imputable*". La conjunció d'aquests dos preceptes (arts. 142 i 143) justificaria que l'habilitació legal que es reconeixia a favor dels pares de fills majors d'edat en el cas que segueixen cobrint la seva instrucció i educació.

Al costat d'aquest argument s'acumula un altre, d'igual naturalesa però emparat en una altra habilitació legal, ara a l'article 37 de la Llei 30/1992, del règim jurídic administratiu, que exigeix un interès legítim i directe per tal d'accedir als expedients administratius (i un expedient acadèmic, on consten les qualificacions, ho és). Pensem en un pare i/o mare que assumeix el pagament dels estudis del seu fill universitari. Tal vegada aquest pare o aquesta mare han tingut, fins i tot, que demanar un crèdit per a cobrir les despeses de l'ensenyament. Han sacrificat altres interessos familiars a costa de proporcionar al seu fill l'educació. El jove, no obstant això, no sembla estudiar mai. Passen els anys i l'estudiant no els ensenya mai les qualificacions. Poden aquests pares sol·licitar l'accés a l'expedient acadèmic? Si són els pares que assumeixen les despeses dels estudis del seu fill, ostentarien un interès legítim i directe a conèixer el resultat d'aquesta inversió econòmica en l'educació del fill i, en conseqüència, és el propi art. 37 de la Llei 30/1992 el que els hi obre l'accés a l'expedient acadèmic.

Com a conclusió, doncs i en la nostra opinió, res justifica una restricció a l'accés dels expedients acadèmics dels pares dels estudiants universitaris majors d'edat en la situació acabada d'esmentar.

# Es poden facilitar dades dels estudiants a una empresa per a una oferta de treball?

Si reps una trucada d'una empresa que recluta personal sol·licitant noms i adreces d'estudiants amb una nota mitjana determinada o més, dient que tenen una bona oferta d'ocupació per a aquests alumnes. Pots facilitar aquesta informació?

No podríem facilitar cap dada d'un estudiant. El més adequat seria que es remeti l'empresa a la Borsa de Treball, ja que són els experts per tractar aquest tipus de temes, garantint la reserva o confidencialitat que calgui.

# Podem facilitar dades d'un estudiant a una universitat estrangera?

Des d'una universitat nord-americana se sol·licita a la Universitat de Barcelona verificació sobre si una determinada persona està matriculada o inscrita en la nostra universitat. Concretament, es demana si es troba a temps complet i quin va ser el primer quadrimestre o semestre de la seva inicial matriculació. S'assenyala que aquesta informació és rellevant en relació al seu progrés acadèmic en la NCAA (la National Collegiate Athletic Association (NCAA) és una associació composta d'unes 1200 institucions, conferències, organitzacions, universitats i individus que organitzen la majoria dels programes esportius universitaris dels EUA).

## Resposta

La Directiva 95/46/CE del Parlament Europeu i del Consell, així com la nostra Llei de protecció de dades de caràcter personal de 1999, no permet facilitar l'esmentada informació sense el consentiment de la persona afectada. El més pràctic seria contactar amb la persona sobre la que es sol·licita la informació i plantejar-li la qüestió. En cas que aquesta accepti que es faciliti aquesta informació a Ohio State Athletics, caldrà que ens ho comuniqui mitjançant correu electrònic, que caldria conservar.

Un cop rebut el correu electrònic, ja es podria respondre a la demanda.

# Transferències internacionals de dades

Una transferència internacional de dades és un tractament de dades que suposa una transmissió de dades fora del territori de l'Espai Econòmic Europeu (UE+Islandia, Liechtenstein i Noruega) bé constitueixi una cessió o comunicació de dades, bé tingui per objecte la realització d'un tractament de dades per compte del responsable del fitxer establert en territori espanyol (art. 5.1.s del Reglament).

