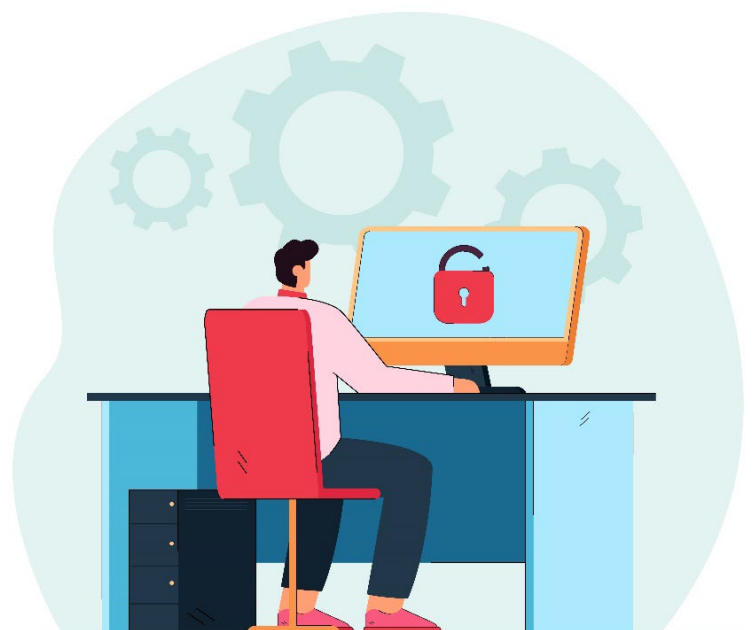


Guia de protecció de dades per als col·legis professionals i consells de col·legis

Actualització: juny 2024

Col·lecció guies. Núm. 6



© Barcelona, 2022

El contingut d'aquest informe és titularitat de l'Autoritat Catalana de Protecció de Dades i resta subjecte a la llicència de Creative Commons BY-NC-ND.

L'autoria de l'obra es reconeixerà a través de la inclusió de la menció següent:

Obra titularitat de l'Autoritat Catalana de Protecció de Dades.

Llicenciada sota la llicència CC BY-NC-ND.



La llicència presenta les particularitats següents:

Es permet lliurement:

Copiar, distribuir i comunicar públicament l'obra, sota les condicions següents:

- **Reconeixement:** S'ha de reconèixer l'autoria de l'obra de la manera especificada per l'autor o el llicenciador (en tot cas, no de manera que suggereixi que gaudeix del suport o que dona suport a la seva obra).
- **No comercial:** No es pot emprar aquesta obra per a finalitats comercials o promocionals.
- **Sense obres derivades:** No es pot alterar, transformar o generar una obra derivada a partir d'aquesta obra.

Avís: En reutilitzar o distribuir l'obra, cal que s'esmentin clarament els termes de la llicència d'aquesta obra.

El text complet de la llicència es pot consultar a

<https://creativecommons.org/licenses/by-nc-nd/4.0/deed.ca>.

Índex

Índex.....	2
Presentació.....	5
1. Marc normatiu	6
2. Conceptes clau	7
3. El tractament de dades als col·legis professionals	10
4. Les finalitats del tractament.....	13
5. La licitud del tractament	14
5.1 Les bases jurídiques del tractament.....	15
5.1.1 El consentiment de la persona afectada	16
5.1.2 L'execució d'un contracte.....	19
5.1.3 El compliment d'una obligació legal	20
5.1.4 La protecció d'interessos vitals	20
5.1.5 El compliment d'una missió d'interès públic o en l'exercici de poders públics	20
5.1.6 La satisfacció d'un interès legítim	21
5.2 Les categories especials de dades.....	22
5.3 Les comunicacions de dades	25
5.3.1 Accés de tercers a dades personals de les persones col·legiades a través de la finestra única	27
5.3.2 Accés dels candidats en un procés electoral a les dades de col·legiats.....	29
5.3.3 Comunicació de sancions disciplinàries, inhabilitacions i incompatibilitats	30
5.3.4 Comunicacions de dades a administracions públiques, a altres col·legis i als consells de col·legis.....	31
5.3.5 Comunicació de dades a cossos policials	33
5.4 Disposicions aplicables a tractaments específics	34
5.4.1 Tractament de dades relatives a infraccions i sancions administratives	34
5.4.2 Tractament de dades del personal dels col·legis professionals	35
5.4.2.1 Dades de contacte professional del personal del col·legi.....	35
5.4.2.2 Videovigilància en l'àmbit laboral.....	35
5.4.2.3 Ús de dispositius digitals	37
5.4.3 Tractament de dades de contacte de persones al servei de persones jurídiques, d'empresaris individuals i de professionals liberals	38

5.4.4 Tractament amb fins de videovigilància	39
5.4.5 Sistemes interns de denúncies	40
5.4.6 Tractament de dades amb finalitats estadístiques.....	41
6. Obligacions del responsable del tractament abans d'iniciar el tractament	42
6.1 La proporcionalitat del tractament; el principi de minimització	43
6.2 La protecció de dades des del disseny i per defecte	44
6.3 L'anàlisi de riscos	45
6.4 L'avaluació d'impacte i la consulta prèvia.....	47
6.5 El registre i l'inventari d'activitats del tractament.....	51
7. Obligacions del responsable del tractament i de l'encarregat durant el tractament	53
7.1 La informació a les persones afectades	54
7.2 L'atenció dels drets de les persones afectades	58
7.2.1 Aspectes comuns.....	58
7.2.2 Dret d'accés.....	61
7.2.3 Dret de rectificació	63
7.2.4 Dret de supressió.....	64
7.2.5 Dret a la limitació del tractament.....	65
7.2.6 Dret a la portabilitat.....	66
7.2.7 Dret d'oposició	67
7.2.8 Dret a no ser objecte de decisions automatitzades	68
7.3. L'exactitud i l'actualització de les dades	69
7.4 L'encàrrec del tractament	71
7.4.1 La figura de l'encarregat del tractament.....	71
7.4.2 Formalització de l'encàrrec	72
7.4.3 Obligacions de l'encarregat del tractament	73
7.4.4 Subcontractació	74
7.4.5 Responsabilitat	74
7.5 El delegat de protecció de dades	76
7.6 Les transferències internacionals de dades.....	78
7.7 La seguretat de les dades: integritat i confidencialitat.....	81
7.7.1 El deure de confidencialitat	81
7.7.2 La integritat de les dades	82

7.7.3 La disponibilitat de les dades	83
7.7.4 L'anàlisi de riscos.....	83
7.7.5 Les mesures de seguretat.....	84
7.7.6 La gestió dels incidents de seguretat	85
7.8 La política de protecció de dades	88
7.9 L'adopció d'altres mesures proactives	89
7.9.1 Els codis de conducta	90
7.9.2 Les certificacions, segells i marques	91
8. Obligacions del responsable un cop finalitza el tractament; la conservació de les dades.	92
8.1 Limitació del termini de conservació	92
8.2 El deure de bloqueig	94
9. Règim de responsabilitat.....	95
9.1 Reclamacions davant l'Autoritat Catalana de Protecció de Dades.....	95
9.2. Reclamacions davant els òrgans jurisdiccionals	98
9.3. Indemnització per danys i perjudicis	99
10. Autoritat de control: l'Autoritat Catalana de Protecció de Dades.	99
10.1 Naturalesa i objecte.....	99
10.2 Àmbit d'actuació	100
10.3 Organització	101
10.4 Funcions i potestats.....	101
Abreviatures	105
Annexos.....	107

Presentació

L'Autoritat Catalana de Protecció de Dades, en el marc del Conveni de col·laboració amb l'Associació Intercol·legial, ha elaborat aquesta Guia de protecció de dades per als col·legis professionals i els consells de col·legis recollint els canvis normatius produïts arran la plena aplicació, a partir del dia 25 de maig de 2018, del Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades (RGPD)) i la posterior aprovació de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.

L'RGPD obliga tant els responsables del tractament com les autoritats de protecció de dades a ser proactius en la seva actuació a l'hora de garantir el tractament adequat de les dades personals. Per això, aquesta guia pretén oferir una visió àmplia de la normativa de protecció de dades que permet no només donar solució als problemes més freqüents amb que es trobin els col·legis professionals, sinó també detectar-los i donar-hi solució abans que es produeixin.

L'objecte d'aquesta guia no és substituir els textos normatius d'aplicació, que són els que en qualsevol cas determinen de manera detallada el contingut de les obligacions del responsable del tractament, sinó recollir d'una manera general, sistematitzada i entenedora els aspectes més rellevants a l'hora de tractar dades personals. També oferir criteris orientadors que els col·legis professionals han de tenir en compte en la seva actuació diària, per tal d'adequar-la al que estableix la normativa de protecció de dades personals.

Per fer-ho, en cadascun dels apartats de la Guia es recull en primer lloc un resum dels aspectes més rellevants de la normativa aplicable, que es complementa amb un seguit de preguntes i respostes freqüents, amb indicació de la normativa aplicable més rellevant en cada apartat. Tot i que, per simplificar la lectura en aquesta guia sovint es farà referència només als col·legis professionals, les consideracions que conté són extensibles als consells de col·legis professionals.

Espero que us sigui una eina útil per garantir de manera efectiva els drets i les llibertats de les persones afectades.

Meritxell Borràs i Solé
Directora

1. Marc normatiu

- Reglament (UE) núm. 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE.
- Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.
- Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.¹
- Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.²
- 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 l'Agència Catalana de Protecció de Dades, de 10 de febrer de 2009, sobre el tractament de dades de caràcter personal mitjançant càmeres amb fins de videovigilància.²
- Recomanació 1/2008 de l'Autoritat Catalana de Protecció de Dades sobre la difusió d'informació que contingui dades de caràcter personal a través d'Internet.

També convé tenir en compte les següents guies publicades per l'APDCAT:

- [Guia per al compliment del deure d'informar a l'RGPD](#)
- [Guia sobre l'encarregat del tractament a l'RGPD](#)
- [Guia pràctica sobre l'avaluació d'impacte relativa a la protecció de dades](#)
- [Orientació per a l'aplicació provisional de la disposició addicional setena de l'LOPDGDD \(publicació del núm. de DNI\)](#)
- [Llista de tipus d'operacions de tractament que s'han de sotmetre a AIPD](#)

¹ Els articles 23 i 24 continuen essent aplicables en l'àmbit de l'RGPD.

² Aplicable en allò que no sigui contrari a l'RGPD i l'LOPDGDD.

2. Conceptes clau

Afectat: persona física titular de les dades personals sotmeses a tractament.

En aquesta guia s'empra el terme persona afectada i no interessat, que empra l'RGPD, per tal d'evitar confondre'l amb el concepte d'interessat que regula la normativa del procediment administratiu.

Anonimització: tractament de dades que produeix la ruptura de la cadena d'identificació de la persona afectada, de manera que les dades ja no es puguin atribuir a una persona física identificada o identificable.

Categories especials de dades: dades personals que, per la seva naturalesa, reben una protecció especial atès el seu caràcter sensible en relació amb els drets i llibertats fonamentals dels afectats i els riscos que es poden derivar del seu tractament.

En formen part:

- Les opinions polítiques.
- Les conviccions religioses o filosòfiques.
- L'afiliació sindical.
- Les dades que revelen l'origen ètnic o racial.
- Les dades genètiques.
- Les dades biomètriques destinades a identificar de manera unívoca una persona física.
- Les dades relatives a la salut.
- Les dades relatives a la vida sexual o a l'orientació sexual d'una persona física.

Les dades relatives a infraccions i condemnes penals i les relatives a infraccions i sancions administratives no es consideren categories especials de dades, tot i que ambdues categories compten amb un règim específic que introdueix algunes restriccions al seu tractament.

Dades personals: qualsevol informació sobre una persona física identificada o identificable. En conseqüència, la normativa de protecció de dades no afectarà la informació relativa a persones jurídiques o quan és anònima, és a dir, quan no es pot relacionar amb una persona física.

La protecció de dades personals abasta tots els aspectes de la vida d'una persona física. Per això, per exemple, en el cas dels professionals liberals o dels empresaris individuals pot abastar també aspectes de la seva vida professional.

Es considera **persona identificable** la persona que pot ser identificada directament o indirectament, en particular mitjançant un identificador, com per exemple un nom, un número d'identificació, dades de localització, un identificador en línia o un o diversos elements propis

de la identitat física, fisiològica, genètica, psíquica, econòmica, cultural o social d'aquesta persona.

La normativa de protecció de dades personals no s'aplica a les dades de les persones difuntes.

Destinatari: persona física o jurídica, autoritat pública, servei o qualsevol altre organisme al qual es comuniquen dades personals, tant si és un tercer com si no.

No es consideren destinataris els encarregats del tractament, ni les autoritats públiques que poden rebre dades personals en el marc d'una investigació concreta.

Tampoc el personal propi dels col·legis professionals, quan accedeix a les dades personals en exercici o desenvolupament de les seves funcions.

Elaboració de perfils: qualsevol forma de tractament automatitzat de dades personals consistent en l'ús de les dades per avaluar determinats aspectes d'una persona física; en especial, per analitzar o predir aspectes relatius al rendiment professional, la situació econòmica, la salut, les preferències personals, els interessos, la fiabilitat, el comportament, la ubicació o els moviments d'aquesta persona

Encarregat del tractament: persona física o jurídica, autoritat pública, servei o qualsevol altre organisme que tracta dades personals per compte del responsable del tractament.

Fonts accessibles al públic: actualment la normativa de protecció de dades no conté una definició de què s'ha d'entendre com a font accessible al públic, ni estableix cap règim específic pel que fa al tractament de les dades que poden contenir. Es pot considerar com a font d'accés públic, qualsevol conjunt d'informació que és de lliure accés per a la ciutadania.

Responsable del tractament: persona física o jurídica, autoritat pública, servei o qualsevol altre organisme que, sol o juntament amb d'altres, determina les finalitats i els mitjans del tractament.

Poden ser responsables dels respectius tractaments els col·legis professionals, qualsevol dels seus òrgans o ens instrumentals o entitats sense personalitat jurídica que actuïn en el tràfic jurídic com a subjecte diferenciat.

Pot haver-hi més d'un responsable del tractament. En aquest cas, les responsabilitats de cadascun s'han de determinar en un acord establert a aquest efecte, atenent a les activitats que efectivament duu a terme cadascun dels **corresponsables** del tractament.

Pseudonimització: tractament de les dades personals de manera que ja no es puguin atribuir a un afectat sense utilitzar informació addicional, sempre que aquesta informació consti per separat i estigui subjecta a mesures tècniques i organitzatives destinades a garantir que les dades personals no s'atribueixen a una persona física identificada o identificable.

Les dades personals **pseudonimitzades**, que es poden atribuir a una persona física utilitzant informació addicional, com per exemple un codi, es consideren informació sobre una persona física identificable.

Tercer: persona física o jurídica, autoritat pública, servei o organisme diferent de la persona afectada, del responsable del tractament, de l'encarregat del tractament i de les persones autoritzades per tractar les dades personals sota l'autoritat directa del responsable o de l'encarregat.

Tractament: qualsevol operació o conjunt d'operacions realitzades sobre dades personals o conjunts de dades personals, ja sigui per procediments automatitzats o no, com la recollida, el registre, l'organització, l'estructuració, la conservació, l'adaptació o la modificació, l'extracció, la consulta, la utilització, la comunicació per transmissió, difusió o qualsevol altra forma d'habilitació d'accés, acarament o interconnexió, limitació, supressió o destrucció.



El tractament de les dades relatives a les societats professionals del col·legi està dins l'àmbit d'aplicació de la normativa de protecció de dades?

L'RGPD i l'LOPDGDD només són d'aplicació a les dades de persones físiques. Per tant, no ho seria respecte de les dades d'una societat professional. Ara bé, les societats professionals estan formades o gestionades per persones físiques (sòcies, representants, administradores, etc.), respecte de les quals sí que són d'aplicació l'RGPD i l'LOPDGDD.

Una adreça de correu electrònic facilitada pel col·legi a una persona col·legiada és una dada personal?

Els col·legis professionals poden adoptar diferents criteris en la confecció de les adreces de correu electrònic que faciliten als seus col·legiats (adreces personalitzades, no personalitzades o adreces genèriques). Si l'adreça de correu electrònic es pot associar directament o indirecta a una persona física, és una dada personal, el tractament de la qual s'ha d'adequar als principis i les garanties de la normativa de protecció de dades.

Normativa aplicable: arts. 4, 9, 10 i 26 RGPD; 10 i 27 LOPDGDD.

3. El tractament de dades als col·legis professionals

En exercici de les funcions que tenen encomanades, els col·legis professionals i els consells de col·legis professionals han de tractar com a responsables del tractament nombroses dades personals de diferents col·lectius, com ara les de les persones col·legiades, del personal del col·legi, dels proveïdors, de les persones assistents a activitats o altres persones amb les quals es relacionen. Aquestes dades poden ser de diferents tipologies (identificatives, de característiques personals, de formació, professionals, econòmiques, de menors, etc.).

En el cas dels col·legis professionals és important tenir en compte que, en alguns aspectes previstos a la normativa de protecció de dades, el règim aplicable pot dependre de si el col·legi està actuant en exercici de funcions públiques o funcions privades. Això serà rellevant, per exemple, a l'hora de determinar la base jurídica (consentiment, missió en interès públic, interès legítim, etc.); l'obligació d'incorporar un tractament a l'inventari d'activitats de tractament; la possibilitat d'exercir el dret a la portabilitat; l'exigibilitat de l'aplicació de l'Esquema nacional de seguretat; el règim sancionador aplicable; etc.

La normativa reguladora dels col·legis professionals determina que són **funcions públiques** dels col·legis professionals les següents:

- Garantir que l'exercici professional s'adeqüi a la normativa, la deontologia i les bones pràctiques i que es respectin els drets i els interessos de les persones destinatàries de l'actuació professional.
- Vetllar pels drets i pel compliment dels deures i les obligacions dels col·legiats i perquè no es produeixin actes d'intrusisme, de competència deslleial o altres actuacions irregulars.
- Exercir la potestat disciplinària sobre els seus col·legiats, en els termes establerts per la llei i les normes pròpies dels col·legis professionals.
- Visar els projectes i els treballs de les persones col·legiades, en els termes i amb els efectes que estableix la normativa corresponent.
- Participar en el procediment d'obtenció de l'acreditació d'aptitud per exercir la professió col·legiada, si la llei estableix aquest requisit.
- Promoure i facilitar la formació contínua de les persones col·legiades que permeti garantir la seva competència professional.
- Adoptar les mesures necessàries per facilitar l'exercici professional no permanent, en compliment del que estableixen la normativa de la Unió Europea i les lleis.
- Col·laborar amb l'Administració pública mitjançant la participació en òrgans administratius, quan així es prevegi legalment, i emetre els informes que els òrgans o autoritats administratius i judicials els requereixin.
- Informar sobre els projectes de disposicions generals que afectin l'exercici de la professió o la institució col·legial.

- Fomentar l'ús de la llengua catalana entre les persones col·legiades i en els àmbits institucionals i socials en els quals s'exerceix la professió.
- Informar en els processos judicials i administratius en els quals es discuteixin qüestions relatives a honoraris i aranzels professionals.
- Aprovar els seus pressupostos i regular i fixar les aportacions dels col·legiats.
- Les altres funcions de naturalesa pública que els atribueix la legislació vigent o que els hagi delegat una administració pública.

En canvi, són **activitats privades** dels col·legis professionals:

- Fomentar i prestar serveis en interès de les persones col·legiades i de la professió en general.
- Gestionar el cobrament de les remuneracions i dels honoraris professionals a petició de les persones col·legiades, d'acord amb el que estableixen els estatuts respectius.
- Intervenir, per via de mediació o d'arbitratge, en els conflictes professionals entre persones col·legiades o entre aquestes i terceres persones, sempre que ho sol·licitin de comú acord les parts implicades.
- Col·laborar amb les associacions i altres entitats representatives dels interessos dels ciutadans directament vinculades amb l'exercici de la professió col·legiada.
- Facilitar informació en matèria d'honoraris professionals, respectant sempre el règim de lliure competència.
- Custodiar, a petició del professional o la professional i d'acord amb els estatuts, documentació pròpia de la seva activitat que es vegin obligats a guardar de conformitat amb la normativa vigent.
- Altres no vinculades a l'exercici de potestats públiques.

A l'hora de tractar les dades, els col·legis professionals han de tenir en compte els principis que estableix la normativa de protecció de dades, i que s'exposen amb més detall en els apartats següents d'aquesta guia:

- **Principis de licitud, lleialtat i transparència:** les dades s'han de tractar de manera lícita, lleial i transparent en relació amb la persona afectada.
- **Principi de limitació de la finalitat:** les dades s'han de recollir amb finalitats determinades, explícites i legítimes i posteriorment no s'han de tractar de manera incompatible amb aquestes finalitats.
- **Principi de minimització de dades:** les dades han de ser adequades, pertinents i limitades al que és necessari en relació amb les finalitats per a les quals es tracten.
- **Principi d'exactitud:** les dades han de ser exactes i, si cal, actualitzades.
- **Principi de limitació del termini de conservació:** les dades s'han de conservar només durant el període necessari per a les finalitats del tractament.
- **Principi d'integritat i confidencialitat:** les dades s'han de tractar de manera que se'n garanteixi una seguretat adequada, inclosa la protecció contra el tractament no

autoritzat o il·lícit i contra la seva pèrdua, destrucció o dany accidental, mitjançant l'aplicació de les mesures tècniques o organitzatives adequades.

- **Principi de responsabilitat proactiva** (*accountability*): el responsable del tractament és responsable del compliment d'aquests principis i ha de ser capaç de demostrar-ho.

D'acord amb aquests principis, els col·legis professionals han de tenir en compte un seguit d'elements per garantir que el tractament es duu a terme en condicions adequades:

Primer: concretar la finalitat del tractament.

Segon: identificar la base jurídica del tractament.

Tercer: tractar i emprar únicament les dades necessàries per assolir la finalitat.

Quart: establir garanties adequades en la prestació de serveis per compte del col·legi professional que impliquin el tractament de dades personals.

Cinquè: atendre els drets de les persones afectades.

Sisè: complir les obligacions que preveu l'RGPD. Això inclou l'obligació del responsable del tractament d'aplicar les mesures tècniques i organitzatives adequades per garantir i poder demostrar que el tractament és conforme a la normativa de protecció de dades, tenint en compte la naturalesa, l'àmbit, el context i les finalitats del tractament, així com els riscos de probabilitat i gravetat diversa per als drets i les llibertats de les persones físiques.

Inclou, com a mínim, les obligacions següents:

- Facilitar informació sobre el tractament de les dades a les persones afectades.
- Portar el registre i l'inventari d'activitats del tractament.
- Designar un delegat de protecció de dades.
- Aplicar la protecció de dades des del disseny i per defecte.
- Vetllar per l'exactitud i l'actualització de les dades.
- Vetllar per la seguretat de les dades: integritat i confidencialitat.
- Fer l'avaluació d'impacte relativa a la protecció de dades i la consulta prèvia, si escau.
- Aprovar una política de protecció de dades, si escau.

Aquestes mesures s'han de revisar i actualitzar quan calgui.

Setè: adoptar altres mesures proactives per garantir els drets i llibertats de les persones afectades, si escau.

Vuitè: vetllar perquè s'ofereixin garanties adequades en les transferències internacionals de dades.

Novè: vetllar per la conservació adequada de les dades.

És important que el col·legi professional, com a responsable del tractament, estigui en disposició de poder demostrar que s'han adoptat mesures per garantir les condicions adequades dels tractaments, ja sigui a través de protocols, procediments, instruccions internes, documentació, registres, activitats de formació, comunicacions etc. És el que es coneix com responsabilitat proactiva o *accountability*. En els apartats següents d'aquesta guia s'ofereixen orientacions bàsiques per complir aquests aspectes.



Com es pot determinar si la finalitat d'un tractament està vinculada a l'exercici de funcions públiques?

Cal veure si la finalitat es pot incloure dins d'alguna de les funcions públiques que els atribueix la normativa reguladora dels col·legis professionals (Llei 7/2006) o altra normativa. Per altra banda, la jurisprudència també ha reconegut que hi ha diferents activitats dels col·legis que s'han de considerar funcions públiques, com ara les qüestions relatives a la defensa de la corporació, la constitució dels seus òrgans, el seu règim electoral o les decisions sobre col·legiació i disciplina, l'aprovació dels seus pressupostos o també les qüestions relatives als visats col·legials.

I en el cas dels tractaments de dades que fan els consells de col·legis?

Com en el cas dels col·legis professionals, cal veure si la finalitat es pot incloure dins d'alguna de les funcions públiques que els atribueix la normativa reguladora dels col·legis professionals (Llei 7/2006) o altra normativa.

Quina naturalesa té el tractament de dades de precol·legiats?

Pot considerar-se de naturalesa pública, en la mesura que les dades personals que s'hi incorporen es recullen amb vista al procediment d'incorporació al col·legi com a col·legiats. Altrament, si la finalitat del tractament es refereix a activitats que no estan regulades com a funcions públiques del col·legi, s'ha de considerar de naturalesa privada.

4. Les finalitats del tractament

Les dades personals s'han de recollir amb finalitats determinades, explícites i legítimes, i no es poden tractar posteriorment de manera incompatible amb les finalitats inicials per a les quals es van recollir. Per això, és important que abans d'iniciar la recollida, el responsable del tractament estableixi clarament la finalitat i la faci constar tant al registre d'activitats del tractament, com a la informació que ha de facilitar a les persones afectades.

Es consideren compatibles els tractaments de les dades amb finalitats d'arxiu en interès públic, de recerca científica i històrica o amb finalitats estadístiques. No obstant això, caldrà adoptar garanties adequades per a les persones afectades i, en particular, garantir el respecte al principi de minimització. Per complir aquest principi es poden utilitzar mesures com la pseudonimització o fins i tot l'anonimització, sempre que aquestes mesures permetin assolir la finalitat del tractament. En els tractaments que es facin amb aquestes finalitats, la llei pot establir excepcions als drets de les persones afectades.

Una nova finalitat (finalitat posterior o secundària) també es pot considerar compatible quan el nou tractament es basa en el consentiment de les persones afectades o en el dret de la Unió o d'un estat membre amb algun dels objectius que recull l'article 23 de l'RGPD (seguretat de l'estat, defensa, seguretat pública, prevenció, investigació, detecció o enjudiciament d'infraccions penals o deontològiques, execució de sancions penals, objectius importats d'interès públic, protecció de la persona afectada o dels drets i llibertats d'altres, o execució de demandes civils).

Més enllà d'aquests supòsits, el responsable del tractament pot determinar que l'ús de les dades amb una finalitat secundària és compatible amb la finalitat inicial, tenint en compte, entre d'altres, les circumstàncies següents:

- La relació entre les finalitats inicials i les posteriors.
- El context en què s'han recollit les dades, en particular pel que fa a la relació entre les persones afectades i el responsable.
- La naturalesa de les dades personals, en concret si es tracta de categories especials de dades o de dades relatives a condemnes i infraccions penals.
- Les conseqüències del tractament posterior per a les persones afectades.
- L'existència de garanties adequades, com el xifratge o la pseudonimització.

En aquests casos, cal informar les persones afectades de la nova finalitat o finalitat secundària. També de la resta d'aspectes previstos a l'RGPD, llevat que ja se l'hagi informat prèviament.

Normativa aplicable: considerant 50, arts. 5.1.b), 6.4, 13.3 i 89.1 RGPD.

5. La licitud del tractament

L'RGPD estableix que tot tractament de dades personals ha de ser lícit. Això vol dir que, a més de respectar les lleis, com qualsevol altra activitat dels col·legis professionals, només es pot dur a terme si es fonamenta en alguna de les bases jurídiques que estableix l'article 6.1 del mateix RGPD.

Aquestes bases jurídiques no mantenen entre sí cap relació de prioritat o prelación i un mateix tractament pot comptar amb més d'una base jurídica.

L'elecció de la base jurídica del tractament s'ha de fer sempre abans de començar les operacions de tractament, tenint en compte la seva finalitat, i s'ha d'incloure a la informació que es facilita a la persona afectada.

En el cas dels col·legis professionals, quan exerceixin funcions públiques, normalment la base jurídica serà l'exercici d'una missió en interès públic o l'exercici de potestats públiques. De vegades també pot ser, per exemple, el compliment d'una obligació legal o l'execució d'un contracte.

El consentiment de les persones afectades, si bé no es pot descartar amb caràcter general, serà un supòsit poc habitual, tenint en compte que la situació de desigualtat existent, si més no quan s'exerceixen funcions públiques, entre la posició jurídica del col·legi professional i la de la ciutadania o la persona col·legiada que s'hi relaciona, que pot condicionar el caràcter lliure del consentiment.

Quan exerceixin funcions privades, l'habilitació basada en el consentiment pot tenir un paper més important. En aquestes funcions, també cal tenir en compte l'habilitació derivada de la consecució d'un interès legítim.

En el cas de les categories especials de dades, el seu tractament està prohibit amb caràcter general, llevat que, a més d'una de les bases jurídiques de l'article 6.1, concorri alguna de les excepcions de l'article 9.2 de l'RGPD.

5.1 Les bases jurídiques del tractament

Per al compliment del principi de licitud, l'RGPD preveu diferents bases jurídiques en les quals es pot basar la legitimitat del tractament:

- El consentiment de la persona afectada.
- El tractament és necessari per executar un contracte en el qual la persona afectada és part, o bé per aplicar mesures precontractuals a petició seva.
- El tractament és necessari per complir una obligació legal aplicable al responsable del tractament.
- El tractament és necessari per protegir interessos vitals de la persona afectada o d'una altra persona física.
- El tractament és necessari per complir una missió realitzada en interès públic o en l'exercici de poders públics conferits al responsable del tractament.
- El tractament és necessari per satisfer interessos legítims perseguits pel responsable del tractament o per un tercer, sempre que no prevalguin els interessos o els drets i les llibertats fonamentals de la persona afectada.



Un col·legi professional pot tractar dades personals recollides de pàgines web de tercers (números de telèfon, adreces electròniques personals, noms i cognoms, etc.)?

No, llevat que es compti amb alguna de les bases jurídiques previstes a l'RGPD.

5.1.1 El consentiment de la persona afectada

El consentiment constitueix una de les sis bases jurídiques establertes a l'RGPD en què el responsable pot fonamentar el tractament de dades personals.

El consentiment només és una base jurídica adequada si reuneix els requisits establerts en la normativa de protecció de dades. En concret, el consentiment de la persona afectada ha de ser:

Informat. Abans que la persona afectada atorgui el consentiment, cal facilitar-li la informació suficient perquè compregui què està consentint realment.

En aquest sentit, té especial importància la informació sobre la identitat del responsable i les finalitats del tractament, sens perjudici dels altres aspectes als quals ens referirem en l'apartat relatiu a la informació a les persones afectades.

Lliure. La persona afectada ha de disposar d'una capacitat d'elecció i control real, de manera que si decideix no donar el consentiment o retirar-lo, no se'n derivin conseqüències negatives o perjudicis de cap mena.

No es pot considerar que el consentiment ha estat prestat lliurement quan:

- Hi ha un desequilibri evident entre la persona afectada i el responsable del tractament, en particular quan aquest responsable és una autoritat pública. Els col·legis professionals han de tenir-ho especialment en compte quan exerceixen funcions de caràcter públic.
- No permet autoritzar per separat les diferents operacions de tractament de dades, tot i ser adequat en el cas concret.
- L'execució d'un contracte se supedita al consentiment per tractar dades que no són necessàries per al contracte esmentat.

Amb caràcter general, el consentiment no és vàlid si s'exerceix qualsevol influència o pressió inadequada sobre la persona afectada que li impedeixi actuar lliurement d'acord amb la seva voluntat.

Aquestes influències o pressions inadequades poden manifestar-se de formes molt diverses, segons el context i les característiques pròpies del tractament de dades.

Específic. El consentiment es pot requerir per a totes les activitats de tractament que responen a una mateixa finalitat concreta i determinada.

Si el tractament té diverses finalitats, el consentiment s'ha de requerir de manera separada per a cadascuna (consentiment granular).

Inequívoc. La persona afectada ha d'atorgar el seu consentiment mitjançant un acte afirmatiu clar o una manifestació de voluntat d'acceptar el tractament de dades que l'afecten.

A més d'inequívoc, el consentiment ha de ser **explícit** en els supòsits següents:

- Tractament de categories especials de dades.
- Presa de decisions individuals automatitzades.
- Transferències internacionals de dades.

L'anomenat consentiment "tàcit", basat en la inacció de la persona afectada o en l'ús de caselles premarcades, no és admissible.

En canvi, sí que és conforme a l'RGPD la utilització d'una declaració per escrit o la marcadó de caselles en un lloc web.

Si s'empra una declaració escrita que també faci referència a altres assumptes, la part referent a la protecció de dades ha de quedar clarament diferenciada de la resta de declaracions.

La persona afectada té dret a retirar el consentiment en qualsevol moment, de la mateixa manera, o més senzilla, que la fórmula emprada per donar-lo, sense que això afecti la licitud del tractament previ a la revocació basat en el consentiment.

Correspon al responsable demostrar en tot moment que la persona afectada ha atorgat el consentiment i que aquest és vàlid.

Els tractaments de dades iniciats pels col·legis professionals abans de l'aplicació de l'RGPD basats en el consentiment de la persona afectada continuen essent lícits si el consentiment es va prestar amb els requisits que estableix l'RGPD. En especial convé revisar si es va prestar mitjançant una manifestació o acció afirmativa clara.

El consentiment dels menors d'edat

Si la persona afectada és menor d'edat, cal tenir present que el tractament de les seves dades només es pot fonamentar en el seu consentiment si té més de 14 anys. Això, llevat que es tracti de supòsits en què una llei exigeixi l'assistència del titular de la potestat parental o tutela per dur a terme l'acte o el negoci jurídic en el context del qual se sol·licita el consentiment.

En aquest cas, cal explicar en un llenguatge clar i senzill per als menors d'edat de quina manera es tractaran les dades personals

En cas de menors d'edat de menys de 14 anys, el tractament de dades fonamentat en el consentiment requereix el consentiment del titular de la potestat parental o tutela.



Els col·legis professionals poden emprar el consentiment com a base jurídica dels tractaments de dades que duen a terme?

És possible, tot i que normalment el consentiment no és la base jurídica en la qual es poden emprar els tractaments de dades fets en l'exercici de funcions públiques dels col·legis professionals. En l'àmbit de les administracions públiques, quan actuen en exercici de les seves competències, el ciutadà no sempre està en condicions de poder negar el seu consentiment d'una manera lliure. Per això, normalment la base jurídica és la relativa al compliment d'una missió d'interès públic o l'exercici de poders públics.

En canvi, en les seves funcions privades la poden emprar normalment. Alguns exemples en què podria operar el consentiment serien la subscripció a un servei ofert pel col·legi, com una activitat lúdica, la subscripció a la seva pàgina web per rebre comunicacions sobre determinats productes, o la inscripció a una borsa de treball, entre d'altres.

Com pot provar el responsable del tractament el consentiment de la persona afectada a un tractament específic?

L'RGPD estableix l'obligació explícita del responsable de demostrar que la persona afectada ha donat el seu consentiment, però no prescriu com s'ha de fer. Així els responsables del tractament tenen llibertat per escollir el mitjà que permeti complir amb aquesta obligació. En aquest sentit, cal tenir en compte les Directrius 5/2020 sobre el consentiment en el sentit del Reglament (UE) 2016/679 del Comitè Europeu de Protecció de dades (CEPD), adoptades el 4 de maig de 2020.

Si s'han de tractar categories especials de dades (art. 9 RGPD), cal que el consentiment sigui explícit.

Com s'ha d'actuar si es perd la documentació on s'havia recollit el consentiment de la persona afectada per tractar les seves dades?

Si no es disposa d'una altra base jurídica, el col·legi professional ha de cessar en el tractament de dades fins a obtenir novament el consentiment de la persona afectada,

el qual ha de reunir els requisits establerts a l'RGPD. Si es vol fonamentar en una altra base jurídica, les persones afectades han de ser informades de la nova base jurídica i han de poder exercir els drets inherents a aquesta nova base jurídica.

Un col·legi professional pot, sobre la base jurídica del consentiment, utilitzar grups d'un servei de missatgeria instantània per comunicar-se amb els col·legiats?

Sí, sempre que, pel que fa a les funcions públiques, els participants tinguin altres canals alternatius de comunicació amb el col·legi per a les finalitats previstes; és a dir, que aquest servei no se'ls imposi com a única via de comunicació. En tot cas, cal comptar amb el consentiment de totes les persones integrants del grup.

Cal vetllar perquè el servei compleixi amb les mesures de seguretat adequades, tenint en compte la finalitat de les comunicacions per a les quals s'emprarà.

Continua essent vàlid el consentiment atorgat abans de l'entrada en vigor de l'RGPD?

Sí, sempre que reuneixi els requisits establerts per l'RGPD, és a dir, que el consentiment sigui informat, lliure, específic i inequívoc. Altrament, el col·legi ha de cessar en el tractament fins a obtenir novament el consentiment de la persona afectada, llevat que compti amb alguna altra base jurídica.

Normativa aplicable: considerants 32, 38, 42 i 43 i arts. 4.11), 6.1.a), 7, 8, 9.2.a), 22.2.c) i 49.1.a) RGPD; arts. 6, 7 i 9 LOPDGDD.

5.1.2 L'execució d'un contracte

L'RGPD considera lícit el tractament de dades quan és necessari per executar un contracte en què la persona afectada n'és part o per aplicar mesures precontractuals a petició d'aquesta persona.



Els col·legis professionals poden tractar les dades del seu personal laboral sobre la base jurídica relativa a l'execució d'un contracte?

Sí, sempre que aquestes dades siguin necessàries per mantenir o complir la relació laboral que aquests treballadors tenen amb el col·legi o amb algun dels ens que en depenen.

Normativa aplicable: considerants 40 i 44 i art. 6.1 b) RGPD.

5.1.3 El compliment d'una obligació legal

D'acord amb l'RGPD el tractament de dades també pot ser lícit quan és necessari per al compliment d'una obligació legal aplicable al responsable del tractament.

Cal que aquesta obligació estigui prevista en una norma amb rang de llei o en el dret de la Unió Europea.



Un col·legi professional pot comunicar les dades dels seus treballadors a la Tresoreria General de la Seguretat Social en sol·licitar l'afiliació d'un treballador a la Seguretat Social?

Sí, atès que la legislació sectorial aplicable estableix expressament l'obligació de l'empresari, en aquest cas, del col·legi, de sol·licitar l'afiliació de qui ingressi al seu servei.

Normativa aplicable: considerants 41 i 45 i art. 6.1.c) RGPD; art. 8.2 LOPDGDD.

5.1.4 La protecció d'interessos vitals

L'RGPD també permet el tractament de dades quan és necessari per protegir un interès essencial per a la vida de la persona afectada o d'una altra persona física.

En principi, aquesta base jurídica té caràcter subsidiari, és a dir, només ha d'emprar-se quan el tractament de dades no es pot fonamentar en cap altra de les bases jurídiques. Aquesta base jurídica també pot ser aplicable a situacions com ara el tractament de dades amb finalitats humanitàries, inclòs el control i la propagació d'epidèmies, o en situacions d'emergència humanitària, sobretot en cas de catàstrofes naturals o d'origen humà.

Normativa aplicable: considerant 46 RGPD; art. 6.1.d) RGPD.

5.1.5 El compliment d'una missió d'interès públic o en l'exercici de poders públics

L'RGPD permet el tractament de dades personals quan és necessari per complir una missió d'interès públic o en l'exercici de poders públics conferits al responsable del tractament.

La missió d'interès públic o, si escau, els poders públics esmentats han de derivar d'una funció atribuïda al col·legi per una norma amb rang de llei.

La legislació que regula els col·legis professionals els atribueix una sèrie de funcions públiques. Per exemple, garanteixen que l'exercici de la professió s'adeqüi a la normativa, la deontologia i les bones pràctiques; exerceixen la potestat disciplinària sobre els col·legiats;

en visen els projectes i els treballs; regulen i fixen les aportacions col·legials, i promouen la formació contínua dels col·legiats per garantir-ne la competència professional. Sobre aquesta qüestió, ens remetem a l'apartat 3 d'aquesta guia.

Per exercir aquestes i altres funcions públiques que tenen encomanades, els col·legis poden recollir i tractar determinades dades de les persones col·legiades i de terceres persones, sense requerir-ne el consentiment.



Un col·legi professional pot difondre al portal web i per xarxes socials fotografies d'esdeveniments organitzats pel col·legi on apareguin persones físiques, sense el seu consentiment?

La difusió d'imatges de persones físiques que ocupen un càrrec públic o una professió de projecció pública, o de persones que apareixen com a merament accessòries, en actes o esdeveniments organitzats pel col·legi vinculats a les seves funcions públiques pot tenir base jurídica suficient, sempre d'acord amb el que disposa la Llei orgànica 1/1982, de 5 de maig, de protecció civil del dret a l'honor, la intimitat personal i familiar i a la pròpia imatge. Això, sens perjudici que s'apliqui el principi de minimització i se n'informi adequadament les persones afectades.

Quan les imatges estiguin vinculades a l'exercici de les seves funcions privades, pot comptar amb la base jurídica derivada de l'existència de l'interès legítim.

Un col·legi professional pot demanar a una universitat que confirmi si una determinada persona col·legiada, o que ha demanat col·legiar-se, té la titulació habilitant per fer-ho?

Sí. En aquest cas, la base jurídica seria a l'article 6.1.e) en relació amb la normativa que els atribueix el control de l'exercici de la professió i la disposició addicional vuitena de l'LOPDGDD.

Normativa aplicable: considerant 45 i art. 6.1.e) RGPD; art. 8.2 LOPDGDD; arts. 5 i 7 Llei 2/1974; art. 39 i s. i 51 Llei 7/2006.

5.1.6 La satisfacció d'un interès legítim

El tractament de dades personals també pot ser lícit quan és necessari per satisfer interessos legítims perseguits pel responsable del tractament o per un tercer, sempre que no hagin de prevaler els interessos o els drets i les llibertats fonamentals de la persona afectada que requereixen la protecció de dades personals, especialment si la persona afectada és un nen. A aquests efectes, el responsable del tractament ha de fer la ponderació escaient.

Els col·legis professionals poden utilitzar aquesta base jurídica en l'exercici de les seves funcions privades.

En canvi, els col·legis professionals no poden emprar aquesta base jurídica per fonamentar els tractaments de dades que duen a terme en exercici de les seves funcions públiques. No obstant això, aquesta base jurídica pot fonamentar la comunicació de dades personals sol·licitades per altres subjectes en els quals concorre un interès legítim que hagi de prevaldre sobre els drets i interessos de les persones afectades. En aquest cas, per poder aplicar aquesta base jurídica, el col·legi professional ha de fer una ponderació i apreciar en aquestes persones un interès legítim que hagi de prevaldre sobre els drets i interessos de les persones afectades.

Per fer la ponderació d'interessos i determinar si hi concorre un interès legítim que pugui fonamentar el tractament de les dades, cal tenir en consideració tres factors:

- L'interès legítim del responsable o de tercers.
- L'impacte del tractament sobre les persones afectades.
- Les garanties addicionals que s'apliquin als tractaments.