L'article 33 LOPD expressa que no es poden fer transferències de dades personals a països que no proporcionin un nivell de protecció equiparable al que presta la LOPD, llevat que, a més d'haver-se observat el que disposa aquesta Llei, s'obtingui autorització prèvia del director de l'AEPD, que només la pot atorgar si s'obtenen garanties adequades. El caràcter adequat del nivell de protecció que ofereix el país de destinació, l'avalua l'AEPD atenent totes les circumstàncies que concorrin en la transferència o categoria de transferència de dades. El procediment per a sol·licitar aquesta autorització el regula el RLOPD (de l'art. 137 al 144).

Aquesta regla no és aplicable quan l'afectat o usuari hagi donat el seu consentiment inequívoc a la transferència prevista o aquesta tingui com a destinació un Estat membre de l'Espai Econòmic Europeu, o un estat respecte del qual la Comissió de les Comunitats Europees, hagi declarat que garanteix un nivell de protecció adequat.

Principis de Port Segur (Safe Harbour). La Decisió de la Comissió Europea de 26 de juliol de 2000, sobre l'adequació de la protecció conferida pels principis de port segur per a la protecció de la vida privada i les corresponents preguntes més freqüents, publicades pel Departament de Comerç dels Estats Units d'Amèrica. Segons el seu considerant 5 s'assenyala que *"El nivell adequat de protecció de la transferència de dades des de la Comunitat (Europea) a Estats Units d'Amèrica, reconegut per la present decisió, s'ha d'assolir si les entitats compleixen els principis de port segur per a la protecció de la vida privada, a fi de protegir les dades personals transferides d'un Estat membre a Estats Units d'Amèrica, així com les preguntes més freqüents, en què es proporciona orientació per aplicar els principis, publicades pel Govern dels Estats Units d'Amèrica amb data 21 de juliol de 2000"*.

Patriot Act, de 2001: Tota empresa nord-americana està obligada a facilitar a les agències governamentals (FBI i CIA) que ho sol·licitin les dades personals dels seus clients o dels usuaris dels seus serveis. N'hi ha prou amb el simple requeriment, sense necessitat de justificació ni avís als interessats ni, per descomptat, el seu consentiment, tant si són ciutadans americans o europeus.

# Hem de facilitar a una Administració pública tributària determinades dades personals d'un estudiant?

Un Servei de Gestió Tributària d'un Consell Comarcal sol·licita determinades dades de caràcter personal com el domicili d'un estudiant de la UB, per causa d'un deute tributari.

L'article 94.1 de la Llei 58/2003, de 17 de desembre general tributària, assenyala que "Les autoritats, sigui quina sigui la seva naturalesa, els titulars dels òrgans de l'Estat, de les comunitats autònomes i de les entitats locals, els organismes autònoms i les entitats públiques empresarials, les cambres i corporacions, escoles i associacions professionals, les mutualitats de previsió social, les altres entitats públiques, incloses les gestores de la Seguretat Social i els qui, en general, exerceixin funcions públiques, estan obligats a subministrar a l'Administració tributària totes les dades, informes i antecedents amb transcendència tributària que demani aquesta mitjançant disposicions de caràcter general o a través de requeriments concrets, i a prestar, a ella i als seus agents, suport, concurs, auxili i protecció per a l'exercici de les seves funcions Així mateix, participaran en la gestió o exacció dels tributs mitjançant les advertències, repercussions i retencions, documentals o pecuniàries, d'acord amb el que preveuen les lleis o disposicions reglamentàries vigents.(...)

Així, doncs, caldrà cedir les dades personals que tinguin transcendència tributària.

# Cessió de dades a les Forces i Cossos de seguretat (1)

El manteniment de la seguretat pública s'exerceix a través de les forces i cossos de seguretat (art. 1.4 de la L.O. 2/1986, de 13 de març). D'acord amb l'art. 2, en aquest concepte s'han d'incloure tant les forces i cossos de seguretat de l'Estat, els cossos de policia dependents de les CCAA i els cossos de policia dependents de les corporacions locals.

Juntament amb les funcions directament adreçades a esbrinar les actuacions delictives i detenció dels presumptes responsables, també hi ha d'altres funcions encomanades a la Policia per al compliment de les actuacions ordenades per l'autoritat judicial o el Ministeri Fiscal (art. 549.1 de la L.O. Del Poder Judicial i art. 2 RD 769/1987, de 19 de juny, de la policia judicial): Policia judicial/policia científica.

En conseqüència, s'ha de distingir, d'una banda aquelles actuacions de les Forces i Cossos de Seguretat que són dutes a terme en compliment d'un mandat judicial o d'un requeriment efectuat pel Ministeri Fiscal d'aquelles altres que es porten a terme per pròpia iniciativa o a instància d'un superior jeràrquic.

Respecte les actuacions de la policia dutes a terme en compliment d'ordres de l'autoritat judicial o el MF, s'ha de tenir en compte que només són executors d'aquestes ordres. La petició policial es dirigirà al responsable del fitxer. I ja hem vist que la cessió de dades a l'autoritat judicial/fiscal no es precisa el consentiment.

La cessió es pot delegar en el centre. La sol·licitud s'haurà de cursar a través d'un suport documental.

# Cessió o comunicació de dades a les Forces i Cossos de seguretat (2)

Tractarem ara la cessió de dades a les forces i cossos de seguretat en exercici de les funcions d'esbrinament de responsables i les circumstàncies dels fets delictius i no en les funcions d'auxili judicial que acabem de veure.

L'article 22.2 de la LOPD exigiria que quan no es disposi del consentiment dels titulars de les dades personals, la cessió de dades personals es faci únicament

- a) per raó de la prevenció d'un perill real per a la seguretat pública, o
- b) per a la repressió d'infraccions penals (sense requerir que sigui per raó d'un cas o d'una investigació concreta, sinó que simplement que siguin necessaris per atendre o realitzar les finalitats policials).

L'AEPD ha establert les següents condicions quan les forces i cossos de seguretat exerceixen aquestes funcions (Informe jurídic [0133/2008](#)):

"Que quedi degudament acreditat que l'obtenció de les dades resulta necessària per a la prevenció d'un perill real per la seguretat pública o per a la repressió d'infraccions penals. Si es tracta de dades protegides (salut), les dades han de ser absolutament necessàries per als fins d'una **investigació concreta**."

# La informació en Internet no és de lliure utilització

Es denunciava la recepció d'una comunicació comercial no sol·licitada, que havia estat rebuda per tots els usuaris de correu electrònic de la Unitat de Química Física de la Universitat Autònoma de Barcelona (60 persones). El missatge enviat per correu electrònic oferia informació comercial, en concret la següent publicitat de l'entitat:

*"Servei informàtic a domicili, reparacions i components, Resolució d'incidències puntuals i contractes de manteniment, Seguretat (virus, spyware, atacs de hackers, intrusions ...), Connexió a Internet (configuració ADSL, Cable), Xarxes sense fils, Aspectes del maquinari, problemes amb impressores, Mal funcionament de Windows, Realització de Còpies de seguretat, optimització, drivers, reinstal·lacions, Recuperació de dades esborrats accidentalment, Disseny de pàgines web."*

El denunciat manifesta que l'adreça de correu objecte de la denúncia va ser extreta de pàgines web públiques i de lliure accés, que va utilitzar l'enviament d'una comunicació comercial per donar a conèixer la seva activitat professional, per no tenir mitjans econòmics per publicitar d'una altra manera, i que la finalitat dels missatges enviats ser merament informativa o publicitària, sense cap intenció d'estafa, o falsedat. Afegeix que el nombre de missatges enviats era irrisori, comparat amb els enviaments de "spammers" professionals i que el seu criteri de selecció dels destinataris impedeix grans campanyes indiscriminades.

L'AEPD sanciona l'empresa per no poder acreditar el consentiment exprés, de manera prèvia i informada, a 30.000 euros de multa ([Resolució: R/00570/2007](#))



# L'encarregat del tractament no pot utilitzar les dades per a una altra finalitat

[Resolució PS 35/2010](#)

La UAB subscriu un conveni/contracte amb una entitat financera amb la finalitat que aquesta prestés per compte de la universitat el servei d'emissió del "*carnet UAB*".