Un col·legi professional pot trametre informació als seus col·legiats, per correu postal, sobre un nou servei de caràcter privat que ofereix el col·legi, o sobre productes i serveis oferts per tercers, a l'empara de la base jurídica de l'interès legítim?

Aquest tractament, que es podria considerar una activitat de màrqueting directe, es podria basar en l'interès legítim. Això, llevat que la persona col·legiada s'hi hagi oposat, s'hagi inscrit en un sistema d'exclusió publicitària o que de la ponderació de les circumstàncies concurrents en resulti que ha de prevaler el dret a la protecció de dades de les persones afectades.

Si la comunicació es fa per mitjans electrònics és d'aplicació el règim especial configurat per la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i del comerç electrònic.

D'acord amb aquest règim, les comunicacions comercials per mitjans electrònics han de comptar amb el consentiment exprés de les persones afectades, tret dels supòsits en què hi hagi una relació comercial prèvia i la comunicació es refereixi a productes o serveis de la seva pròpia empresa similars als que es van contractar inicialment.

Normativa aplicable: considerant 47 i art. 6.1.f) RGPD; art. 23 i DA 10 LOPDGDD.

5.2 Les categories especials de dades

L'RGPD estableix un règim més restrictiu per tractar determinades dades que, per la seva naturalesa, són particularment sensibles, atès que el seu tractament podria comportar grans

riscos per als drets i llibertats de les persones afectades. En concret, s'estableix una prohibició general de tractament respecte les categories següents:

- Les opinions polítiques.
- Les conviccions religioses o filosòfiques.
- L'afiliació sindical.
- Les dades que revelen l'origen ètnic o racial.
- Les dades genètiques.
- Les dades biomètriques destinades a identificar de manera unívoca una persona física.
- Les dades relatives a la salut.
- Les dades relatives a la vida sexual o a l'orientació sexual d'una persona física.

Malgrat això, el mateix RGPD estableix un seguit d'excepcions en les quals es poden tractar aquestes categories de dades. En el cas dels col·legis professionals, convé destacar-ne les següents:

- El tractament es fonamenta en el consentiment explícit de la persona afectada. Cal tenir en compte que el mer consentiment de la persona afectada pot no ser suficient per aixecar la prohibició del tractament de dades la finalitat principal del qual sigui identificar-ne la ideologia, afiliació sindical, religió, orientació sexual, creences o origen racial o ètnic, quan pugui donar lloc a situacions discriminatòries.
- El tractament és necessari per complir obligacions o exercir drets en l'àmbit laboral, si així ho autoritza el dret de la Unió o de l'estat membre. El dret de l'estat membre pot consistir en una norma amb rang de llei o en un conveni col·lectiu.
- El tractament és necessari per protegir interessos vitals de la persona afectada o d'una altra persona física, en el supòsit que la persona afectada no estigui capacitada físicament o jurídicament per donar el consentiment.
- El tractament es refereix a dades personals que la persona afectada ha fet manifestament públiques.
- El tractament és necessari per formular, exercir o defensar reclamacions o quan els tribunals actuen en exercici de la seva funció judicial.
- El tractament és necessari per raons d'un interès públic essencial, establert en una llei o en el dret de la Unió, que ha de ser proporcional a l'objectiu perseguit, respectar el dret a la protecció de dades en l'essencial i establir mesures adequades i específiques per protegir els interessos i els drets fonamentals de la persona afectada.
- El tractament és necessari per a finalitats de medicina preventiva o laboral, d'avaluació de la capacitat laboral del treballador, de diagnòstic mèdic, de prestació d'assistència o de tractament de tipus sanitari o social, o de gestió dels sistemes i els serveis d'assistència sanitària i social, sobre la base d'una norma amb rang de llei o del dret de la Unió o en virtut d'un contracte amb un professional sanitari. Aquest tipus de tractament l'ha d'efectuar un professional subjecte al deure de secret

o bé sota la seva responsabilitat, o qualsevol altra persona subjecta a l'obligació de secret.

- El tractament és necessari amb finalitats d'arxiu en interès públic, amb finalitats de recerca científica o històrica o amb finalitats estadístiques, sobre la base d'una norma amb rang de llei o dret de la Unió que reguli garanties adequades per als drets i llibertats de les persones afectades.

La concurrència d'alguna de les circumstàncies previstes a l'article 9 RGPD no eximeix de la necessitat de disposar d'una base jurídica de les previstes a l'article 6 RGPD, sinó que actua de manera cumulativa.

En relació amb el tractament de dades genètiques i de dades relacionades amb la salut, s'ha de tenir en compte el que disposa la disposició addicional dissetena de l'LOPDGDD.

Els responsables o encarregats que tractin aquests tipus de dades han de tenir en compte especialment aquesta circumstància quan analitzin els riscos derivats del tractament. A més, si les tracten a gran escala, tenen determinades obligacions específiques com ara fer una avaluació d'impacte, o determinats requisits específics quan vulguin prendre decisions automatitzades, inclosa l'elaboració de perfils.

Tot i no formar part de les categories especials de dades, les dades relatives a condemnes i infraccions penals, així com les relatives a procediments i mesures cautelars i de seguretat connexes, només es poden tractar a l'empara d'una norma de dret de la Unió o en una norma amb rang de llei. Únicament es pot portar un registre complet d'aquestes dades sota el control de les autoritats públiques i de conformitat amb el que estableix la regulació del sistema de registres administratius de suport a l'Administració de justícia.

Pel que fa a les dades relatives a infraccions i sancions administratives, no tenen la condició de categoria especial de dades, tot i que tenen un règim específic. Sobre això, ens remetem a l'apartat 5.4.1 d'aquesta guia.



Es poden utilitzar dades biomètriques per al control horari en l'entorn laboral i per a l'accés a determinades dependències?

Atès que l'RGPD ha inclòs les dades biomètriques dins de les categories especials de dades, cal que hi hagi una norma amb rang de llei o un conveni col·lectiu que ho prevegi expressament. En aquests casos no es pot concloure de manera general que sigui adequat utilitzar aquests sistemes, sinó que cal que, prèviament, el responsable del tractament faci una avaluació d'impacte sobre la protecció de dades per avaluar-ne la proporcionalitat, les garanties i les mesures de seguretat previstes.

Cal que el col·legi professional faci una avaluació d'impacte relativa a la protecció de dades per tractar dades de salut en la gestió de recursos humans?

En principi, si el tractament que es duu a terme només implica la recollida de dades relatives a situacions de baixes dels treballadors, discapacitats, accessibilitat o prevenció de riscos laborals, necessàries per complir amb les obligacions establertes a la normativa vigent, no sembla que sigui exigible per aquest fet una avaluació d'impacte relativa a la protecció de dades.

Un col·legi professional pot facilitar dades al departament competent en matèria de salut de la Generalitat de Catalunya, amb la finalitat de control d'epidèmies?

Sí, l'RGPD habilita que les autoritats en matèria de salut pública tractin dades personals, incloses categories especials de dades, com ara les dades de salut, "quan el tractament és necessari per raons d'interès públic en l'àmbit de la salut pública, com la protecció davant d'amenaques transfrontereres greus per a la salut, o per garantir nivells elevats de qualitat i de seguretat de l'assistència sanitària i dels medicaments o productes sanitaris, sobre la base del dret de la Unió o dels estats membres que estableixi mesures adequades i específiques per protegir els drets i les llibertats de la persona afectada, en particular el secret professional" (articles 6.1.e) i 9.2.i) RGPD). A aquests efectes cal tenir en compte les previsions de la Llei 14/1986, de 25 d'abril, general de sanitat; la Llei 33/2011, de 4 d'octubre, general de salut pública; la Llei orgànica 3/1986, del 14 d'abril, de mesures especials en matèria de salut pública; i la Llei 18/2009, del 22 d'octubre, de salut pública.

El desenvolupament d'aquestes actuacions pot comportar que les autoritats en matèria de salut pública recullin informació, incloses dades de salut i que, si s'escau, la revelin dades de salut relatives a persones contagiades o sospitoses d'estar-ho, quan sigui estrictament necessari per aplicar mesures de control.

Normativa aplicable: considerants 34, 35, 51 a 56, 71 i arts. 9, 10 i 22.4 RGPD; art. 9.1, 10, DA 17a, DF 3a.1, 5a i 11a.2 LOPDGDD.

5.3 Les comunicacions de dades

L'RGPD, a diferència de l'LOPD, no preveu habilitacions específiques per a les comunicacions de dades personals, sinó que se'ls aplica el règim general previst per a la resta de tractaments.

Per tant, qualsevol comunicació de dades requereix alguna de les bases jurídiques esmentades. Si, a més, comporta el tractament de categories especials de dades, també hi ha de concórrer alguna de les excepcions previstes a l'article 9.2 de l'RGPD.

Cal tenir en compte que, en el cas de les funcions públiques del col·legi, tot i que en principi no els resulta aplicable la base jurídica consistent en la satisfacció dels seus interessos legítims, sí que pot habilitar la comunicació de dades a terceres persones fonamentada en els interessos legítims d'aquestes persones.



És legítim que els membres de la junta o l'assemblea del col·legi accedeixin a les retribucions de tots els treballadors del col·legi?

Els membres de la junta o assemblea general d'un col·legi professional poden accedir a les dades de les retribucions dels diferents llocs de treball del col·legi –sense necessitat d'identificar, amb caràcter general, les persones que ocupen els llocs-, en la mesura que resulti necessari per exercir les funcions que tingui atribuïdes aquest òrgan. Això sens perjudici de la possibilitat d'accedir directament a les retribucions percebudes pels òrgans de govern i directius, d'acord amb la normativa de transparència que regula la publicitat activa.

Un col·legi professional pot comunicar a un mitjà de comunicació informació sobre els complements salarials d'un càrrec directiu del col·legi?

Sí. D'acord amb la legislació de transparència, aplicable a les funcions públiques del col·legi, cal publicar de manera individualitzada la informació sobre totes les retribucions percebudes pels seus òrgans de govern i càrrecs directius. A més, és criteri reiterat tant d'aquesta Autoritat com de la Comissió de Garantia d'Accés a la Informació Pública (GAIP) que respecte altre personal que es pugui considerar de confiança o amb altes responsabilitats, normalment associades a un elevat nivell retributiu, també es pugui facilitar aquesta informació.

Els empleats de correus i altres empreses de missatgeria poden demanar les dades identificatives del personal del servei d'atenció al públic d'un col·legi professional a l'efecte de fer-les constar en els justificants de recepció de la documentació lliurada?

Pot ser adequat a la normativa de protecció de dades indicar en el justificant de recepció les dades identificatives de la persona que es fa càrrec de la recepció. Ara bé, no cal facilitar-les, en el cas de notificacions d'òrgans administratius i judicials de documentació presentada al registre general apta per ser registrada. En aquest cas, és suficient de fer-hi constar el segell del col·legi.

Un col·legi professional ha publicat un anunci en un diari oficial sobre una notificació infructuosa en un expedient disciplinari, que no inclou el nom i cognoms, sinó només el número del DNI. És correcte?

Sí. En aquests casos, l'anunci que publica el col·legi ha d'identificar la persona afectada exclusivament amb el número complet del DNI o document equivalent, atès que la finalitat de l'anunci no és donar publicitat general a l'expedient, sinó només poder practicar una notificació per edictes. Únicament si la persona afectada no disposa d'aquests documents identificatius, se l'ha d'identificar mitjançant el nom i cognoms. En cap cas s'ha de publicar el nom i cognoms de manera conjunta amb el número complet del DNI o d'altres documents equivalents.

Normativa aplicable: art. 4.2, 6 i 9 RGPD; DA 7a i 10a LOPDGDD; arts. 3.1.b) i 9.1.b) LTC.

5.3.1 Accés de tercers a dades personals de les persones col·legiades a través de la finestreta única

La normativa que regula els col·legis professionals preveu que han de disposar d'una finestreta única en el seu web, a través de la qual han d'oferir informació clara, inequívoca i gratuïta sobre els aspectes següents:

- L'accés al **registre de col·legiats**, que ha d'estar permanentment actualitzat i en el qual han de constar, almenys, les dades següents: nom i cognoms del professional col·legiat, número de col·legiació, títols oficials que posseeix, domicili professional i situació d'habilitació professional.
- L'accés al **registre de societats professionals**, que ha de tenir el contingut descrit a l'article 8 de la Llei 2/2007, de 15 de març, de societats professionals, que inclou determinada informació personal com ara la identificació dels socis professionals i no professionals (i en relació amb els socis professionals, el número de col·legiat i el col·legi professional al qual pertanyen); i la identificació de les persones que s'encarreguen de l'administració i la representació, amb indicació de la condició de soci professional o no de cadascuna d'elles.
- Les vies de reclamació i els recursos que es poden interposar en cas de conflicte entre el consumidor o usuari i un col·legiat o el col·legi professional.
- Les dades de les associacions o organitzacions de consumidors i usuaris a les quals els destinataris dels serveis professionals poden adreçar-se per obtenir assistència.
- El contingut dels codis deontològics.



S'adequa a l'RGPD la possibilitat que un ciutadà accedeixi a dades que figuren al registre de col·legiats a través del web del col·legi professional?

Sí, perquè es tracta d'una comunicació de dades habilitada per la Llei 2/1974 i la Llei 7/2006, que obliguen a donar accés públic al registre de col·legiats a través del seu web (finestreta única).

Quina informació cal publicar a la finestreta única o comunicar en cas de consulta, respecte dels col·legiats no exercents (inclosos els casos de jubilació o invalidesa) i els col·legiats donats de baixa o difunts o dels seus hereus?

El col·legi pot publicar a través de la finestreta única o comunicar a tercers la informació següent, tant de professionals exercents com no exercents: nom i cognoms, número de col·legiació, titulació, dades de contacte professional (domicili professional, telèfon, adreça de correu electrònic ...) i situació d'habilitació professional. En canvi, no es poden divulgar dades de les persones col·legiades donades de baixa ni de les persones hereves d'un col·legiat difunt. Pel que fa a les dades de col·legiats difunts, tot i que en principi no han de figurar a la finestreta única, cal tenir present que no se'ls aplica la normativa de protecció de dades personals.

La normativa de protecció de dades no impedeix la publicació del domicili personal del col·legiat quan coincideixi amb el domicili professional. Això sens perjudici del deure d'informar-ne prèviament els professionals afectats i de la possibilitat que aquests s'oposin a la divulgació d'aquesta dada, quan la seva situació personal ho justifiqui.

Es pot informar un tercer de la data en què un advocat col·legiat va causar baixa del col·legi o va passar a la situació de no exercent?

La dada relativa a la data concreta en què un advocat col·legiat passa a la situació de no exercent, no forma part de les dades incloses en la normativa que regula la finestra única, ni la seva publicació està emparada per l'article 19 de l'LOPDGDD. No obstant això, atès que pot haver-hi diferents casos en que aquesta data esdevingui rellevant, el col·legi pot facilitar-la a un tercer sempre que es doni alguna de les condicions de licitud del tractament que regula l'RGPD (consentiment, interès legítim, etc.).

El motiu de la situació d'inactivitat d'una persona col·legiada pot formar part del llistat de professionals? Hi pot constar en el període de temps d'inactivitat?

No. Tot i que aquesta llista pot recollir la situació de no exercent o d'inactivitat temporal, no ha de recollir els motius als quals obeeix aquesta situació, ni el període que la persona col·legiada hi pugui romandre. La Llei 2/1974 recull l'obligació de oferir mitjançant la finestra única la dada de la situació d'habilitació professional, és a dir, exercent o no exercent o inactivitat temporal, però no recull l'obligació d'informar sobre una possible inhabilitació.

El llistat de professionals que es publica a la finestra única es pot considerar una font accessible al públic?

Actualment la normativa de protecció de dades no conté una definició de què s'ha d'entendre com a font accessible al públic, ni estableix cap règim específic pel que fa al tractament de les dades que poden contenir. Es pot considerar font d'accés públic, qualsevol conjunt d'informació de lliure accés per la ciutadania.

El col·legi pot facilitar a un col·legiat un llistat de les adreces electròniques de la resta de col·legiats que es dediquen a una especialitat?

Tot i que la dada relativa a l'especialitat no figura expressament entre les dades del registre de col·legiats que la Llei de col·legis professionals habilita a publicar a través de la finestra única (art. 40.bis de la Llei 7/2006), cal tenir en compte que la informació relativa a l'especialitat pot estar estretament relacionada amb les titulacions o amb la situació d'habilitació professional. Per tant, cal admetre'n la publicació o la comunicació a qualsevol persona, atès que es tracta d'un aspecte que pot resultar necessari per garantir millor els drets de les persones consumidores i usuàries.

Quines són les dades de les societats professionals inscrites que s'han de publicar a la finestra única?

El col·legi ha de publicar la informació que preveu l'article 8 de la Llei 2/2007, de 15 de març, de societats professionals que inclou determinada informació personal, com ara la identificació dels socis professionals (número de col·legiat i col·legi professional

al qual pertany) i no professionals, i la identificació de les persones que s'encarreguen de l'administració i la representació, amb indicació de la condició de soci professional o no de cadascuna d'elles.

Respecte de les persones encarregades de l'administració i representació d'aquestes societats, es pot donar accés a les seves dades identificatives. En ambdós casos se'n poden publicar les dades de contacte professional.

Es poden facilitar les dades d'un col·legiat a un tercer, quan les sol·licita per telèfon o per correu electrònic?

Sí. Si la comunicació es limita a les dades incloses a la llista de professionals que ha de publicar s'ha de considerar vinculada directament amb al compliment d'una de les funcions públiques del col·legi, prevista a la Llei 7/2006. Per comunicar altres dades no incloses a la llista esmentada (per exemple, DNI, dades bancàries, domicili particular, etc.), cal disposar d'alguna altra base jurídica.

Un col·legi pot comunicar dades dels col·legiats a l'empresa asseguradora amb qui té contractada l'assegurança col·lectiva de responsabilitat civil professional?

Sí, atès que si el col·legi ha establert una assegurança col·lectiva d'aquest tipus, la incorporació del col·legiat al col·legi comporta que passi a tenir la condició d'assegurat. La comunicació de dades seria necessària per desenvolupar aquesta relació jurídica. Això, sens perjudici que el col·legi ha d'informar els col·legiats sobre aquesta comunicació.

Es pot divulgar la identitat de les persones col·legiades que impulsen la inclusió d'un punt de l'ordre del dia de l'assemblea del col·legi?

S'ha de poder verificar la identitat i la condició de col·legiades de les persones promotores de la iniciativa, com a requisit per admetre-la. A més, la resta de persones col·legiades estan legitimades per consultar la documentació relativa a la convocatòria de l'assemblea. Per tant, la comunicació a la resta de persones col·legiades de la proposició d'incloure un nou punt de l'ordre del dia, identificant-ne les persones promotores, és conforme a la normativa de protecció de dades personals.

Normativa aplicable: art. 10 Llei 2/1974; 40 bis Llei 7/2006; Recomanació 1/2008.

5.3.2 Accés dels candidats en un procés electoral a les dades de col·legiats

L'accés dels candidats al cens electoral es pot considerar emparat en l'existència d'un interès legítim.

Per altra banda, pel que fa al règim d'accés a les dades que conté el cens electoral del col·legi, es pot considerar aplicable la Llei orgànica de règim electoral general (LOREG) com a norma supletòria. En aquest sentit, l'article 41.5 de la LOREG habilitaria el col·legi per proporcionar als candidats la còpia del cens l'endemà que es proclamïn com a candidats,

sense necessitat d'obtenir el consentiment previ de les persones afectades, perquè la cessió està habilitada per la previsió d'aquesta obligació en una norma amb rang de llei.

Cal excloure d'aquesta llista les persones que han exercit el seu dret d'oposició al·legant motius fonamentats en la seva situació personal que en justifiquin l'exclusió, o la no revelació d'algunes de les seves dades (per exemple, la seva adreça postal). En aquest darrer cas, la tramesa d'informació electoral es pot fer a una adreça electrònica o un apartat de correus que hagi designat la persona afectada.

En qualsevol cas, des del punt de vista del dret a la protecció de dades pot ser convenient que, en el moment de regular el procediment electoral en els seus estatuts, els col·legis valorin altres possibilitats diferents de la tramesa a l'adreça postal dels col·legiats, com ara la tramesa a una adreça electrònica designada pel col·legiat, la tramesa postal conjunta feta pel mateix col·legi, etc.



Es pot lliurar un llistat de les persones col·legiades, amb indicació de les seves dades de contacte, a una persona col·legiada interessada a concórrer a les eleccions a la junta de govern del col·legi?

El lliurament d'un llistat dels col·legiats (nom, cognoms i adreça de correu electrònic) a una persona col·legiada, proclamada candidata es pot considerar emmarcat en la satisfacció d'interessos legítims i, per tant, un tractament emparat en la base jurídica de l'article 6.1.f) de l'RGPD. La informació esmentada només es pot utilitzar per a la finalitat específica de facilitar la comunicació entre les persones candidates i la resta de persones col·legiades durant el període de campanya electoral.

La normativa de protecció de dades no estableix previsions específiques en relació amb la manera concreta de lliurar les dades personals.

Normativa aplicable: art. 6.1.c) RGPD; 41.5 LOREG.

5.3.3 Comunicació de sancions disciplinàries, inhabilitacions i incompatibilitats

Als efectes que estableix l'article 3.3 de la Llei 2/1974, els col·legis poden comunicar les sancions disciplinàries imposades als seus col·legiats a la resta dels col·legis territorials de la professió de què es tracti. Aquesta habilitació afecta només la informació necessària perquè la resolució sancionadora pugui desplegar els seus efectes en tot el territori.