Una estudiant s'assabenta que li han obert un compte corrent sense que tingúes coneixement, i presenta una denúncia davant l'APDCAT imputant a la UAB haver cedit les seves dades com a estudiant a l'entitat financera.

L'APDCAT considera que la UAB no havia comès cap infracció, sinó que el que havia fet és formalitzar un contracte de serveis incloent una clàusula que conté els requisits de l'article 12 LOPD i del reglament RLOPD i, per tant, arxiva la denúncia contra la universitat. No obstant, inicia d'ofici un procediment sancionador contra l'entitat financera.

L'APDCAT considera que l'entitat financera va utilitzar les dades facilitades per la UAB per "*tractar les dades personals d'una determinada estudiant amb una finalitat diferent a la que figurar en el contracte abans esmentat, i en concret, per obrir un compte corrent a aquesta estudiant*" (fet provat segon), i la sanciona per una infracció greu a una multa de 60.101,21 euros.

# Cancel·lació de dades personals

Les dades seran cancel·lades quan hagin deixat de ser necessàries o pertinents per a la finalitat per a la qual van ser recavades. La cancel·lació donarà lloc al **bloqueig** de les dades, conservant-se únicament a la disposició de les Administracions Públiques, Jutges i Tribunals, per a l'atenció de les possibles responsabilitats nascudes del tractament, durant el termini de prescripció d'aquestes. Complert el citat termini s'haurà de procedir a la supressió (art. 16.3 LOPD).

No obstant, no procedeix eliminar els documents que consten en expedients administratius, atès que l'Administració té l'obligació d'arxivar la documentació que pertany als esmentats expedients, en virtut de les lleis de patrimoni corresponents i les seves normes de desenvolupament, que regeixen la guàrdia i custòdia d'aquests documents, el seu emmagatzematge, la forma i el temps de destrucció.

**Vigileu!**. No es poden llançar a l'escombraria documents que contenen dades de caràcter personal. Resolució del procediment sancionador [PS 64/2011](#) al Departament D'Ensenyament de la Generalitat. La policia local va aixecar acta en comprovar que al costat del contenidor de cartró i paper hi havia uns documents amb dades de caràcter personal que tenien com a capçalera aquest Departament.

### **3. Mesures de seguretat més significatives a l'àmbit dels fitxers la gestió acadèmica**

# La seguretat i les mesures de seguretat

El fet de tractar dades de caràcter personal ens obliga a protegir-les. Per fer-ho, hem d'adoptar mesures de seguretat perquè les dades que tractem no es perdin o no s'alterin de manera accidental o malintencionada. I, per descomptat, hem d'evitar que persones que no han de fer res amb aquestes dades les puguin veure o utilitzar.

La normativa (art. 9 LOPD) obliga a aplicar unes mesures de seguretat concretes d'acord amb el tipus de dades que tractem. Evidentment, com més sensible o delicada sigui la dada personal, més exigents seran les mesures de protecció; és per això que les mesures de seguretat poden ser de nivell bàsic, mitjà o alt.

L'article 9 de la LOPD estableix el següent:

1. *“El responsable del fitxer i, si s'escau, l'encarregat del tractament han d'adoptar les mesures de caràcter tècnic i organitzatiu necessàries que garanteixin la seguretat de les dades de caràcter personal i n'evitin l'alteració, la pèrdua, el tractament o l'accés no autoritzat, tenint en compte l'estat de la tecnologia, la naturalesa de les dades emmagatzemades i els riscos a què estan exposats, tant si provenen de l'acció humana o del medi físic o natural.*
2. *No s'han de registrar dades de caràcter personal en fitxers que no compleixin les condicions que es determinin per via reglamentària en relació amb la seva integritat i seguretat i a les dels centres de tractament, locals, equips, sistemes i programes.”*

La normativa exigeix que aquestes mesures de seguretat es recullin i descriguin en el que anomena *document de seguretat* (Art. 88.1 del RLOPD). El responsable del fitxer ha d'elaborar un document de seguretat que reculli les mesures d'índole tècnica i organitzativa conformes amb la normativa de seguretat vigent que és de compliment obligat per al personal amb accés als sistemes d'informació.