Cal tenir en compte que la finestreta única pot reflectir les conseqüències de la inhabilitació (el col·legiat no apareixerà com a exercent) però sense fer referència a la sanció d'inhabilitació.



En quins casos els col·legis estan habilitats per la llei per comunicar informació relativa a la comissió d'infraccions administratives i a la imposició de sancions?

La comunicació d'informació sobre la comissió d'infraccions administratives o la imposició de sancions està habilitada per llei quan es comuniquen les sancions disciplinàries que impliquen inhabilitació o separació professional al consell de col·legis, perquè en doni trasllat a la resta de col·legis i als òrgans judicials (art. 6.1.e i 6.4 RGPD i art. 3.3 de la Llei 2/1974).

En la resta de supòsits no hi ha, amb caràcter general, una habilitació legal que permeti donar publicitat als expedients o les resolucions sancionadores ni per publicar les sancions imposades. Això sens perjudici que quan s'hagi imposat una sanció d'inhabilitació o de separació el col·legiat afectat s'hagi d'excloure de la llista de professionals del col·legi, mentre durin els efectes de la sanció.

Un col·legi professional pot comunicar a una universitat, amb la finalitat de controlar el compliment del règim d'incompatibilitats, una llista dels projectes visats respecte de determinats professionals que també tenen la condició de professors de la universitat esmentada?

La universitat pot accedir a les dades personals incloses a la finestra única.

D'altra banda, en el marc d'un procediment per incompliment de la normativa d'incompatibilitats, també es pot comunicar a la universitat la dada consistent en si professors amb dedicació a temps complet han sol·licitat el visat de certs treballs professionals, sense necessitat de requerir el consentiment previ d'aquests professors.

Un col·legi professional pot publicar la resolució de baixa forçosa d'un col·legiat per impagament, en el tauler d'anuncis o en un diari oficial?

No. Quan les resolucions adoptades no s'han pogut notificar personalment als col·legiats afectats, el col·legi està habilitat legalment per notificar-les per mitjà d'un anunci al butlletí oficial, però això no inclou la publicació de la resolució. L'anunci ha d'identificar la persona afectada exclusivament amb el seu número de DNI i ha de limitar-se a incloure la informació necessària perquè la persona afectada pugui recollir la notificació.

Normativa aplicable: art. 6.1.c) RGPD; 3.3 i 10.2.a) Llei 2/1974; DA 7a LOPDGDD.

5.3.4 Comunicacions de dades a administracions públiques, a altres col·legis i als consells de col·legis

Els col·legis professionals d'àmbit territorial han de facilitar als consells generals o superiors, i si escau als consells autonòmics de col·legis, la informació relativa a les altes, baixes i qualssevol altres modificacions que afectin els registres de col·legiats i de societats

professionals, perquè en prenguin coneixement i ho anotin en els seus registres centrals de col·legiats i de societats professionals.

A banda d'això, en altres supòsits, els col·legis professionals poden haver de comunicar dades a altres administracions públiques. Caldrà alguna de les bases jurídiques de l'article 6 de l'RGPD. En qualsevol cas, si no es disposa del consentiment o d'una llei que ho prevegi expressament, la comunicació només es pot fer per a una activitat que sigui compatible.



Un col·legi d'advocats pot comunicar al consell de col·legis la llista de col·legiats inscrits en el torn d'ofici i assistència al detingut?

El col·legi professional pot comunicar aquest llistat al Consell de l'Advocacia Catalana, sense requerir el consentiment previ als professionals afectats, si és necessari per controlar que es compleix el règim d'incompatibilitats previst per a la inscripció en el servei del torn d'ofici d'un determinat col·legi professional. Aquesta comunicació troba legitimació en l'article 6.1.e) i 6.4 de l'RGPD, en tractar-se d'una cessió de dades entre corporacions públiques per exercir una competència pública que versa sobre una mateixa matèria, com és la de regular i organitzar els serveis d'assistència lletrada i defensa i representació gratuïta, la qual inclou vetllar pel correcte funcionament d'aquest servei.

Això no exclou l'obligació de complir el deure d'informació. D'acord amb el que disposa l'article 14 de l'RGPD, el Consell dels Col·legis ha d'informar els professionals de manera expressa, precisa i inequívoca, en un termini raonable i com a màxim d'un mes, des de la comunicació, llevat que el col·legi professional ja els hagi informat anteriorment.

Cal demanar el consentiment per cedir les dades de què disposa la demarcació territorial catalana del col·legi professional d'àmbit estatal per constituir un col·legi professional català independent?

Les dades es poden cedir sense el consentiment dels afectats, en la mesura que de les previsions de la Llei 7/2006, de 31 de maig, de l'exercici de professions titulades i dels col·legis professionals, se'n desprèn que hi ha habilitació legal suficient per fer la comunicació (article 6.1.e) i 6.4). La cessió ha de comprendre només les dades personals de les persones col·legiades amb domicili professional únic o principal a Catalunya que siguin adequades, pertinents i no excessives perquè puguin col·legiar-se en el col·legi de Catalunya.

El nou col·legi, serà el nou responsable del tractament i haurà de complir el deure d'informació als afectats en els termes establerts a l'article 14 de l'RGPD, així com a la resta de principis i obligacions previstes en la normativa de protecció de dades personals.

Un col·legi d'advocats pot comunicar informació a l'Administració tributària sobre els informes elaborats en relació amb minuts presentades per advocats col·legiats?

La comunicació generalitzada d'informació sobre aquest tipus d'informes –que inclogui la identificació dels advocats corresponents– a l'Administració tributària no resulta justificada a l'empara de l'article 94.1 de l'LGT, atesa la manca de

transcendència tributària d'aquests informes, que es tracta només d'estimacions provisionals sobre els honoraris, i que no hi ha una disposició general que prevegi aquest requeriment generalitzat d'informació.

Un col·legi pot comunicar dades de salut de les persones col·legiades a una administració pública, per fer un estudi estadístic?

Si un col·legi disposa de dades de salut dels seus col·legiats i una administració pública les requereix per fer un estudi estadístic sobre morbiditat de determinats col·lectius professionals, a manca de consentiment de les persones afectades, el col·legi només pot comunicar aquestes dades prèvia anonimització.

Un col·legi pot accedir a informació de què disposen les administracions públiques, per controlar el compliment del deure de col·legiació de determinats professionals?

Sí, atès que el control de la col·legiació obligatòria forma part de les funcions atribuïdes als col·legis professionals.

Un col·legi professional pot comunicar a un jutjat la dada relativa al número d'identificació fiscal d'un col·legiat?

Si un Jutge ho requereix per exercir les funcions que té atribuïdes, aquesta comunicació s'adequa a la normativa de protecció de dades, ja que té l'habilitació legal a l'RGPD i a l'LOPJ.

Normativa aplicable: art. 6.1 lletres c) i e) RGPD; art. 25 LOPDGDD; 10.4 Llei 2/1974; Llei 1/1996.

5.3.5 Comunicació de dades a cossos policials

Pel que fa a les comunicacions de dades als cossos policials, cal tenir en compte que la Llei orgànica 7/2021 disposa l'obligació de qualsevol persona física o jurídica de proporcionar a les autoritats competents les dades, els informes i els justificants necessaris que els sol·licitin, de manera motivada, concreta i específica, en els supòsits següents:

- Per a la investigació i l'enjudiciament d'infraccions penals o per a l'execució de penes per part de les autoritats judicials, el ministeri fiscal o la policia judicial. De les sol·licituds d'informació fetes per la policia judicial, se n'ha de donar compte en tot cas a l'autoritat judicial i fiscal. La comunicació de dades que duguin a terme l'Administració tributària, la Inspecció de Treball i l'Administració de la Seguretat Social, s'ha de fer d'acord amb la seva legislació específica.
- Per a la prevenció, la detecció i la investigació d'infraccions penals per les autoritats competents.
- Per a la prevenció i la protecció enfront d'un perill real i greu per a la seguretat pública per les autoritats competents.

Aquestes determinacions no eximeixen d'obtenir l'autorització judicial pertinent, quan sigui exigible.

Incomplir aquest deure de col·laboració, o facilitar informació a les persones afectades per aquestes comunicacions, es tipifica com a infracció en diferents preceptes de la Llei orgànica (art. 58.j i 59.j).

Normativa aplicable: art. 7 Llei orgànica 7/2021.

5.4 Disposicions aplicables a tractaments específics

5.4.1 Tractament de dades relatives a infraccions i sancions administratives

L'RGPD no regula específicament el tractament de dades relatives a infraccions i sancions administratives. Ara bé, l'LOPDGDD sí que estableix determinades condicions específiques per tractar aquestes dades, de les quals en formarien part, per exemple, les dades relatives a les infraccions disciplinàries imposades a l'empara de la normativa que regula els col·legis professionals. En concret, l'LOPDGDD permet que les puguin tractar els òrgans competents per instruir el procediment sancionador, per declarar les infraccions o imposar les sancions, sempre que el tractament es limiti a les dades estrictament necessàries per a aquesta finalitat.

Fora d'aquest supòsit, només es poden tractar si:

- Es compta amb el consentiment exprés de la persona afectada
- Ho autoritza una norma amb rang de llei, en la qual s'han de regular, si escau, garanties addicionals pels drets i les llibertats de les persones afectades.
- El tractament el duen a terme advocats o procuradors a partir de la informació facilitada pels seus clients per exercir les seves funcions.

En qualsevol cas, aquest tipus de dades queden excloses del dret d'accés a la informació pública regulat per la legislació de transparència, llevat que les persones hi hagin consentit, que ho prevegi una llei o que la mateixa persona afectada les hagi fet manifestament públiques.

Normativa aplicable: art. 27 LOPDGDD; art. 15.1 LT; art. 23 LTC.

5.4.2 Tractament de dades del personal dels col·legis professionals

5.4.2.1 Dades de contacte professional del personal del col·legi

Els col·legis professionals responsables o encarregats del tractament poden publicar les dades professionals de contacte i, si escau, les relatives a la funció o el lloc que exerceixin les persones físiques que hi presten serveis, quan es derivi d'una obligació legal o sigui necessari per exercir les seves funcions.

Requisits:

- El tractament s'ha de referir únicament a les dades necessàries per a la seva localització professional.
- La finalitat del tractament ha de ser únicament mantenir relacions de qualsevol índole amb el col·legi professional.

Normativa aplicable: art.19 LOPDGDD

5.4.2.2 Videovigilància en l'àmbit laboral

Els col·legis professionals poden tractar les imatges obtingudes a través de sistemes de càmeres o videocàmeres per exercir les funcions de control dels seus treballadors, sempre que s'exerceixin dins del seu marc legal i amb els límits inherents a aquest.

Per valorar la proporcionalitat de la instal·lació del sistema de videovigilància cal tenir en compte:

- Si el sistema de videovigilància és apte per aconseguir la finalitat perseguida.
- Si no existeixen altres mesures menys intrusives per aconseguir la finalitat i amb la mateixa eficàcia.
- Si és una mesura equilibrada, és a dir, si ofereix més beneficis per a l'interès general que perjudicis.

La utilització de sistemes similars per a la gravar veus al lloc de treball s'admet únicament quan hi concorren riscos rellevants per a la seguretat de les instal·lacions, els béns i les persones derivats de l'activitat que es duu a terme al centre de treball.

En qualsevol cas, la utilització d'aquests sistemes està sotmesa a determinats límits i garanties:

- Intervenció mínima, és a dir, els controls han de tenir com a objectiu inspeccionar l'execució de les obligacions laborals, sense excedir de qüestions vinculades al seu desenvolupament.

- El respecte a la dignitat de la persona treballadora. En cap cas s'admet la instal·lació de sistemes de gravació de sons ni de videovigilància a vestidors o lavabos ni a llocs destinats al descans o esbarjo de les persones treballadores, com ara menjadors o llocs anàlegs.
- Abans d'iniciar la captació, el col·legi ha d'informar els treballadors, i si escau els seus representants, de l'existència d'aquests dispositius, de manera expressa, clara i inequívoca, d'acord amb el que s'estableix a l'apartat 5.4.4 d'aquesta guia. Si s'han captat treballadors en la comissió flagrant d'un acte il·lícit s'entén complert el deure d'informar quan hi hagi almenys el dispositiu informatiu en un lloc prou visible que informi de l'existència del tractament, de la identitat del responsable i de la possibilitat d'exercir els drets que preveuen els articles 15 a 22 de l'RGPD.
- Els sistemes de videovigilància que captin imatges o veus, amb independència que s'enregistrin o no, s'han d'inscriure en el registre d'activitats de tractament. El sistema de videovigilància pot estar format per una càmera o per diverses càmeres en una mateixa instal·lació o en diverses sempre que obeeixin a una mateixa finalitat i el tractament tingui unes característiques equiparables.

Quan un col·legi professional implanti un sistema de videovigilància que comporti l'accés d'una empresa de seguretat privada a les imatges o veus que es captin, aquesta empresa té la consideració d'encarregat del tractament.

La supressió de les dades d'aquests sistemes de gravació s'ha de dur a terme en el termini màxim d'un mes des que es van captar, excepte quan s'hagin de conservar per acreditar que s'han comès actes que atempten contra la integritat de persones, béns o instal·lacions. En aquest cas, les imatges s'han de posar a disposició de l'autoritat competent en un termini màxim de setanta-dues hores des que es té coneixement de l'existència de la gravació.

L'obligació de bloqueig que preveu l'article 32 de l'LOPDGDD no és aplicable a aquests tractaments.

Sobre aquesta qüestió cal tenir en compte també el que s'exposa a l'apartat 5.4.4 d'aquesta guia i, en especial la Instrucció 1/2009 d'aquesta Autoritat, sobre el tractament de dades de caràcter personal mitjançant càmeres amb fins de videovigilància.



Un col·legi professional vol instal·lar videocàmeres a la seu col·legial per a finalitats de seguretat i de control horari amb fins laborals. Què cal tenir en compte?

Cal tenir en compte si la instal·lació de cada càmera respon a una o altra finalitat, o a les dues, i analitzar en conseqüència si s'ajusta a la normativa i en especial a la Instrucció 1/2009. Només poden accedir a les imatges les persones autoritzades per raó de les seves funcions. Cal tenir especialment en compte el principi de proporcionalitat.

Pel que fa a les càmeres amb finalitats de control laboral, a banda d'analitzar si hi ha mecanismes de control horari i de presència alternatius i menys lesius per als drets de les persones afectades per determinar-ne la proporcionalitat, cal informar els treballadors i els seus representants que s'han instal·lat.

Quin ha de ser el termini de conservació de les imatges de les càmeres amb finalitat de control laboral?

En relació amb els tractaments de videovigilància, l'LOPDGDD preveu el termini de conservació d'un mes com a màxim. Això no vol dir que necessàriament s'hagi d'esgotar aquest termini. Per aplicació del principi de limitació del termini de conservació, les imatges s'han de suprimir al més aviat possible, si no hi ha circumstàncies que en justifiquin la conservació.

Normativa aplicable: art. 22 i 89 LOPDGDD; art. 20 i 20.bis ET.

5.4.2.3 Ús de dispositius digitals

Les persones treballadores tenen dret a la protecció de la seva intimitat en l'ús dels dispositius digitals, com ara ordinadors, tauletes, *smartphones* o comptes de correu que el col·legi posi a la seva disposició.

El col·legi només pot accedir als continguts derivats de l'ús de mitjans digitals facilitats a les persones treballadores per a les finalitats següents:

- Controlar el compliment de les obligacions laborals.
- Garantir la continuïtat dels serveis.
- Garantir la integritat dels dispositius esmentats.

L'ús de dispositius digitals requereix:

- Que el col·legi estableixi els criteris d'utilització respectant els estàndards mínims de protecció de la intimitat dels treballadors d'acord amb els usos socials i els drets reconeguts constitucionalment i legalment.
Els representants de les persones treballadores han de poder participar en l'elaboració d'aquests criteris.
- Que s'informi les persones treballadores dels criteris establerts.

L'accés del col·legi professional al contingut de dispositius digitals respecte dels quals n'hagi admès l'ús amb finalitats privades requereix:

- Que se n'hagin especificat els usos autoritzats de manera precisa.
- Que s'estableixin garanties per preservar la intimitat de les persones treballadores (per exemple, presència de la persona afectada, si és possible, o en el seu defecte, d'un representant dels treballadors; aixecar una acta; garantir el no accés a la informació privada que pugui constar-hi; etc.).

Sobre aquesta qüestió es recomana consultar la [Recomanació 1/2013](#), d'aquesta Autoritat, sobre l'ús del correu electrònic a l'àmbit laboral.



Un col·legi professional pot controlar els ordinadors assignats als seus treballadors, amb la finalitat de verificar-ne l'ús?

Sí. Si el tractament es duu a terme durant la prestació del servei i per assegurar-ne el normal funcionament, el col·legi no necessitaria disposar del consentiment previ de les persones afectades. En qualsevol cas, convé tenir aprovades normes internes sobre l'ús de les TIC que siguin conegudes pels treballadors, i dur a terme la intervenció d'acord amb aquestes normes i amb el principi de proporcionalita.

Normativa aplicable: art. 87 LOPDGDD; arts. 20 i 20.bis ET.

5.4.3 Tractament de dades de contacte de persones al servei de persones jurídiques, d'empresaris individuals i de professionals liberals

Els col·legis professionals poden tractar les dades necessàries per a la localització professional dels professionals liberals i empresaris individuals, quan s'hi refereixin únicament en aquesta condició i no es tractin per establir-hi una relació com a persones físiques, sempre que es derivi d'una obligació legal o sigui necessari per exercir les seves funcions públiques.

També poden tractar les dades de contacte i, si escau, les relatives a la funció o el lloc que exerceixen, de les persones físiques que presten serveis en una persona jurídica, quan:

- Es tractin únicament les dades necessàries per a la seva localització professional.
- La finalitat del tractament sigui únicament mantenir relacions de qualsevol índole amb la persona jurídica en què la persona afectada presti els seus serveis.
- Es derivi d'una obligació legal o sigui necessari per exercir les seves funcions públiques.



Un col·legi professional pot utilitzar dades de contacte professional de treballadors d'empreses, de personal de l'administració o de professionals liberals recollides de les pàgines web d'aquestes organitzacions, per establir-hi contacte professional?

Sí. Sempre que sigui per establir-hi contacte professional.

Normativa aplicable: art. 19 LOPDGDD.

5.4.4 Tractament amb fins de videovigilància

Els col·legis professionals poden captar imatges a través de sistemes de càmeres o videocàmeres amb la finalitat de preservar la seguretat de les persones i béns, així com de les seves instal·lacions.

No obstant això, amb caràcter general, els col·legis professionals no poden captar imatges de la via pública amb aquests sistemes, llevat que sigui imprescindible per a la finalitat de preservar la seguretat de les persones i béns, i de les seves instal·lacions.

Els col·legis professionals han d'informar de l'existència de les càmeres col·locant un cartell informatiu en un lloc prou visible amb el contingut mínim, següent:

- L'existència del tractament.
- La identitat del responsable.
- La possibilitat d'exercir els drets que preveuen els articles 15 a 22 de l'RGPD.
- El lloc on les persones afectades poden obtenir la resta d'informació sobre el tractament que requereix l'RGPD. S'hi pot incloure un codi de connexió o una adreça d'Internet per obtenir aquesta informació.

Cal tenir en compte que la ubicació dels cartells informatius ha de permetre a les persones afectades preveure quines són les àrees vigilades. Així, per a les càmeres de videovigilància en edificis o instal·lacions, s'ha de col·locar un cartell informatiu en cadascun dels accessos a l'àrea videovigilada. Si estan dividits per plantes amb diferents responsables o amb finalitats diferents, a més a més, cal col·locar un altre cartell informatiu en cadascuna de les plantes on hi hagi càmeres, ubicat en un espai d'accés principal a l'àrea o zona videovigilada.

Les dades s'han de suprimir en el termini màxim d'un mes des de la seva captació. Quan s'hagin de conservar per acreditar la comissió d'actes que atemptin contra la integritat de persones, béns o instal·lacions les imatges s'han de posar a disposició de l'autoritat competent en un termini màxim de setanta-dues hores des que es té coneixement de l'existència de la gravació.

L'obligació de bloqueig no és aplicable a aquests tractaments.

Sobre aquesta qüestió cal tenir en compte la Instrucció 1/2009 d'aquesta Autoritat, sobre el tractament de dades de caràcter personal mitjançant càmeres amb fins de videovigilància.



Es poden instal·lar càmeres de videovigilància a la seu del col·legi amb fins de seguretat?

Sí, atès que, sempre que es respectin la resta de principis i garanties de la normativa de protecció de dades, la implantació d'aquest tipus de sistemes de

videovigilància en les seves instal·lacions es pot considerar inclosa en el compliment de la missió en interès públic que tenen encomanada els col·legis professionals.

Quant de temps es poden conservar les imatges obtingudes a través d'un sistema de videovigilància?

Quan no es pugui assolir la finalitat perseguida sense emmagatzemar les imatges, el període de conservació no ha de ser superior al necessari per complir la finalitat de vigilància per a la qual s'han recollit o enregistrat. Amb caràcter general, no es pot excedir el termini d'un mes per suprimir-les.

Com s'apliquen les mesures de seguretat en els tractaments de dades mitjançant sistemes de videovigilància?

Les mesures de seguretat s'han de determinar cas per cas d'acord amb l'anàlisi de riscos realitzada. Les mesures de seguretat han de ser apropiades per garantir la confidencialitat, la integritat i la disponibilitat de les dades. En aquest sentit, convé tenir en compte les previsions específiques en matèria de videovigilància que conté la Instrucció 1/2009.

En quins casos s'han de fer còpies de seguretat dels tractaments de videovigilància?

D'acord amb la Instrucció 1/2009, si les dades es guarden per un període superior a una setmana, cal fer còpies de seguretat setmanalment.

Normativa aplicable: art. 22 LOPDGDD; Instrucció 1/2009.

5.4.5 Sistemes interns de denúncies

Els col·legis professionals poden crear sistemes d'informació a través dels quals se'ls pugui comunicar la comissió, en el col·legi o en l'actuació de contractistes del col·legi, d'actes o conductes que puguin ser contraris a la normativa general o sectorial aplicable. Aquestes denúncies poden ser anònimes.

En tot cas, cal adoptar les mesures necessàries per preservar la identitat i garantir la confidencialitat de les dades de les persones afectades per la informació subministrada, especialment la de la persona que ha comunicat els fets a l'entitat, i s'ha identificat.

Cal informar els empleats i els contractistes sobre l'existència d'aquests sistemes d'informació.

Només poden accedir a les dades contingudes en aquests sistemes:

- Les persones que exerceixen les funcions de control intern i de compliment, inclosos els encarregats del tractament que es designin eventualment.

- El personal amb funcions de gestió i control de recursos humans únicament quan pugui escaure l'adopció de mesures disciplinàries respecte d'una persona treballadora.
- Altres persones, quan sigui necessari per adoptar mesures disciplinàries o per tramitar els procediments judicials.

Les dades de qui ha fet la comunicació, les dels treballadors i les de tercers s'han de conservar en el sistema de denúncies únicament durant el temps imprescindible per decidir sobre la procedència d'iniciar una investigació sobre els fets denunciats.

En tot cas les dades s'han de suprimir del sistema de denúncies un cop transcorreguts tres mesos des que s'hi van introduir. Tot i això, l'òrgan al qual correspon investigar els fets denunciats les pot continuar tractant amb aquesta finalitat.

Les denúncies que no s'hagin cursat només poden constar al sistema de manera anonimitzada.

No és aplicable l'obligació de bloqueig.



Un treballador d'una empresa que presta serveis al col·legi pot emprar el sistema d'informació de denúncies internes per comunicar al col·legi deficiències en la gestió del servei?

Sí. El sistema de denúncies internes del col·legi també permet informar de conductes o actes en l'actuació dels contractistes que puguin ser contraris a la normativa general o sectorial aplicable.

Normativa aplicable: art. 24 LOPDGDD.

5.4.6 Tractament de dades amb finalitats estadístiques

S'entén per tractament amb finalitats estadístiques qualsevol operació de recollida i tractament de dades personals necessàries per a enquestes estadístiques o per a la producció de resultats estadístics d'acord amb la normativa que regula l'estadística oficial. Aquests resultats es poden utilitzar amb diferents finalitats, inclosa la recerca científica.

El tractament de dades personals amb finalitats estadístiques s'ha de sotmetre al que disposa la seva legislació específica, en especial pel que fa a la regulació del secret estadístic, així com a l'RGPD i a l'LOPDGDD.

L'RGPD preveu que el tractament amb finalitat estadística es pot considerar compatible amb la finalitat inicial del tractament, sempre que s'adoptin garanties adequades per als drets i llibertats de les persones afectades. Si es tracten categories especials de dades cal que el

tractament amb finalitats estadístiques estigui previst expressament en una norma amb rang de llei, que sigui proporcional a l'objectiu perseguit, i que prevegi garanties adequades.

La comunicació de les dades als òrgans competents en matèria estadística només s'entén habilitada per complir una missió realitzada en interès públic o en l'exercici de poders públics conferits al responsable del tractament, quan:

- L'estadística per a la qual es requereix la informació l'exigeix una norma de dret de la Unió.
- Està inclosa en els instruments de programació estadística previstos legalment.

El tractament amb finalitats estadístiques requereix:

- Que les dades personals tractades siguin adequades, pertinents i limitades al que és necessari en relació amb les finalitats per a les quals es tracten.
- Que es garanteixin els drets i les llibertats de les persones afectades, adoptant les mesures tècniques i organitzatives adequades. Aquestes mesures poden incloure la pseudonimització o l'anonimització, sempre que sigui possible.
- Que, a banda del deure d'informació previst a l'article 13 de l'RGPD s'informi la persona de la qual se sol·liciten les dades del següent:
 - El caràcter i la finalitat de l'estadística.
 - El caràcter obligatori o facultatiu de les respostes.
 - La conseqüència de la manca de resposta.
 - Les garanties per preservar l'anonimat (secret estadístic).
- Les categories especials de dades i les dades personals relatives a condemnes i infraccions penals són d'aportació estrictament voluntària i només es poden recollir amb el consentiment previ exprés de les persones afectades.
- El resultat del tractament amb finalitats estadístiques, no pot comportar la difusió de dades personals, sinó de dades agregades que no han de permetre identificar persones físiques. Ni el resultat ni les dades personals que s'empren amb aquesta finalitat no es poden utilitzar per donar suport a mesures o decisions relatives a persones físiques concretes.
- Es poden denegar les sol·licituds d'exercici dels drets de les persones afectades previstos a l'RGPD de les dades emparades per les garanties del secret estadístic.

Normativa aplicable: considerant 162 i arts. 5.1.b), 9.2.j) i 89 RGPD; art. 25 LOPDGDD; LEC.

6. Obligacions del responsable del tractament abans d'iniciar el tractament

Abans d'emprendre qualsevol actuació que impliqui el tractament de dades personals, el col·legi responsable del tractament ha de dur a terme un seguit d'actuacions:

1. Fer una **anàlisi** del “cicle de vida” o recorregut de les dades al llarg del seu tractament, a fi d’identificar:

- Si és necessari un nou tractament.
- Quines dades personals s’han de recollir i per a quina finalitat.
- Com es recolliran (formularis en paper, electrònicament, telefònicament, etc.).
- Qui les tractarà (àrees, departaments, persones usuàries, etc.).
- Com circularan dins l’entitat (en suport paper, telemàticament, etc.).
- A qui se cediran o quines transferències internacionals es faran i com es farà.
- Com es conservaran i, si escau, com i quan es destruiran.

2. Dissenyar el tràmit o servei tenint en compte el dret a la protecció de dades: **protecció de dades des del disseny i protecció de dades per defecte**.

3. Fer una anàlisi de riscos.

4. Fer, si escau, una avaluació d’impacte i una consulta prèvia.

5. Incorporar l’activitat de tractament al **registre** i l’**inventari d’activitats del tractament**.

6.1 La proporcionalitat del tractament; el principi de minimització

D’acord amb el principi de minimització, manifestació del principi de proporcionalitat en l’àmbit de la protecció de dades, les dades personals han de ser adequades, pertinents i limitades al que és necessari en relació amb les finalitats per a les quals es tracten.

Aquest principi comporta:

- Evitar tractaments generalitzats, excessivament amplis, indiscriminats o genèrics.
- No tractar dades personals quan no sigui necessari per assolir una determinada finalitat.
- Quan calgui tractar dades personals, emprar-ne només les mínimes i indispensables.
- Utilitzar, quan sigui possible, el mecanisme de la pseudonimització. Aquest mecanisme permet que les puguin tractar treballadors del col·legi professional o d’un encarregat del tractament i, si escau, terceres persones sense que tinguin accés a les dades identificatives. Tot i continuar essent dades personals, la pseudonimització permet minimitzar els riscos inherents a qualsevol tractament de dades personals.

Normativa aplicable: art. 5.1.c) RGPD.



El col·legi pot recollir qualsevol tipus d'informació sobre els col·legiats?

D'acord amb el principi de minimització de dades, el col·legi només pot recollir i tractar les dades que siguin adequades, pertinents i limitades al necessari en relació amb l'àmbit i les finalitats relacionades amb la seva activitat.

La informació d'un col·legiat es pot limitar, a petició seva, a un simple apartat de correus?

No. D'acord amb la normativa reguladora de les funcions dels col·legis professionals, els col·legis han de tractar altres dades necessàries per mantenir la relació jurídica establerta entre el col·legiat i el col·legi professional.

6.2 La protecció de dades des del disseny i per defecte

La protecció de dades des del disseny comporta que el responsable, tant en el moment de determinar els mitjans de tractament com en el moment del tractament mateix, atenent l'estat de la tècnica, el cost de l'aplicació, la naturalesa, l'àmbit, el context i les finalitats del tractament, així com els riscos que comporta el tractament per als drets i les llibertats de les persones, ha de fer el següent:

- Implantar les mesures tècniques i organitzatives adequades per aplicar de manera efectiva els principis de protecció de dades (com ara la pseudonimització).
- Integrar les garanties necessàries en el tractament, per protegir els drets de les persones afectades.

La protecció de dades per defecte obliga el responsable del tractament a aplicar les mesures tècniques i organitzatives adequades per garantir que, per defecte, el tractament afecta de la menor manera possible les persones afectades. Així, per exemple, implica que:

- Únicament es tracten les dades personals necessàries per a cadascuna de les finalitats específiques del tractament.
- L'abast del tractament és només l'estrictament necessari per assolir la finalitat perseguida.
- Les dades només es conserven durant el termini necessari per assolir la finalitat perseguida.
- Les dades personals no són accessibles a un nombre indeterminat de persones físiques, sense la intervenció de la persona afectada.



Què impliquen la protecció de dades des del disseny i la protecció de dades per defecte, en la posada en marxa d'una app per oferir un nou servei?

Seguint aquests principis, en el moment de dissenyar l'aplicació el col·legi hauria d'analitzar totes les implicacions que pot comportar la seva posada en marxa per a la protecció de dades de les persones afectades: necessitat o no de tractar dades personals, dades concretes que es recullen, termini de conservació, mesures de seguretat, exercici de drets dins de l'aplicació, etc. i incorporar mesures per minimitzar els riscos que es generin (protecció de dades des del disseny).

Alhora, hauria de vetllar, per exemple, perquè la comunicació de dades a terceres persones requereixi un acció positiva de la persona usuària o perquè la geolocalització de les persones usuàries només romangui activa quan l'app estigui en ús, i que això requereixi una acció positiva de la persona usuària (protecció de dades per defecte).

Normativa aplicable: considerant 78 i art. 25 RGD.

6.3 L'anàlisi de riscos

L'anàlisi de riscos és l'instrument a partir del qual el responsable del tractament determina les mesures tècniques i organitzatives necessàries per establir un nivell de seguretat adequat al risc.

Per fer una anàlisi de riscos cal:

- Identificar les amenaces i els riscos: possible fuga d'informació, suplantació d'identitats, errors tècnics que provoquin una duplicació de registres amb informació contradictòria, destrucció de la informació per causes ambientals, talls de subministrament elèctric, etc.
- Avaluar el risc: si hi ha alguna probabilitat que l'amenaça es produeixi i quin seria l'impacte (probabilitat i gravetat del risc).
- Tractar el risc: quines mesures es poden aplicar per reduir la probabilitat que l'amenaça es produeixi i l'impacte que causaria en la persona afectada.

L'anàlisi de riscos s'ha de fer abans d'iniciar el tractament i s'ha de revisar periòdicament i sempre que es produeixi algun canvi substancial en el tractament.

Per identificar i avaluar els riscos s'ha de tenir especialment en compte si el tractament pot comportar alguna d'aquestes situacions:

- Discriminació, usurpació d'identitat o frau, pèrdues financeres, dany per a la reputació, pèrdua de confidencialitat de dades subjectes al secret professional,

reversió no autoritzada de la pseudonimització o qualsevol altre perjudici econòmic, moral o social significatiu per als afectats.

- Privació als afectats dels seus drets i llibertats o que se'ls pugui impedir exercir el control sobre les seves dades personals.
- Tractament no merament incidental o accessori de les categories especials de dades, de dades relacionades amb infraccions o condemnes penals o relacionades amb la comissió d'infraccions administratives.
- Avaluació d'aspectes personals de les persones afectades amb la finalitat de crear o utilitzar els seus perfils personals, en particular mitjançant l'anàlisi o la predicció d'aspectes referits al seu rendiment a la feina, la seva situació econòmica, la seva salut, les seves preferències o interessos personals, la seva fiabilitat o comportament, la seva solvència financera, la seva localització o els seus moviments.
- Tractament de dades de grups d'afectats en una situació d'especial vulnerabilitat i, en particular, de menors d'edat i persones amb discapacitat.
- Tractament massiu que impliqui un gran nombre d'afectats o comporti la recollida d'una gran quantitat de dades personals.
- Tractament de dades personals que hagin de ser objecte d'una transferència, amb caràcter habitual, a tercers estats o organitzacions internacionals respecte dels quals no s'hagi declarat un nivell adequat de protecció.
- Qualsevol altra que, a parer del responsable o de l'encarregat, pugui tenir rellevància i, en particular les previstes en codis de conducta i estàndards definits per esquemes de certificació.

L'anàlisi de riscos s'ha de fer en tots els tractaments, amb independència que el tractament s'hagi de sotmetre o no a una avaluació d'impacte sobre la protecció de dades. Si es fa una avaluació d'impacte sobre la protecció de dades, l'anàlisi de riscos n'ha de formar part.

Pel que fa a les mesures de seguretat que calgui adoptar per fer front als riscos que s'identifiquin en l'anàlisi, ens remetem a l'apartat 7.7.5 d'aquesta guia.



Quina metodologia pot seguir un col·legi professional per avaluar els riscos d'un tractament?

D'acord amb la disposició addicional primera de l'LOPDGDD, l'ENS determina les mesures de seguretat que cal implantar per protegir les dades personals a les entitats del sector públic. L'ENS només exigeix l'ús d'una metodologia d'anàlisi de riscos amb reconeixement internacional sense citar-ne cap de concreta.

La metodologia Magerit és una d'aquestes metodologies. El CCN-Cert (Centro Criptológico Nacional) ofereix diverses **eines** que poden ser útils per a l'avaluació de riscos.

Es poden instal·lar programes informàtics que tractin dades personals en dispositius que són propietat dels treballadors del col·legi, per tal que puguin desenvolupar les tasques que tenen encomanades fora de les instal·lacions del col·legi?

Atès que aquesta actuació pot comportar riscos tant per a la seguretat de les dades personals de les quals és responsable el col·legi, com per a la privacitat dels seus treballadors, com a pas previ a autoritzar-ne l'ús (decisió que correspon al col·legi), cal fer una anàlisi de riscos i implementar les mesures tècniques i organitzatives apropiades per fer front als riscos detectats.

A l'efecte de garantir la implementació d'aquestes mesures, és recomanable recórrer a eines de gestió centralitzada de dispositius mòbils (MDM). En l'ús d'aquestes eines cal respectar la privacitat dels treballadors.

Normativa aplicable: art. 32 RGPD; art. 28 LOPDGDD; ENS.

6.4 L'avaluació d'impacte i la consulta prèvia

Avaluació d'impacte relativa a la protecció de dades (AIPD)

Una avaluació d'impacte en la protecció de dades (AIPD) és un procediment que pretén identificar i controlar el riscs per als drets i les llibertats de les persones, associats a un tractament de dades.

El responsable té l'obligació de fer una avaluació de l'impacte en la protecció de dades abans del tractament, quan sigui probable que per la seva naturalesa, abast, context o fins suposi un alt risc per als drets i llibertats de les persones físiques, especialment quan s'utilitzin noves tecnologies. Per tant, sempre cal verificar aquest aspecte a l'hora de determinar la necessitat de fer o no una AIPD.

Entre d'altres supòsits, d'acord amb l'RGPD cal fer una avaluació d'impacte en els supòsits següents:

- Avaluació sistemàtica i exhaustiva d'aspectes personals de persones físiques basada en un tractament automatitzat, com l'elaboració de perfils, sobre la base de la qual es prenen decisions que produeixen efectes jurídics per a les persones físiques o que les afecten significativament de manera similar.
- Tractament a gran escala de les categories especials de dades, o de les dades personals relatives a condemnes i infraccions penals.

A l'efecte de determinar si el tractament es fa a gran escala es poden tenir en compte els elements següents:

- El nombre de persones afectades, ja sigui en termes absoluts o com a proporció d'una determinada població.
 - El volum i la varietat de dades tractades.
 - La durada o permanència de l'activitat de tractament.
 - L'extensió geogràfica de l'activitat de tractament.
- Observació sistemàtica a gran escala d'una zona d'accés públic.

Aquesta no és una llista tancada.

Per altra banda, i d'acord amb les previsions de l'RGPD, l'Autoritat Catalana de Protecció de Dades ha elaborat i publicat al seu web [una llista de tipus de tractament](#), no exhaustiva, per facilitar als responsables dels tractaments la identificació dels tractaments que poden requerir una avaluació d'impacte. En la majoria dels casos en què el tractament compleixi amb dos o més criteris de la llista, cal fer una AIPD. Com més criteris reuneixi el tractament en qüestió, més gran és el risc que comporta el tractament i més certa es tindrà que cal fer una AIPD.

Actualment s'identifiquen els criteris següents:

- Tractaments que impliquen perfilat o valoració de subjectes, inclosa la recollida de dades del subjecte en múltiples àmbits de la seva vida (rendiment en el treball, personalitat i comportament), que cobreixin diversos aspectes de la seva personalitat o sobre els seus hàbits.
- Tractaments que impliquen la presa de decisions automatitzades o que contribueixin en gran mesura a la presa d'aquestes decisions, incloent qualsevol tipus de decisió que impedeixi a una persona afectada exercir un dret o tenir accés a un bé o un servei o formar part d'un contracte.
- Tractaments que impliquin l'observació, monitorització, supervisió, geolocalització o control de la persona afectada de forma sistemàtica i exhaustiva, inclosa la recollida de dades i metadades a través de xarxes, aplicacions o en zones d'accés públic, així com el processament d'identificadors únics que permeten la identificació d'usuaris de serveis de la societat de la informació com poden ser els serveis web, TV interactiva, aplicacions mòbils, etc.
- Tractaments que impliquen l'ús de categories especials de dades a què fa referència l'article 9.1 de l'RGPD, dades relatives a condemnes o infraccions penals a què es refereix l'article 10 de l'RGPD o dades que permeten determinar la situació financera o de solvència patrimonial o deduir informació sobre les persones relacionada amb categories especials de dades.

- Tractaments que impliquin l'ús de dades biomètriques amb el propòsit d'identificar de manera única una persona física.
- Tractaments que impliquen l'ús de dades genètiques per a qualsevol fi.
- Tractaments que impliquen l'ús de dades a gran escala.
- Tractaments que impliquen l'associació, combinació o enllaç de registres de bases de dades de dos o més tractaments amb finalitats diferents o per responsables diferents.
- Tractaments de dades de subjectes vulnerables o en risc d'exclusió social, incloses dades de menors de 14 anys, majors d'edat amb algun grau de discapacitat, discapacitats, persones que accedeixen a serveis socials i víctimes de violència de gènere, així com els seus descendents i persones que estiguin sota la seva guàrdia i custòdia.
- Tractaments que impliquen la utilització de noves tecnologies o un ús innovador de tecnologies consolidades, inclosa la utilització de tecnologies a una nova escala, amb un nou objectiu o combinades amb altres, de manera que suposi noves formes de recollida i utilització de dades amb risc per als drets i llibertats de les persones.
- Tractaments de dades que impedeixen a les persones afectades exercir els seus drets, utilitzar un servei o executar un contracte, com ara tractaments en què les dades han estat recopilades per un responsable diferent al que les ha de tractar i en què és d'aplicació alguna de les excepcions sobre la informació que s'ha de proporcionar a les persones afectades segons l'article 14.5 (b, c i d) de l'RGPD.

Com a excepció, no cal fer una avaluació d'impacte relativa a la protecció de dades si el tractament està previst en una disposició normativa i durant la tramitació del projecte normatiu ja es va sotmetre a una AIPD.

L'obligació de fer l'avaluació d'impacte correspon al responsable del tractament, amb la col·laboració de l'encarregat del tractament i amb l'assessorament del delegat de protecció de dades.

L'avaluació ha d'incloure, com a mínim:

- Una descripció sistemàtica de les operacions de tractament previstes i de les finalitats del tractament, inclòs, si escau, l'interès legítim perseguit.
- Una avaluació de la necessitat i la proporcionalitat de les operacions de tractament, en relació amb la seva finalitat.
- Una avaluació dels riscos per als drets i les llibertats de les persones afectades.
- Les mesures previstes per afrontar els riscos, incloses garanties, mesures de seguretat i mecanismes que garanteixen la protecció de dades personals i per demostrar la conformitat amb la normativa de protecció de dades, tenint en compte els drets i els interessos legítims de les persones afectades.

Sobre aquesta qüestió es recomana consultar la [Guia pràctica sobre l'avaluació d'impacte relativa a la protecció de dades](#) i la [Plantilla d'avaluació d'impacte relativa a la protecció de dades](#) elaborades per aquesta Autoritat.

Per altra banda, al web de l'APDCAT també es pot descarregar una [aplicació](#) per fer l'avaluació d'impacte relativa a la protecció de dades.

Consulta prèvia

Si de l'avaluació d'impacte en la protecció de dades en resulta que el tractament previst pot infringir l'RGPD o comportaria un alt risc si no es prenen mesures per mitigar-lo, el responsable ha de formular una consulta prèvia a l'Autoritat Catalana de Protecció de Dades, a través del tràmit electrònic que figura a la seu electrònica.

La consulta ha d'anar acompanyada, com a mínim, de la informació següent:

- L'avaluació d'impacte realitzada.
- Si escau, les responsabilitats respectives del responsable, dels corresponsables i dels encarregats implicats en el tractament, especialment en cas de tractament dins d'un grup empresarial.
- Les finalitats i els mitjans del tractament previst.
- Les mesures i les garanties establertes per protegir els drets i les llibertats de les persones afectades.
- Les dades de contacte del delegat de protecció de dades.
- Qualsevol altra informació que sol·liciti l'APDCAT.