Veure: [http://www.ub.edu/secretariageneral/ca/proteccio\\_dades/pd\\_docsseguretat.html](http://www.ub.edu/secretariageneral/ca/proteccio_dades/pd_docsseguretat.html)

# Aplicació dels Nivells de seguretat

**Tots els fitxers o tractaments** de dades de caràcter personal han d'adoptar les mesures de seguretat qualificades de **nivell bàsic**.

S'han d'implantar, a més de les mesures de seguretat de nivell bàsic, les mesures de **nivell mitjà**, en els següents fitxers o tractaments de dades de caràcter personal:

- a) Els que continguin un conjunt de dades de caràcter personal que ofereixin una definició de les **característiques o de la personalitat dels ciutadans** i que permetin avaluar determinats aspectes de la seva **personalitat o comportament** (hàbits de compra, relacions personals, ..)

A més de les mesures de nivell bàsic i mitjà, les mesures **de nivell alt** s'han d'aplicar en els següents fitxers o tractaments de dades de caràcter personal:

- a) Els referits a ideologia, **afiliació sindical**, religió, creences, origen racial, **salut** o vida sexual.
- b) Els que continguin dades derivades d'actes de **violència de gènere**.

En el cas de fitxers o tractaments de dades d'ideologia, **afiliació sindical**, religió, creences, origen racial, **salut** o vida sexual només s'han d'implantar les mesures de seguretat de nivell bàsic quan:

- a) Les dades s'utilitzin amb l'única finalitat de realitzar una **transferència dinerària** a les entitats de què els afectats siguin associats o membres.
- b) Es tracti de **fitxers o tractaments no automatitzats** on de forma **incidental o accessòria** s'incloguin les dades sense tenir relació amb la seva finalitat.

També es poden implantar les mesures de seguretat de nivell bàsic en els 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 l'afectat, **amb motiu del compliment de deures públics** (art. 81.6 del RLOPD)

# Quadre resum de mesures de seguretat

<b>Mesures de seguretat</b> (a) Automatitzats / (na) No automatitzats		<b>Bàsic</b>	<b>Mitjà</b>	<b>Alt</b>
<b>Bàsic</b>	Funcions i obligacions del personal Registre d'incidències Control d'accés Gestió de suports i documents Identificació i autenticació Còpies de suport i recuperació Arxiu: garantir-ne la conservació Arxiu: localització i consulta Arxiu: exercici de drets Dificultar l'accés al dispositiu que conté documents Evitar l'accés a persones no autoritzades (si no és possible l'anterior) Custòdia dels documents per part del personal.	(a) / (na) (a) / (na) (a) / (na) (a) / (na) (a) (a) (na) (na) (na) (na) (na) (na)		
<b>Mitjà</b>	Responsable de seguretat Auditoria Registre d'entrada i sortida de suports Limitació dels intents d'accés no autoritzat Control d'accés físic Registrar procediments de recuperació com a incidents		(a) / (na) (a) / (na) (a) (a) (a) (a)	
<b>Alt</b>	Identificació de suports codificada Xifrat de suports durant el transport o protecció de documentació Xifrat de dispositius portàtils Evitar concurrència de riscos en còpies i procediments de recuperació Registre d'accessos a la informació o documentació Xifrat de les telecomunicacions (xarxes públiques / sense fil) Dispositius d'emmagatzemament en zones tancades Control de còpia o reproducció dels documents Destrucció de les còpies sense utilitat.			(a) (a) / (na) (a) (a) (a) / (na) (a) (na) (na) (na)