L'Autoritat ha d'assessorar per escrit el responsable en el termini de vuit setmanes des de la sol·licitud de consulta, prorrogable a sis setmanes més indicant els motius. L'Autoritat pot fer ús, si escau, de tots els poders d'investigació, correctius, d'autorització i consultius que li confereix l'RGPD, entre els quals hi ha prohibir l'operació de tractament.



Un col·legi professional ha de fer una avaluació d'impacte si vol utilitzar dades biomètriques per controlar l'entrada a les instal·lacions del col·legi?

En el cas que la utilització de les dades biomètriques es vulgui iniciar o s'hagi iniciat amb posterioritat al 25 de maig de 2018, caldria fer una avaluació d'impacte relativa a la protecció de dades d'aquesta part del tractament. I si del resultat de l'avaluació en resulta una situació d'alt risc, s'hauria de plantejar una consulta prèvia a l'APDCAT d'acord amb l'article 36 de l'RGPD. Si el tractament s'ha iniciat abans de la data esmentada, tot i no ser obligatori seria recomanable.

Els col·legis professionals han de publicar les AIPD que fan?

L'RGPD no estableix l'obligació de publicar les AIPD, tot i que pot ser una bona pràctica fer-ho, de manera completa o parcial, extraient-ne les parts que puguin afectar els drets i llibertats de les persones o la seguretat del tractament. En qualsevol

cas, els responsables l'han de comunicar a l'APDCAT si fan una consulta prèvia, o si els ho sol·licita l'Autoritat.

Cal trametre a l'Autoritat Catalana de Protecció de Dades les avaluacions d'impacte relatives a la protecció de dades?

No. Només s'han de comunicar a l'APDCAT en cas que es faci una consulta prèvia, o si ho sol·licita l'Autoritat.

Normativa aplicable: considerants 84, 90 a 96; arts. 35, 36 i 58 RGPD; art. 28 LOPDGDD.

6.5 El registre i l'inventari d'activitats del tractament

El registre d'activitats del tractament és un instrument documental que ha de permetre tenir una imatge actualitzada dels tractaments que duu a terme el col·legi professional. És essencial per a la gestió de riscos, pel compliment dels principis i les obligacions i perquè l'autoritat de control el pugui supervisar.

L'RGPD exceptua de l'obligació de portar el registre d'activitats del tractament els responsables amb menys de 250 empleats que només duguin a terme tractaments ocasionals que no comportin el tractament de categories especials de dades o relatives a infraccions i condemnes penals i que no puguin suposar un risc per als drets i llibertats de les persones afectades. No obstant això, els col·legis professionals, sempre hauran de portar aquest registre, atesa l'amplitud dels tractaments que han de realitzar i el seu caràcter no ocasional.

El registre d'activitats de tractament, que ha de constar en format electrònic, ha d'incloure la informació següent:

- Nom i dades de contacte del responsable i, si escau, del corresponent, així com del delegat de protecció de dades.
- Finalitats del tractament.
- Descripció de les categories de persones afectades i les categories de dades personals tractades.
- Categories de destinataris als quals es preveu comunicar les dades personals, inclosos els de tercers països o organitzacions internacionals, si escau.
- Si escau, transferències internacionals de dades previstes, amb identificació del tercer país o organització internacional de destí. Si es basa en garanties adequades, també s'ha d'identificar la documentació on consten.
- Terminis previstos per suprimir les dades, quan sigui possible.
- Descripció general de les mesures tècniques i organitzatives de seguretat, quan sigui possible.

Els col·legis professionals han de fer públic a la seu electrònica o al web un inventari de les seves activitats de tractament, accessible per mitjans electrònics. Hi ha de constar la informació del registre d'activitats del tractament i la seva base legal, com a mínim per als tractaments que es relacionin amb l'exercici de potestats de dret públic.

El registre i l'inventari s'han de mantenir actualitzats, abans d'iniciar el tractament i cada cop que es produeixi un canvi significatiu en el tractament. S'ha de comunicar al delegat de protecció de dades qualsevol addició, modificació o exclusió en el seu contingut.

L'APDCAT ha desenvolupat i publicat al seu web una **aplicació** per crear, mantenir i gestionar el registre de les activitats de tractament, amb la finalitat d'oferir suport als responsables del tractament. L'aplicació permet donar d'alta les diferents activitats de tractament, així com modificar-les i donar-les de baixa quan calgui. També permet generar un document amb les activitats de tractament que s'han inclòs al registre, per poder-lo publicar, si escau.

El registre ha d'estar a disposició de l'Autoritat Catalana de Protecció de Dades per a l'exercici de les seves funcions com a autoritat de control.

Quan el col·legi professional actuï com encarregat del tractament, també ha de portar un registre d'activitats del tractament diferenciat, en el qual hi consti:

- El nom i les dades de contacte de l'encarregat i de cada responsable per compte del qual actua l'encarregat i, si escau, del representant del responsable o de l'encarregat i del delegat de protecció de dades.
- Les categories de tractaments efectuats per compte de cada responsable.
- Les transferències internacionals de dades personals previstes, inclosa la identificació del tercer país o organització internacional de destí. Si es basa en garanties adequades, també s'ha d'identificar la documentació on consten.
- La descripció general de les mesures tècniques i organitzatives de seguretat (quan sigui possible).



Com pot el col·legi organitzar el registre d'activitats del tractament?

Una possibilitat per organitzar aquest registre és partir dels fitxers que el col·legi havia notificat al Registre de Protecció de Dades de Catalunya, i detallar totes les operacions que s'efectuen sobre cada conjunt estructurat de dades.

També es pot organitzar al voltant d'operacions de tractament concretes, vinculades a una finalitat bàsica comuna de totes elles (per exemple "registre de col·legiats", "gestió comptable" o "gestió de recursos humans i nòmines"), o bé d'acord amb altres criteris diferents.

Un col·legi professional es planteja comunicar a una associació mundial de professionals dades de representants d'associacions culturals del municipi, amb el seu consentiment. Això podria afectar la informació del registre d'activitats de tractament?

Sí. El registre d'activitats de tractament ha d'incloure quins són els destinataris de les dades, inclosos els de tercers països, així com les transferències internacionals de dades que es puguin produir. Si el registre no ho preveia, s'hi hauria d'incorporar, atès que suposa un canvi significatiu del tractament inicial.

Els tractaments que duu a terme la comissió de cultura del col·legi professional i dels quals n'és responsable la comissió de cultura, s'han d'incloure en el registre d'activitats del tractament del col·legi?

Els tractaments que duu a terme s'han d'incloure al registre d'activitats de tractament del responsable del tractament. No obstant això, res impedeix que dins d'una mateixa organització tots els tractaments puguin formar part d'un mateix registre, sempre que quedi clar qui és el responsable de cadascun.

Com s'ha de publicar l'inventari d'activitats de tractament per mitjans electrònics?

Els col·legis professionals han de fer públic l'inventari a la seva seu electrònica o al seu web i fer-hi constar la informació del registre d'activitats del tractament i la seva base legal. Això, com a mínim per als tractaments relacionats amb l'exercici de potestats de dret públic, tant si actua com a responsable, com si ho fa com a encarregat del tractament.

Cal notificar a l'Autoritat Catalana de Protecció de Dades els tractaments inscrits al registre d'activitats de tractament?

No. El registre ha d'estar a disposició de l'Autoritat Catalana de Protecció de Dades per a l'exercici de les seves funcions com a autoritat de control, però no cal notificar els tractaments que s'hi inscriuen.

Normativa aplicable: considerant 82, art. 30 RGPD; 31, 77.1.g) i DF 11a LOPDGDD; 6.bis LT.

7. Obligacions del responsable del tractament i de l'encarregat durant el tractament

Les persones afectades disposen d'un seguit de drets durant el tractament de les dades:

- Dret a ser informades sobre el tractament i els seus principals elements
- Dret d'accés
- Dret de rectificació
- Dret de supressió
- Dret a la limitació del tractament

- Dret a la portabilitat
- Dret d'oposició
- Dret a no ser objecte de decisions automatitzades

A més, el responsable del tractament ha de complir tot un seguit d'obligacions i garanties, encaminades a assegurar l'adequació del tractament a la normativa vigent. Aquestes obligacions són d'aplicació durant la recollida, l'emmagatzematge, la utilització o la comunicació de les dades personals i, en algun cas (deure de confidencialitat), fins i tot després que finalitzi la relació jurídica. Aquestes obligacions són:

- Formalitzar l'encàrrec del tractament.
- Nomenar el delegat de protecció de dades.
- Complir el règim de transferències internacionals de dades.
- Garantir la seguretat de les dades: integritat i confidencialitat.
- Aprovar una política de protecció de dades.

A més, en virtut del principi de responsabilitat proactiva, el responsable del tractament ha d'adoptar qualsevol altra mesura per garantir el compliment dels principis de la normativa de protecció de dades i fer front als riscos que es puguin generar per als drets i llibertats de les persones físiques. En especial, destaquen la promoció i/o adhesió als codis de conducta i l'obtenció de certificats, segells o marques en matèria de protecció de dades.

7.1 La informació a les persones afectades

Les persones afectades tenen dret a ser informades sobre les condicions en què el responsable durà a terme el tractament de les seves dades, sense necessitat de demanar-ho.

Correspon al responsable del tractament complir aquesta obligació i estar en condicions de demostrar que l'ha complert.

La informació ha de ser:

- Concisa, transparent, intel·ligible i de fàcil accés.
- En un llenguatge clar i senzill, especialment quan la informació s'adreça a un menor. S'han d'evitar les fórmules enrevessades i que incorporin remissions a textos legals o que no es distingeixin de la informació sobre altres qüestions.
- Per escrit o per altres mitjans, inclosos els electrònics.
- Facilitada de manera que el responsable pugui acreditar que l'ha facilitat.

Pel que fa al contingut de la informació, s'ha de diferenciar si les dades s'obtenen de la persona afectada o no.

Si les dades s'obtenen de la persona afectada, en el moment en què s'obtenen se l'ha d'informar sobre:

- La identitat i dades de contacte del responsable i, si escau, del seu representant.
- Les dades de contacte del delegat de protecció de dades.
- Les finalitats i la base jurídica del tractament.
- Els interessos legítims perseguits en què es fonamenta el tractament, si escau.
- Els destinataris o categories de destinataris de les dades, si escau.
- La intenció de transferir les dades a un tercer país o a una organització internacional i l'instrument per fer-ho, així com el lloc on es pot obtenir una còpia de les garanties adequades, si escau.
- El termini durant el qual es conservaran les dades, o els criteris per determinar-lo.
- El dret a sol·licitar l'accés a les dades, la rectificació o la supressió de les dades, la limitació del tractament, l'oposició al tractament i la portabilitat de les dades.
- El dret a retirar en qualsevol moment el consentiment que s'ha prestat, si el tractament es fonamenta en aquesta base jurídica.
- Si la comunicació de dades és un requisit legal o contractual o un requisit necessari per subscriure un contracte, i si la persona afectada està obligada a facilitar les dades i les conseqüències de no facilitar-les.
Igualment, quan es recullen dades relatives a la ideologia, la religió o les creences, cal advertir expressament la persona afectada del seu dret a no facilitar aquests tipus de dades.
- El dret a presentar una reclamació davant una autoritat de control.
- L'existència de decisions automatitzades, inclosa l'elaboració de perfils, i la informació sobre la lògica aplicada i les seves conseqüències.

Si les dades no s'obtenen de la persona afectada, a més dels aspectes que s'acaben de relacionar també se l'ha d'informar de:

- Les categories de dades personals que es tracten.
- La font d'on procedeixen les dades personals.

En ambdós casos, l'LOPDGDD ha previst la possibilitat d'utilitzar un mecanisme de doble capa per informar les persones afectades. A la primera capa, que es pot incloure per exemple als formularis de recollida de dades, hi ha de constar la informació bàsica juntament amb una remissió a una adreça electrònica o altre mitjà que permeti a la persona afectada accedir de manera senzilla a la segona capa amb la resta d'informació prevista a l'RGPD.

Quan les dades s'obtenen directament de la persona afectada, la primera capa ha d'incloure:

- La identitat del responsable del tractament i del seu representant, si escau.

- La finalitat del tractament.
- La possibilitat d'exercir els drets

Quan les dades no s'obtenen directament de la persona afectada, la primera capa també ha d'incloure:

- Les categories de dades objecte de tractament.
- Les fonts de les quals procedeixen les dades.

La informació s'ha de posar a disposició de les persones afectades en el **termini** següent:

- Si les dades s'obtenen de la persona afectada, en el moment en què se sol·liciten les dades.
- Si les dades no s'obtenen de la persona afectada, en un termini raonable, no superior a un mes, tret que calgui fer-ho amb anterioritat perquè hi concorre alguna de les causes següents:
 - Si les dades s'han d'utilitzar per comunicar-se amb la persona afectada, cal informar abans o en la primera comunicació amb ella.
 - Si està previst comunicar-les a un altre destinatari, cal informar abans o en el moment d'aquesta comunicació.

Excepcions al deure d'informar:

a) Quan les dades s'obtenen de la persona afectada, no cal informar si:

- La persona afectada ja disposa de la informació.
- Pot afectar la defensa nacional, la seguretat pública o la persecució d'infraccions penals.

b) Quan les dades no s'obtenen de la persona afectada, no cal informar si:

- És impossible o suposa un esforç desproporcionat (en particular, en cas de tractaments amb finalitats d'arxiu o estadístics o d'investigació científica o històrica), o impossibilita o obstaculitza greument els objectius del tractament.
- Hi ha una previsió legal expressa del tractament (obtenció o comunicació que ha comportat la recollida de les dades).
- Hi ha una obligació de secret legal.
- Pot afectar la defensa nacional, la seguretat pública o la persecució d'infraccions penals.

També cal tenir en compte que la Llei orgànica 7/2021, estableix que no s'ha d'informar de les comunicacions de dades que es facin per atendre els requeriments d'informació dels òrgans judicials, el ministeri fiscal i la policia judicial, per a la investigació o l'enjudiciament

d'infraccions penals o l'execució de les penes, o amb finalitats de prevenció i protecció davant un perill real i greu per a la seguretat pública.

En els annexos d'aquesta guia s'ofereixen models de clàusules informatives que, en qualsevol cas, cal adaptar a les circumstàncies del tractament concret que es pretén fer:

- Annex 1: **Model de clàusula informativa per a documents de recollida de dades pel col·legi professional**
- Annex 2: **Model de clàusula informativa per actualitzar les dades que apareixen a la llista o guia de persones col·legiades**

Sobre aquesta qüestió, es recomana consultar la **Guia per al compliment del deure d'informar a l'RGPD** publicada per aquesta Autoritat.



Quina informació han de donar els col·legis professionals als col·legiats, sobre les dades recollides per elaborar la guia o la llista professional i la seva publicació posterior?

El col·legi ha d'informar dels aspectes previstos als articles 13 i 14 de l'RGPD i a l'article 11 de l'LOPDGDD. En especial, convé informar sobre les dades que es difondran en compliment de l'obligació de posar a disposició de les persones usuàries i consumidores destinatàries dels serveis professionals determinada informació a través de la finestra única.

Quin mitjà pot utilitzar el col·legi professional per complir amb el deure d'informació prèviament a la recollida de dades?

El deure d'informació es pot complir de diverses maneres, com ara incloure la clàusula informativa en els formularis, impresos o qüestionaris emprats en la recollida de dades. Si no es poden emprar formularis, i les circumstàncies ho justifiquen, es poden col·locar cartells informatius en els punts de recollida de les dades, que siguin clarament visibles i accessibles per als col·legiats. La informació inclosa als cartells ha de ser completa i detallada. En tot cas, s'ha de complir amb el que disposen els articles 13 a 14 de l'RGPD i, si escau, l'article 11 de l'LOPDGDD.

Si, en el marc d'un procediment en exercici de les seves funcions públiques, un col·legi professional ha de consultar dades que ja estaven en poder d'una administració pública, n'ha d'informar les persones afectades?

Sí. Si a l'empara de l'article 28.2 de l'LPAC, un col·legi professional consulta dades que estiguin en poder d'una altra administració, ha d'informar les persones afectades sobre aquesta consulta i de la possibilitat d'oposar-s'hi.

Quan no cal demanar el consentiment, s'ha d'informar igualment les persones afectades?

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

Cal incloure la clàusula informativa en tots els correus electrònics que envia el col·legi professional als col·legiats?

No. No és obligatori, si ja es va informar en el moment de la recollida de les dades. Però pot ser recomanable incloure-la, així com tenir-la a disposició de les persones afectades a través del web, per tal que les persones que es relacionen amb el col·legi coneguin on són les seves dades, el tractament que se'n fa, qui n'és el responsable i com poden exercir els seus drets.

Normativa aplicable: considerants 58, 60 a 62 i arts.12, 13 i 14 RGPD; art. 11 i DA 14a LOPDGDD; art. 24 LOPD; art. 7 de la Llei orgànica 7/2021.

7.2 L'atenció dels drets de les persones afectades

7.2.1 Aspectes comuns

L'RGPD reconeix a la persona afectada el poder de control sobre les seves dades personals i li atorga la possibilitat d'exercir els drets d'accés, rectificació, supressió, limitació del tractament, portabilitat de les dades, oposició i a no ser objecte de decisions individuals automatitzades.

També estableix el dret a ser informat sobre el tractament. No obstant això, atès que aquest dret no requereix una sol·licitud de les persones afectades sinó que el responsable està obligat a complir-lo directament sense que calgui sol·licitar-ho, s'analitza de manera específica a l'apartat 7.1 d'aquesta guia.

El responsable del tractament ha de facilitar l'exercici d'aquests drets i ha d'adoptar les mesures oportunes per garantir que les persones de la seva organització que tenen accés a dades personals i les que atenen el públic puguin informar del procediment que han de seguir les persones afectades per exercir els seus drets.

Es tracta de drets personalíssims. Per tant, els ha d'exercir la mateixa persona afectada o un tercer per representació, davant el responsable del tractament.

Sol·licitud:

- La sol·licitud es pot presentar per qualsevol mitjà que permeti deixar constància de la identitat de la persona que la formula i de la seva presentació.

S'ha de possibilitar la presentació de sol·licituds per mitjans electrònics, especialment quan les dades es tracten per aquests mitjans. En aquest cas, si és possible, la informació s'ha de facilitar en aquest format, llevat que la persona afectada demani que se li lliuri d'una altra manera.

- El responsable ha de prendre les mesures raonables per verificar la identitat de la persona afectada que exerceix un dret. Si té dubtes raonables quant a la identitat de qui presenta la sol·licitud, pot demanar informació addicional per confirmar-la.
- El responsable no està obligat a mantenir, obtenir o tractar informació addicional per tal d'identificar la persona afectada amb l'única finalitat de poder atendre les sol·licituds d'exercici de drets. Si les dades personals que tracta no li permeten relacionar la informació amb la persona afectada que exerceix el dret, l'ha d'informar sobre aquesta circumstància. En aquest cas, els drets reconeguts per l'RGPD no són d'aplicació, tret que la persona afectada faciliti informació addicional que en permeti la identificació.
- En cas que el responsable no cursi la sol·licitud de la persona afectada en el termini d'un mes des que l'ha rebut, l'ha d'informar de les raons per les quals no ha actuat, així com de la possibilitat de presentar una reclamació davant l'autoritat de control i d'exercir accions judicials.
- L'exercici de qualsevol d'aquests drets té caràcter gratuït. No obstant això, si les sol·licituds són infundades o excessives, especialment perquè són repetitives, el responsable pot cobrar un cànon raonable segons els costos administratius que es derivin de facilitar la informació, la comunicació o l'actuació demanada, o es pot negar a actuar davant la sol·licitud. Correspon al responsable demostrar el caràcter infundat o excessiu de la sol·licitud. A aquests efectes, es pot considerar repetitiu exercir el dret d'accés més d'una vegada en el termini de sis mesos, tret que hi hagi una causa legítima per fer-ho.
- El responsable pot comptar amb la col·laboració dels encarregats per atendre les sol·licituds d'exercici dels drets. Aquesta col·laboració s'ha d'establir en el contracte d'encàrrec de tractament.
- S'ha d'atendre la sol·licitud d'exercici del dret sense dilació indeguda i en qualsevol cas en el termini màxim d'un mes des que es va rebre, prorrogable dos mesos més si cal, segons la complexitat i el nombre de sol·licituds. En cas de pròrroga, se n'ha d'informar la persona afectada dins del termini del primer mes, i indicar els motius de la dilació.

Als [annexos 3, 4, 5, 6 i 7](#) d'aquesta guia podeu trobar models per exercir els drets d'accés, rectificació, supressió, oposició i limitació.

Limitació dels drets:

Aquests drets només es poden limitar mitjançant una norma amb rang de llei o el dret de la Unió, que respecti els drets i les llibertats fonamentals i sigui una mesura necessària i proporcionada en una societat democràtica per salvaguardar:

- La seguretat de l'Estat.
- La defensa.
- La seguretat pública.
- La prevenció, investigació, detecció o enjudiciament d'infraccions penals o l'execució de sancions penals.
- Altres objectius importants d'interès públic general de la Unió Europea o d'un estat membre (econòmic, financer, fiscal, pressupostari i monetari, sanitat pública, seguretat social).
- La protecció de la independència judicial i dels procediments judicials.
- La prevenció, investigació, detecció i enjudiciament d'infraccions de normes deontològiques en les professions regulades.
- La supervisió, inspecció o reglamentació vinculada amb l'exercici de l'autoritat pública en qualsevol dels supòsits esmentats en els apartats anteriors.
- La protecció de la persona afectada o dels drets i les llibertats d'altres.
- L'execució de demandes civils.

Així, per exemple, l'article 23 de l'LOPD, que l'LOPDGDD manté vigent, estableix que es pot denegar l'exercici dels drets d'accés, rectificació o cancel·lació (supressió):

- En funció dels perills que es puguin derivar per a la defensa de l'Estat o la seguretat pública, la protecció dels drets i les llibertats de tercers o les necessitats de les investigacions que s'estiguin duent a terme.
- Quan els responsables dels fitxers de la hisenda pública considerin que això pot obstaculitzar les actuacions administratives tendents a assegurar el compliment de les obligacions tributàries i, en tot cas, quan la persona afectada estigui essent objecte d'actuacions inspectores.

Reclamació de tutela de drets

Per exercir els seus drets, el ciutadà s'ha d'adreçar al responsable del tractament. Si la sol·licitud no es respon en el termini d'un mes (llevat que hagi estat ampliat), o es denega 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.

La tutela dels drets reconeguts per l'RGPD 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.

L'Autoritat trasllada la reclamació al responsable del tractament i, un cop rebudes les alegacions dins del termini legalment establert i practicades totes les proves, ha de dictar resolució i notificar-la, en el termini de 6 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.

Quan la resolució de la reclamació és estimatòria, l'Autoritat Catalana de Protecció de Dades requereix el responsable del tractament perquè en el termini dels 10 dies següents a la notificació, faci efectiu l'exercici del dret reclamat.



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

Sí, l'exercici del dret no es pot denegar pel sol motiu que la persona afectada opti per un altre mitjà.

El responsable del tractament pot excloure la possibilitat d'exercir els drets a través del correu electrònic?

No, la persona interessada pot demanar que el dret d'accés es faci efectiu a través del correu electrònic i té dret a rebre la informació en aquest mateix format. Ara bé, cal tenir en compte que si el col·legi ofereix un determinat sistema per fer efectiu el dret d'accés i la persona afectada el rebutja, el col·legi no ha de respondre dels riscos per a la seguretat de la informació que poden derivar de l'elecció.

Cal respondre la sol·licitud quan no es disposa de dades o ja s'han destruït?

Sí, les sol·licituds d'exercici dels drets sempre s'han de respondre de manera expressa sense dilació indeguda i dins el termini màxim d'un mes, llevat que se n'hagi acordat la pròrroga.

Normativa aplicable: arts. 11, 12, 23 i 77 RGPD; arts. 12 a 18 i DA 14a LOPDGDD; art. 23 LOPD; arts. 5.b) i 16 LACPD; art. 117 i s. RLOPD.

7.2.2 Dret d'accés

La persona afectada té dret a saber si el responsable del tractament tracta les seves dades personals i, si és així, té dret a accedir a aquestes dades i a obtenir la informació següent:

- Les finalitats del tractament.
- Les categories de dades personals que es tracten.
- Els destinataris o les categories de destinataris als quals s'han comunicat o es comunicaran les dades.
- El termini previst de conservació de les dades personals o els criteris utilitzats per determinar-lo.

- El dret a sol·licitar al responsable del tractament la rectificació o la supressió de les dades, la limitació del tractament o el dret a oposar-s'hi.
- El dret a presentar una reclamació davant l'autoritat de control competent.
- L'origen de les dades, quan no s'han obtingut de la persona afectada.
- L'existència de decisions automatitzades, inclosa l'elaboració de perfils, la lògica aplicada i les conseqüències d'aquest tractament.
- En cas de transferències internacionals de dades, les garanties adequades que s'ofereixen.

A més, té dret a obtenir una còpia gratuïta de les dades objecte del tractament, sempre que no afecti negativament els drets i les llibertats d'altres. Per a còpies posteriors, es pot establir un cànon segons els costos administratius.

El dret d'accés es pot exercir en relació amb dades concretes o amb la totalitat de les dades sotmeses a tractament.

En casos d'especial complexitat, el responsable del tractament pot facilitar a la persona afectada una llista dels seus tractaments i demanar-li que especifiqui respecte de quins exerceix el seu dret.

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 tractament.

Si se sol·licita per mitjans electrònics, la persona afectada té dret a rebre la informació en aquest mateix format.

Si el col·legi ofereix un determinat sistema per fer efectiu el dret d'accés i la persona afectada el rebutja, el col·legi no ha de respondre dels riscos per a la seguretat de la informació que poden derivar de l'elecció.



Com pot un col·legiat conèixer la informació que té un col·legi professional sobre la seva persona?

El col·legiat pot conèixer aquesta informació exercint el dret d'accés, mitjançant una sol·licitud adreçada al col·legi corresponent.

És possible denegar l'exercici del dret d'accés per la dificultat o l'elevat cost que pot suposar al col·legi professional?

Quan les sol·licituds siguin manifestament infundades o excessives, especialment pel seu caràcter repetitiu, el responsable pot cobrar un cànon o inadmetre la sol·licitud. A aquests efectes, es pot considerar repetitiu exercir el dret d'accés més d'una vegada en el termini de sis mesos, tret que hi hagi una causa legítima per fer-ho.

Si la persona afectada tria un mitjà diferent al que se li ofereix, que suposa un cost desproporcionat, la sol·licitud s'ha de considerar excessiva, per la qual cosa la persona afectada ha d'assumir l'excés de costos que comporta la seva tria.

Els hereus d'una persona col·legiada difunta poden exercir, en el seu nom, el dret d'accés a les seves dades en poder del col·legi?

La normativa de protecció de dades no és aplicable al tractament de dades de persones difuntes. Ara bé, l'LOPDGDD preveu expressament que determinades persones que hi estan vinculades "per raons familiars o de fet", poden accedir a la informació relativa a la persona difunta i, si escau, demanar-ne la rectificació o la supressió. Això, llevat que consti la prohibició expressa del titular de la informació o que determinades previsions legals puguin limitar l'exercici d'aquesta facultat.

Això pot incloure també l'accés dels hereus a un compte de correu facilitat pel col·legi.

En el cas d'un professional difunt, el despatx professional al qual pertanyia pot accedir a la informació del compte de correu electrònic facilitat pel col·legi professional?

El despatx professional de la persona difunta únicament pot accedir a les dades d'aquell si ha estat expressament habilitat a aquest efecte, en un document de voluntats digitals o una altra autorització.

Cal recordar la conveniència d'aprovar normes d'utilització del sistema de correu electrònic dels col·legis professionals, que hagin estat aprovades i acceptades pels seus usuaris i que prevegin, a més dels sistema d'accés al correu, les condicions d'ús i de conservació i altres eventualitats, com el destí de la informació en cas de defunció, que siguin aplicables a manca de manifestació expressa de la persona interessada.

Normativa aplicable: art. 15 RGPD; arts. 3, 12 i 13 LOPDGDD; art. 28 RLOPD.

7.2.3 Dret de rectificació

La persona afectada té dret a obtenir la rectificació de les seves dades personals que siguin inexactes i que es completin les seves dades incompletes.

El responsable ha de:

- Comunicar la rectificació efectuada a cadascun dels destinataris a qui s'hagin comunicat les dades, tret que sigui impossible o exigeixi un esforç desproporcionat.
- Informar la persona afectada sobre els destinataris, si ho demana.

La rectificació de les dades dona lloc al bloqueig de les dades rectificades. Sobre això ens remetem a l'apartat 8.2 d'aquesta guia.



Un col·legiat pot demanar la rectificació de les dades que apareixen a la guia o llista de professionals?

Sí, indicant les dades errònies que s'han de corregir i aportant la documentació que ho acredita.

Quin és el termini per resoldre i notificar una sol·licitud de rectificació?

La sol·licitud de rectificació s'ha de resoldre i notificar en el termini màxim d'un mes a comptar a partir de la data de recepció de la sol·licitud. Aquest termini es pot prorrogar dos mesos més (tres, en total), tenint en compte la complexitat o el nombre de sol·licituds.

Normativa aplicable: arts. 16 i 19 RGPD; 14 i 32 LOPDGDD.

7.2.4 Dret de supressió

La persona afectada té dret a obtenir la supressió de les seves dades personals ("dret a l'oblit"), quan:

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

Si el responsable ha comunicat les dades, cal que:

- Adopti mesures raonables, tret que sigui impossible o exigeixi esforços desproporcionats, per informar de la supressió els destinataris que estan tractant aquestes dades, per tal que, si escau, les suprimeixin. Quan s'hagin fet públiques, ha d'adoptar les mesures raonables, incloses mesures tècniques, per informar els

responsables que les estan tractant de la sol·licitud de l'afectat de suprimir qualsevol enllaç o còpia de les dades.

- Informi la persona afectada sobre els destinataris, si ho demana.

Quan la supressió derivi de l'exercici del dret d'oposició al tractament per a finalitats de màrqueting directe, el responsable pot conservar les dades identificatives de la persona afectada necessàries amb la finalitat d'impedir tractaments futurs per a aquesta finalitat.

El dret de supressió no s'aplica quan el tractament és necessari per a:

- L'exercici del dret a la llibertat d'expressió i informació.
- El compliment d'una obligació legal, o per complir una missió realitzada en interès públic o en l'exercici de poders públics conferits al responsable.
- Raons d'interès públic en l'àmbit de la salut.
- L'existència de finalitats d'arxiu en interès públic, de recerca científica o històrica o finalitats estadístiques.
- La formulació, l'exercici o la defensa de reclamacions.

La supressió de les dades dona lloc al bloqueig de les dades suprimides. Sobre això, vegeu l'apartat 8.2 d'aquesta guia.



Un col·legi professional està obligat a suprimir les dades bancàries que havia facilitat un col·legiat per pagar les quotes, si el col·legiat ho sol·licita?

Sí, si ja no son necessàries. No es poden suprimir si és imprescindible mantenir-les per cobrar les quotes derivades de la relació jurídica establerta entre el col·legiat i el col·legi professional –per exemple, perquè la normativa col·legial estableix únicament aquest sistema de pagament- .

Els hereus poden exercir el dret de supressió de dades de la persona difunta?

L'LOPDGDD preveu expressament que determinades persones vinculades amb la persona difunta "per raons familiars o de fet" puguin demanar la rectificació o la supressió de les dades de la persona difunta. Això, llevat que consti la prohibició expressa del titular de la informació o que determinades previsions legals puguin limitar l'exercici d'aquesta facultat.

Normativa aplicable: arts. 17 i 19 RGPD; 3, 15 i 32 LOPDGDD.

7.2.5 Dret a la limitació del tractament

El dret a la limitació del tractament consisteix a marcar les dades personals, amb la finalitat de limitar-ne el tractament en el futur només per a determinades finalitats. No s'ha de confondre amb el bloqueig de dades.

Es pot sol·licitar la limitació:

- Quan la persona afectada ha exercit els drets de rectificació o oposició i mentre el responsable determina si escau atendre la sol·licitud.
- Quan el tractament és il·lícit, però la persona afectada s'oposa a la supressió i en sol·licita la limitació.
- Quan les dades són innecessàries per al tractament, però la persona afectada s'oposa a la supressió perquè les necessita per formular, exercir o defensar reclamacions.

Mentre dura la limitació, el responsable només pot tractar les dades, més enllà de conservar-les, en els casos següents:

- Amb el consentiment de la persona afectada.
- Per formular, exercir o defensar reclamacions.
- Per protegir els drets d'una altra persona física o jurídica.
- Per raons d'interès públic importants de la Unió o de l'estat membre.

Quan una persona afectada ha obtingut la limitació del tractament, cal informar-la abans que s'aixequi la mesura.

Quan s'ha limitat el tractament, el responsable ha de:

- Fer constar la limitació de manera clara en els seus sistemes d'informació.
- Comunicar la limitació efectuada a cadascun dels destinataris a qui s'hagin comunicat les dades, tret que sigui impossible o exigeixi un esforç desproporcionat.
- Informar la persona afectada sobre els destinataris, si ho demana.

Normativa aplicable: art. 18 RGPD; 16 LOPDGDD.

7.2.6 Dret a la portabilitat

En virtut del dret a la portabilitat, la persona afectada té dret a rebre, en un format estructurat, d'ús comú i de lectura mecànica, les seves dades personals que ha facilitat a un responsable del tractament.

Aquest dret també inclou la possibilitat que es transmetin directament del responsable a un altre responsable, si és tècnicament possible.

Perquè el dret de portabilitat sigui aplicable, cal que es compleixin les condicions següents:

- La recollida de les dades es va basar en el consentiment o en un contracte.
- El tractament es fa amb mitjans automatitzats.

Limitacions:

- No es pot exercir aquest dret quan el tractament es fonamenta en el compliment d'una missió d'interès públic o és inherent a l'exercici de poders públics. Per tant, no és aplicable quan el col·legi professional actua en exercici de les seves funcions públiques.
- No pot afectar negativament els drets i llibertats d'altres persones.



Es pot exercir el dret de portabilitat en l'àmbit dels col·legis professionals?

Només es pot exercir quan el tractament es basa en el consentiment de la persona afectada o quan el tractament sigui necessari per executar un contracte en el qual la persona afectada és part o bé per aplicar mesures precontractuals a petició seva. No es pot exercir quan el tractament és necessari per exercir una missió en interès públic o per exercir potestats públiques.

Quan se sol·licita la portabilitat a un col·legi professional en relació amb un tractament de dades derivat de les funcions públiques del col·legi, cal respondre la persona afectada, tenint en compte que el dret de portabilitat no s'aplica en aquest cas?

Sí. Tot i que el dret a la portabilitat en principi no ha de prosperar, en relació amb els tractaments que duen a terme els col·legis professionals per exercir les seves funcions públiques, sempre cal atendre qualsevol sol·licitud i donar-hi resposta dins del termini previst.

Cal que en les clàusules informatives de protecció de dades que el col·legi adreça a les persones afectades, s'indiqui la possibilitat d'exercir el dret de portabilitat?

El col·legi ha d'informar sobre la possibilitat d'exercir el dret a la portabilitat quan la base jurídica del tractament sigui el consentiment o l'execució d'un contracte. Quan la base jurídica del tractament sigui una altra, com ara el compliment d'una obligació legal, l'exercici d'una potestat pública o el compliment d'una missió en interès públic, la informació sobre la possibilitat d'exercir aquest dret no s'hi ha d'incloure, atès que no és possible exercir-lo.

Normativa aplicable: art. 20 RGPD; 17 LOPDGDD.

7.2.7 Dret d'oposició

La persona afectada té dret a oposar-se, en qualsevol moment, al tractament de les seves dades personals en els supòsits següents:

- Quan el tractament es basa en **una missió realitzada en interès públic** o en **l'exercici de poders públics** conferits al responsable, o en **l'interès legítim** perseguit pel responsable del tractament o per un tercer. En aquest cas, l'oposició

s'ha de fonamentar en motius relacionats amb la seva situació personal. El responsable del tractament ha de deixar de tractar-les, tret que acrediti motius legítims imperiosos que prevalguin sobre els interessos, els drets i les llibertats de la persona afectada, o per formular, exercir o defensar-se de reclamacions.

- Quan el tractament té per objecte el **màrqueting directe**, inclosa l'elaboració de perfils relacionats amb el màrqueting.
- Quan el tractament té fins **estadístics o d'investigació científica o històrica** i s'invoca un motiu relacionat amb la seva situació personal, llevat que sigui necessari per al compliment d'una missió en interès públic.

En l'àmbit dels serveis de la societat de la informació, les persones afectades han de poder exercir aquest dret per mitjans automatitzats.



Un col·legiat es pot oposar a la publicació de les seves dades personals a la guia o llista de professionals, sense causa justificada?

El col·legiat pot oposar-se a aquest tractament, si al·lega motius relatius a la seva situació personal, com per exemple raons de seguretat, patir algun tipus d'amenaça, etc. En aquest cas, un cop feta la ponderació amb els interessos que justifiquen la publicació, el col·legi l'ha d'excloure del llistat professional, llevat que hi hagi motius legítims imperiosos que justifiquin que es mantinguin publicades.

Pel que fa a la possibilitat de demanar que s'excloquin les seves dades del llistat de professionals del col·legi de la utilització per a finalitats de publicitat o prospecció comercial, en aquest cas no cal al·legar cap situació personal, sinó que n'hi ha prou de sol·licitar-ho.

Normativa aplicable: art. 21 RGPD.

7.2.8 Dret a no ser objecte de decisions automatitzades

La persona afectada té dret a no ser objecte d'una decisió basada només en el tractament automatitzat de les seves dades, inclosa l'elaboració de perfils, que produeixi efectes jurídics sobre ella o que l'afecti negativament.

Només es poden adoptar aquestes decisions en els supòsits següents:

- a) Si és necessari per **formalitzar o executar un contracte** entre la persona afectada i un responsable de tractament.
- b) Si està autoritzat per una **norma amb rang de llei** o pel dret de la Unió que estableixi garanties adequades per als drets i llibertats de les persones afectades.
- c) Si es basa en el **consentiment** explícit de la persona afectada.

Garanties exigibles:

- En els tres casos, s'han d'establir mesures adequades per salvaguardar els drets, les llibertats i els interessos legítims de la persona afectada.
- En els casos de les lletres a) i c), la persona afectada té dret a:
 - Obtenir intervenció humana per part del responsable.
 - Expressar el seu punt de vista.
 - Impugnar la decisió.
- Les decisions no es poden basar en categories especials de dades, llevat que:
 - Es disposi del consentiment de la persona afectada, o
 - Calgui tractar-les per raons d'interès públic essencial establert per una llei o el dret de la Unió.

Normativa aplicable: art. 22 RGPD.

7.3. L'exactitud i l'actualització de les dades

Les dades han de ser exactes i, si cal, s'han d'actualitzar. El responsable ha d'adoptar d'ofici totes les mesures raonables perquè les dades personals inexactes se suprimeixin o es rectifiquin, sense dilació. També les pot haver de rectificar, quan escaigui, com a conseqüència que les persones afectades hagin exercit el dret de rectificació.

Això fa necessari que, per mantenir la informació actualitzada, el col·legi professional hagi de disposar d'uns mecanismes individualitzats d'actualització a instància de les persones interessades, així com procediments massius periòdics d'actualització i, si escau, de supressió de les dades.

La inexactitud de les dades no és imputable al responsable del tractament si les ha obtingut:

- Directament de la persona afectada.
- D'un mediador o responsable, si les normes aplicables al sector d'activitat a què pertanyi el responsable del tractament estableixen la possibilitat que un intermediari o mediador reculli en nom propi les dades de les persones afectades, per transmetre-les al responsable. El mediador o intermediari assumeix les responsabilitats que es puguin derivar si les dades que comunica al responsable no es corresponen amb les que ha facilitat la persona afectada.
- D'un altre responsable, en virtut del dret a la portabilitat exercit per la persona afectada.
- D'un registre públic.

Les dades rectificades estan sotmeses al deure de bloqueig. Sobre això, ens remetem a l'apartat 8.2 d'aquesta guia.

Actualització de les llistes de professionals

Tant la normativa de protecció de dades com la normativa sectorial obliguen els col·legis professionals, com a responsables del tractament, a verificar periòdicament que les dades publicades s'adeqüen a la realitat dels col·legiats. S'ha de fer a través d'un procediment que permeti comprovar si les dades són correctes, i modificar la guia en cas de baixa o defunció d'algun col·legiat. Aquesta revisió periòdica és independent de l'obligació d'atendre les sol·licituds de rectificació o supressió de les persones afectades.

- **Verificació de l'actualització de dades de la llista de professionals col·legiats:** es recomana que abans de publicar una nova edició de la llista o guia professional, el col·legi informi els col·legiats de les dades que contindrà la guia o llistat i els ofereixi la possibilitat de demanar la rectificació de les dades incorrectes i d'oposar-se a que alguna o totes les seves dades apareguin a la llista.

Els col·legiats també tenen dret a demanar que s'exclouï l'ús de les seves dades personals per a finalitats de publicitat o prospecció comercial. Per tant, el col·legi també ha d'informar d'aquesta possibilitat, en el moment que faci la comunicació per actualitzar les dades.

A l'[annex 2](#) d'aquesta guia podeu trobar un model de la clàusula informativa per actualitzar les dades que apareixen a la llista o guia de persones col·legiades.

- **Rectificació de les dades:** si el col·legi detecta que algunes de les dades són inexactes, les ha de rectificar al més aviat possible i, en qualsevol cas, en el termini d'un mes des de la recepció de la sol·licitud, si n'hi ha.



Com s'ha d'actuar si la persona afectada sol·licita la rectificació de les dades que considera inexactes a un encarregat del tractament que actua per compte del col·legi?

A l'acord d'encàrrec del tractament, s'ha d'establir de manera clara si correspon a l'encarregat del tractament atendre i donar resposta a les sol·licituds dels drets a l'autodeterminació informativa, com ara el dret de rectificació, o bé establir expressament que la seva única obligació és comunicar al responsable del tractament que s'ha exercit un dret.

En el primer supòsit, l'acord ha d'establir la forma i els terminis per atendre o, si escau, donar resposta a les sol·licituds d'exercici de drets. En el segon supòsit, cal establir la forma i el termini en què la sol·licitud i, si escau, la informació corresponent a l'exercici del dret, s'han de comunicar al responsable del tractament.

Quins mecanismes d'actualització, individualitzats o massius, pot adoptar el responsable del tractament?

Sens perjudici de les rectificacions que pugui fer arran de les sol·licituds d'exercici del dret de rectificació, o de les inexactituds de les quals tingui coneixement per altres vies, el col·legi pot establir mecanismes de revisió periòdica. Per exemple, pot

comunicar les dades de què disposa, per tal que cada persona pugui confirmar si les seves dades són correctes i actualitzades.

Normativa aplicable: art. 5.1.d) RGPD; art. 4 i 32 LOPDGDD.

7.4 L'encàrrec del tractament

7.4.1 La figura de l'encarregat del tractament

En algunes ocasions, el desplegament de l'activitat col·legial pot requerir col·laborar amb altres entitats en determinats àmbits o externalitzar determinats serveis que comportin el tractament de dades personals. Pel que fa a la protecció de dades personals, això s'ha de fer a través de la figura de l'encarregat del tractament.