Font: Escola d'Administració Pública de Catalunya

# Mesures de seguretat de nivell bàsic

## *Per a tots els tractaments*

- a) **Control d'accés** (articles 91 i 105.2): hem de tenir una llista actualitzada de qui té autorització per usar les dades, en la qual s'indiqui què pot fer cada usuari (consultar, fer llistats, modificar, suprimir, etc. ); això implica que hi ha d'haver un control d'accés a les dades que permeti gestionar aquests permisos. Cada usuari ha d'estar autoritzat només a accedir a aquella informació necessària per al desenvolupament de les seves funcions. Vegeu: "[consultas ilegales](#)". El Punt Neutre Judicial és una xarxa de Serveis que ofereix als òrgans judicials les dades necessàries en la tramitació judicial mitjançant accessos directes a aplicacions i bases de dades del propi Consell, d'organismes de l'Administració General de l'Estat i d'Altres Institucions amb objectiu de facilitar i reduir els temps de tramitació, d'augmentar la seguretat, i de Millorar la Satisfacció dels usuaris. Després de detectar que prop del 50% de les consultes que els funcionaris de justícia realitzaven a les bases de dades a les que tenen accés són per tafanejar informació confidencial sobre les seves ex parelles, familiars o amics, es va fer una Circular reguladora de l'accés.
- b) **Gestió de suports i documents** (articles 92 i 105.2): Si cal fer una còpia de les dades ubicades en un sistema informàtic, per exemple si les volem copiar en un CD/DVD o en una memòria USB, disc dur extern o ordinador portàtil, cal que etiquetem el suport que contindrà les dades; d'aquesta manera, podrem saber que allà hi ha dades personals emmagatzemades. Òbviament, aquest suport extern també s'haurà de protegir de l'accés de tercers no autoritzats.
- c) **Registre d'incidències** (articles 90 i 105.2)
- d) **Treball fora dels locals o ubicacions habituals de tractament** (article 86): si volem treure les dades fora dels locals del responsable del fitxer, per exemple en algun dels suports relacionats en el control d'accés, o simplement lliurar-les annexades a un correu electrònic, cal que aquesta sortida d'informació estigui autoritzada.

## *Per als tractaments automatitzats*

- a) **Identificació i autenticació** (article 93): el responsable del fitxer o tractament ha d'establir els mecanismes necessaris per garantir la identificació i autenticació inequívoca i personalitzada dels usuaris (veure definicions a l'apartat 7.3.1). Les contrasenyes s'han de proporcionar i emmagatzemar de manera que quedi garantida la seva confidencialitat i integritat; amb una periodicitat no superior a un any les contrasenyes han de ser modificades.
- b) **Còpies de suport i recuperació** (article 94): cal fer còpies de seguretat, per si l'ordinador en el qual tenim les dades es veu afectat per una avaria o un mal funcionament que impedeixi accedir a les dades, o que aquestes quedin en un estat tal que resultin inservibles.

## *Per als tractaments no automatitzats*

- a) **Dificultar l'accés al dispositiu que conté documents** (article 107): l'accés als arxius, armaris, calaixos, etc. on es guardin documents s'ha de realitzar mitjançant algun mecanisme que obstaculitzi el lliure accés (panys o similars)

## Recordeu que...

- a) Les dades de caràcter personal són de les persones i no de l'entitat o empresa que les utilitza.
- b) Abans de recollir dades, comproveu que el fitxer està creat i registrat.
- c) Sempre doneu el dret d'informació, i demaneu el consentiment quan calgui.
- d) Sol·liciteu només dades que siguin adequades, pertinents i no excessives per a finalitats concretes, i actualitzeu-les.
- e) Faciliteu l'exercici de drets "ARCO" als titulars de les dades.
- f) No cediu dades sense comprovar que ho podeu fer.
- g) Doneu compliment al deure de secret.
- h) Cas que contracteu serveis a empreses que impliqui el tractament de dades, reviseu els contractes. Recordeu l'article 12 LOPD.
- i) Adopteu les mesures de seguretat adequades.



# Moltes gràcies

Contacte: [protecciodedades@ub.edu](mailto:protecciodedades@ub.edu)

Pàgina web: <http://bit.ly/xNkkQo>