L'encarregat del tractament, o encarregat, és la persona física o jurídica, autoritat pública, servei o qualsevol altre organisme que tracta dades personals per compte del responsable del tractament.

La figura de l'encarregat permet que els col·legis professionals externalitzin serveis i, alhora, puguin conservar el control efectiu sobre el tractament de les dades personals, amb independència que totes o algunes de les tasques materials que impliqui el tractament les dugui a terme una altra persona o entitat. Això succeeix, per exemple quan un col·legi encarrega a un tercer la gestió de la destrucció de documentació, la gestió de nòmines, el manteniment d'equips informàtics, l'allotjament d'informació, etc.

En aquests casos, quan l'accés del tercer a les dades personals és necessari per prestar el servei, i s'ha formalitzat l'encàrrec del tractament, no es considera comunicació de dades.

Cal tenir en compte que la normativa de contractes del sector públic, en els casos en què és aplicable, estableix que té la consideració d'encarregat del tractament qualsevol contractista que, per executar la prestació, hagi d'accedir a dades personals de les quals en sigui responsable l'entitat que ha adjudicat el contracte.

A l'hora d'escollir l'encarregat, el responsable del tractament ha de vetllar perquè reuneixi les garanties necessàries per dur a terme el tractament de dades personals. A aquest efecte, l'RGPD preveu, per exemple, que els encarregats es puguin adherir a codis de conducta o certificar-se, en el marc dels esquemes de certificació previstos en el mateix RGPD.

7.4.2 Formalització de l'encàrrec

La regulació de la relació entre el responsable i l'encarregat s'ha d'establir a través d'un contracte, conveni, acord, o acte jurídic que els vinculi. Ha de constar per escrit, inclòs el format electrònic.

El contracte o acte jurídic ha de tenir el contingut mínim següent, també quan l'encàrrec el formuli la norma reguladora de les competències de l'òrgan:

- L'objecte.
- La durada.
- La naturalesa.
- La finalitat del tractament.
- El tipus de dades personals.
- Les categories de persones afectades.
- Les obligacions i els drets de l'encarregat, en particular:
 - Seguir les instruccions del responsable.
 - Garantir el respecte al deure de confidencialitat.
 - Prendre totes les mesures de seguretat necessàries per garantir un nivell de seguretat adequat al risc.
 - Respectar el règim de subcontractació.
 - Assistir el responsable sempre que sigui possible, d'acord amb la naturalesa del tractament i mitjançant les mesures tècniques i organitzatives adequades.
 - Ajudar el responsable a garantir el compliment de les obligacions de seguretat.
 - Posar a disposició del responsable la informació necessària per demostrar que compleix les seves obligacions i permetre i contribuir a l'execució d'auditories.
 - A elecció del responsable, retornar, suprimir, o lliurar les dades a un altre encarregat. En tot cas, l'encarregat del tractament pot conservar les dades bloquejades, mentre es puguin derivar responsabilitats de la seva relació amb el responsable del tractament.

Els contractes d'encàrrec formalitzats abans de la plena aplicabilitat de l'RGPD (25 de maig de 2018) s'hi han d'adaptar perquè les seves clàusules reflecteixin tots els continguts de l'RGPD, d'acord amb els criteris següents:

- Contractes i acords d'encàrrec amb data de venciment: mantenen la seva vigència fins la data de venciment que tenen assenyalada.
- Contractes i acords d'encàrrec amb durada indefinida: mantenen la vigència fins el 25 de maig de 2022.

En qualsevol cas, durant la vigència del contracte o acord, qualsevol de les parts pot exigir a l'altra la modificació del contracte, per adaptar-la al que estableix l'RGPD.

A més, cal tenir en compte que en l'àmbit de la contractació del sector públic, quan sigui aplicable, els plecs de clàusules també han d'incloure les previsions següents:

- La finalitat per a la qual se cediran aquestes dades.
- L'obligació del futur contractista de sotmetre's a la normativa nacional i de la Unió Europea en matèria de protecció de dades, sense perjudici del que estableix l'últim paràgraf de l'apartat 1 de l'article 202 de l'LCSP.
- L'obligació de l'empresa adjudicatària de presentar abans de la formalització del contracte una declaració en la qual posi de manifest on estaran ubicats els servidors i des d'on es prestaran els serveis que hi estan associats.
- L'obligació de comunicar qualsevol canvi que es produeixi, al llarg de la vida del contracte, de la informació facilitada en la declaració a què es refereix el punt anterior.
- L'obligació dels licitadors d'indicar en la seva oferta, si tenen previst subcontractar els servidors o els serveis que hi estan associats, el nom o el perfil empresarial, definit per referència a les condicions de solvència professional o tècnica dels subcontractistes.

7.4.3 Obligacions de l'encarregat del tractament

A banda de les obligacions esmentades, establertes en el contracte o acte jurídic vinculant, l'RGPD estableix un seguit d'obligacions directament exigibles als encarregats del tractament.

Així, l'encarregat ha de complir les obligacions següents:

- Implantar les mesures tècniques i organitzatives adequades per garantir un nivell de seguretat adequat al risc del tractament.
- Designar un representant, en cas que l'encarregat estigui establert fora de la Unió Europea.
- Portar un registre de totes les categories d'activitats de tractament efectuades.
- Nomenar un delegat de protecció de dades, si escau.
- Vetllar perquè les dades personals es tractin correctament.
- Complir el règim aplicable a les transferències internacionals.
- Cooperar amb l'autoritat de control.
- Notificar les violacions de seguretat al responsable del tractament.

7.4.4 Subcontractació

L'encarregat del tractament pot subcontractar nous encarregats, amb l'autorització prèvia del responsable. L'autorització ha de ser per escrit i pot ser específica o general.

Si l'autorització no concreta el subencarregat o s'hi produeixin canvis, abans de fer-los efectius l'encarregat n'ha d'informar el responsable per tal de donar-li l'oportunitat d'oposar-s'hi.

El subencarregat s'ha de vincular amb l'encarregat mitjançant un contracte o acte jurídic anàleg al que s'ha d'establir entre l'encarregat i el responsable, i està sotmès a les mateixes obligacions que l'encarregat.

Si el subencarregat incompleix les obligacions de protecció de dades, l'encarregat inicial continua essent plenament responsable davant del responsable del tractament pel que fa al compliment de les obligacions del subencarregat.

7.4.5 Responsabilitat

Els col·legis professionals tenen, com a responsables del tractament, un deure de diligència a l'hora d'escollir l'encarregat del tractament. Cal que en triïn un que ofereixi garanties suficients respecte de la implantació i el manteniment de les mesures tècniques i organitzatives apropiades, d'acord amb el que estableix l'RGPD, i que garanteixi la protecció dels drets de les persones afectades.

L'encarregat respon directament del compliment de les obligacions que li imposa l'RGPD. Cal tenir en compte que el règim sancionador específic previst per l'LOPDGDD per a les entitats del sector públic, i en concret per a les corporacions de dret públic quan les finalitats del tractament es relacionen amb l'exercici de potestats de dret públic, només és aplicable a l'encarregat del tractament si, atesa la seva naturalesa, està inclosa dins les entitats que enumera l'article 77 de l'LOPDGDD. En cas contrari, se li ha d'aplicar el règim sancionador general, amb independència de la naturalesa de l'entitat responsable del tractament.

Pel que fa als danys que s'hagin produït, correspon a l'encarregat respondre dels danys causats pel tractament quan no hagi complert amb les obligacions de l'RGPD adreçades específicament a l'encarregat, o hagi actuat en contra de les instruccions del responsable. Quan hi hagi més d'un encarregat o quan el responsable i l'encarregat hagin participat conjuntament en la producció dels danys, hi ha responsabilitat solidària entre ells. Per tant, la persona afectada pot exigir tota la indemnització de qualsevol d'ells, sens perjudici de la possibilitat que qui l'hagi satisfet pugui reclamar al corresponsable o corresponsables la part de la indemnització corresponent.

Quant a la responsabilitat assumida per l'encarregat, si en el moment de determinar les finalitats i els mitjans del tractament un encarregat infringeix l'RGPD, se l'ha de considerar responsable pel que fa a aquest tractament.

Sobre la figura de l'encàrrec del tractament es recomana consultar la [Guia sobre l'encarregat del tractament a l'RGPD](#), elaborada per aquesta Autoritat. També podeu tenir en compte les [clàusules contractuals tipus aprovades](#) per la Comissió Europea mitjançant la Decisió d'execució (UE) 2021/915, de 4 de juny de 2021.



Per tal que un ens tracti dades per compte d'un col·legi professional, n'hi ha prou que aquest li doni certes indicacions o instruccions?

No. Quan l'ens instrumental accedeix a dades personals que es tracten sota la responsabilitat del col·legi, ha de fer-ho comptant amb el contracte o acte jurídic vinculant, en els termes de l'article 28.3 de l'RGPD.

Un col·legi professional pot facilitar dades dels col·legiats a una empresa externa perquè faci una enquesta per al col·legi?

Sí. En aquest cas, l'empresa tindria la condició d'encarregat del tractament, sempre que signi el contracte d'encarregat amb el col·legi amb el contingut que estableix l'article 28.3 de l'RGPD.

Des del punt de vista de la normativa de protecció de dades, quins són els requisits que ha de complir el col·legi per encarregar el cobrament de les quotes dels col·legiats a una entitat financera?

El col·legi ha d'escollir una entitat que ofereixi garanties adequades pel que fa al tractament de les dades que el col·legi li faciliti o que reculli l'entitat per compte del col·legi, i ha de subscriure un contracte o acord d'encàrrec amb aquesta entitat, amb el contingut que estableix l'article 28.3 de l'RGPD.

Qui és el responsable del tractament, quan el col·legi professional encarrega la recollida de dades i l'elaboració de la guia o llista professional a una entitat col·laboradora?

En aquest cas, el responsable del tractament és el col·legi. L'entitat col·laboradora és un encarregat del tractament, sempre que se subscrigui el contracte o acord d'encàrrec corresponent.

Normativa aplicable: considerant 81 i 97 i arts. 4.8, 28, 29, 32.1 i 82 RGPD; arts. 33, 70, 77 i DT 5a LOPDGGDD; 11 LRJSP; arts. 35.1.d), 71.2.d), 116.1, 122.2, 202.1, 215.4 i DA 25a LCSP.

7.5 El delegat de protecció de dades

Tots els col·legis professionals i els consells de col·legis han de designar obligatòriament un delegat de protecció de dades (DPD). La resta d'entitats dependents dels col·legis professionals l'han de designar si hi concorre algun dels supòsits següents:

- La seva activitat principal consisteix en operacions de tractament que, per la seva naturalesa, abast o finalitats, requereixen una observació habitual i sistemàtica de les persones afectades a gran escala.
- La seva activitat principal consisteix en el tractament a gran escala de categories especials de dades o dades relatives a condemnes i infraccions penals.

En qualsevol cas, els ens dependents que no hi estiguin obligats poden designar-lo de manera voluntària.

Requisits necessaris per ser delegat de protecció de dades:

- No s'estableix una titulació específica, ni certificat, tot i que es requereix que tingui coneixements especialitzats en dret, sobre la legislació i pràctiques nacionals i europees en matèria de protecció de dades i un profund coneixement de l'RGPD que li permeti identificar els riscos associats a les operacions del tractament, tenint en compte la naturalesa, l'abast, el context i les finalitats del tractament.
- Coneixements del sector de l'activitat de què es tracti. En aquest cas coneixements sobre l'àmbit professional del col·legi, l'activitat i l'organització col·legial, les operacions de tractament que es duen a terme i els sistemes d'informació.

El delegat de protecció de dades pot ser:

- Intern: personal del col·legi professional o del consell de col·legis
- Extern: una persona, organització o empresa aliena al col·legi sempre que s'acreditin les competències professionals a què fa referència l'RGPD, es garanteixi que no hi ha cap conflicte d'interès i es formalitzi un contracte d'encàrrec del tractament, per tal que pugui accedir a la informació personal de la qual és responsable el col·legi, necessària per exercir les funcions del delegat de protecció de dades. Si el delegat és una organització, convé designar una persona com a punt de contacte.

Cal tenir en compte que l'RGPD ofereix diferents possibilitats per flexibilitzar aquesta exigència. Així, per exemple, un mateix delegat de protecció de dades pot assumir, per encàrrec, aquesta funció respecte de diversos col·legis; un col·legi o consell de col·legis pot prestar aquest servei a altres col·legis, etc.

Pel que fa a la **posició** del delegat de protecció de dades, cal tenir en compte els aspectes següents:

- El responsable o l'encarregat han de garantir que el delegat de protecció de dades participa de manera adequada i en el moment oportú en totes les qüestions relatives a la protecció de dades personals.
- El responsable o l'encarregat li han de donar suport i li han de facilitar els recursos necessaris per complir les seves tasques.
- Cal garantir la independència a l'hora d'exercir les seves funcions. El delegat de protecció de dades no està sotmès a les instruccions del responsable o l'encarregat, ni pot ser sancionat ni destituït per l'exercici de les seves funcions.
- El delegat de protecció de dades ha de rendir comptes directament al nivell jeràrquic més alt del responsable o de l'encarregat.
- Tot i que pot assumir altres tasques, el responsable o l'encarregat han d'evitar que això pugui donar lloc a un conflicte d'interessos. Conseqüentment, no es pot designar com a delegat de protecció de dades una persona que participi en el procés de presa de decisions sobre els tractaments o en la seva implementació, en aspectes tan cabdals com, per exemple, l'adopció de les mesures de seguretat (com és el cas del responsable de seguretat), o que assumeixi la representació i defensa de la corporació.
- El delegat de protecció de dades ha de tenir visibilitat suficient: un cop designat el nom i les seves dades de contacte s'han d'incloure al registre d'activitats del tractament; a més, les dades de contacte s'han d'incloure tant a la informació que es facilita a les persones afectades com en les respostes a l'exercici de drets. També s'han de publicar al web, per tal que les persones afectades puguin contactar-hi de manera fàcil i directa.
- La seva designació, i qualsevol canvi que es produeixi, s'ha de comunicar a l'Autoritat Catalana de Protecció de Dades.

Funcions del delegat de protecció de dades:

- Informar i assessorar el responsable o l'encarregat i els empleats que s'ocupen del tractament de les seves obligacions en matèria de protecció de dades.
- Supervisar el compliment del que disposa la normativa de protecció de dades personals i de les polítiques del responsable o de l'encarregat del tractament, en matèria de protecció de dades personals.
- Oferir l'assessorament que se li sol·liciti sobre l'avaluació d'impacte relativa a la protecció de dades i supervisar-ne l'aplicació.
- Cooperar amb l'autoritat de control.
- Actuar com a punt de contacte de l'autoritat de control per a qüestions relatives al tractament.
- Intervenir en cas d'una reclamació presentada per la persona afectada davant el col·legi professional o bé quan li sigui remesa per l'Autoritat Catalana de Protecció de Dades.



Un col·legi professional ha modificat el registre d'activitats de tractament, atesos els canvis produïts en diversos tractaments. Ha d'avisar el seu DPD d'aquests canvis?

Sí. Tenint en compte el que disposa l'article 31.1 de l'LOPDGDD, li ha de comunicar qualsevol addició, modificació o exclusió en el contingut del registre.

L'obligació de publicar les dades del delegat de protecció de dades requereix incloure'n el nom?

L'obligació de publicar les dades de contacte del delegat de protecció de dades pot complir-se difonent un número de telèfon de contacte, una adreça postal i/o una adreça electrònica, sense incloure-hi necessàriament el nom. No obstant això, al registre d'activitats del tractament hi han de constar el nom i cognoms i les dades de contacte.

El delegat de protecció de dades pot exercir funcions de responsable de seguretat, o han de ser persones diferents?

El DPD actua com interlocutor davant l'autoritat de control, fa recomanacions, informa, assessora i supervisa els tractaments, entre d'altres. En canvi, el responsable de seguretat s'encarrega d'implementar les mesures de seguretat necessàries des d'una esfera tècnica i gestiona els riscos que es puguin plantejar. Previsiblement, hi pot haver un conflicte d'interessos entre ambdues figures que impedeix que coincideixin en una mateixa persona.

No obstant això, la col·laboració entre ambdós és imprescindible.

Normativa aplicable: arts. 37, 38 i 39 RGPD; arts. 34.1.a), 35, 36 i 37 LOPDGDD.

7.6 Les transferències internacionals de dades

Quan els col·legis professionals necessiten transferir dades fora de l'Espai Econòmic Europeu (per exemple, perquè han contractat com a encarregada del tractament una empresa de fora d'aquest àmbit, han externalitzat determinats serveis al núvol, o utilitzen determinades plataformes de serveis, entre d'altres supòsits), cal tenir en compte que les dades personals només es poden comunicar fora de l'Espai Econòmic Europeu en els casos següents:

- A països, territoris o sectors específics sobre els quals la Comissió Europea ha adoptat una decisió que reconeix que ofereixen un nivell de protecció adequat. Es poden consultar els països amb decisió d'adequació al [web de la Comissió Europea](#).
- Quan s'han ofert garanties adequades sobre la protecció que les dades rebran a la seva destinació. El responsable o l'encarregat del tractament només poden fer una transferència internacional si el destinatari ofereix garanties adequades i les

persones afectades compten amb drets exigibles i accions legals efectives. Aquestes garanties es poden oferir mitjançant:

- Un instrument jurídicament vinculant i exigible entre les autoritats o els organismes públics.
- Normes corporatives vinculants.
- Clàusules tipus de protecció de dades adoptades per la Comissió Europea³.
- Clàusules tipus de protecció de dades adoptades per una autoritat de control i aprovades per la Comissió Europea.
- Un codi de conducta aprovat, juntament amb compromisos vinculants i exigibles del responsable o de l'encarregat del tractament que al país tercer s'apliquen les garanties adequades, incloses les relatives als drets de les persones afectades.
- Un mecanisme de certificació, juntament amb compromisos vinculants i exigibles del responsable o de l'encarregat del tractament que al país tercer s'apliquen les garanties adequades, incloses les relatives als drets de les persones afectades.
- Amb l'autorització de l'Autoritat Catalana de Protecció de Dades, si s'aporten les garanties adequades mitjançant:
 - Clàusules contractuals entre el responsable o l'encarregat i el responsable, l'encarregat o el destinatari de les dades personals al país tercer o organització internacional.
 - Disposicions incorporades en acords administratius entre les autoritats o els organismes públics, que incloguin drets efectius i exigibles per a les persones interessades. Aquesta possibilitat pot ser aplicable als col·legis professionals, quan es tracti de l'exercici de les seves funcions públiques.
- Quan sigui d'aplicació alguna de les excepcions següents:
 - a) La persona afectada ha donat explícitament el seu consentiment a la transferència proposada, després d'haver estat informada dels riscos d'aquestes transferències a causa de l'absència d'una decisió d'adequació i de garanties adequades.

³ Cal tenir en compte la Decisió d'execució de la (UE) 2021/914 de la Comissió de 4 de juny de 2021 relativa a les clàusules contractuals tipus per a la transferència de dades personals a tercers països de conformitat amb el Reglament (UE) 2016/679 del Parlament Europeu i del Consell i l'annex a aquesta decisió.

- b) La transferència és necessària per executar un contracte entre la persona afectada i el responsable del tractament, o per executar mesures precontractuals adoptades a sol·licitud de la persona afectada.
- c) La transferència és necessària per formalitzar o executar un contracte entre el responsable del tractament i una altra persona física o jurídica, en interès de la persona afectada.
- d) La transferència és necessària per raons importants d'interès públic, que ha d'estar reconegut pel dret de la Unió o dels estats membres, que s'aplica al responsable del tractament.
- e) La transferència és necessària per formular, exercir o defensar reclamacions.
- f) La transferència és necessària per protegir drets vitals de la persona afectada o d'altres persones, quan la persona afectada està físicament o jurídicament incapacitada per donar-hi el consentiment.
- g) La transferència s'efectua des d'un registre públic que, de conformitat amb el dret de la Unió o dels estats membres, té per objecte facilitar informació al públic i és obert a la consulta del públic en general o de qualsevol persona que hi acrediti un interès legítim, però només si es compleixen, en cada cas particular, les condicions que estableix el dret de la Unió o dels estats membres per fer la consulta. En aquest cas, no ha d'abastar la totalitat de les dades personals ni categories senceres de dades personals que conté el registre.

Les excepcions previstes a les lletres *a)*, *b)* i *c)* no són aplicables a les activitats desplegades pels col·legis professionals en exercici de poders públics.

- Si no es dona cap de les condicions anteriors, la transferència internacional de dades només es pot fer si es compleixen totes les condicions següents:
 - No és repetitiva.
 - Només afecta un nombre limitat de persones afectades.
 - És necessària per a les finalitats d'interessos legítims imperiosos perseguits pel responsable del tractament.
 - El responsable del tractament ha avaluat totes les circumstàncies concurrents en la transferència de dades i, basant-se en aquesta avaluació, ha ofert garanties adequades respecte de la protecció de dades personals.

Aquesta possibilitat no és aplicable a les activitats desenvolupades pels col·legis professionals en l'exercici dels seus poders públics.

El responsable ha d'informar l'APDCAT de la transferència. També n'ha d'informar les persones afectades, així com dels interessos legítims imperiosos perseguits.

Normativa aplicable: considerants 101 a 116 i arts. 40, 44 a 50 i 57.r) RGPD; arts. 40 a 43 LOPDGDD.

7.7 La seguretat de les dades: integritat i confidencialitat

El responsable del tractament i l'encarregat han de vetllar perquè les dades es tractin de manera que se'n garanteixi una seguretat adequada, inclosa la protecció contra el tractament no autoritzat o il·lícit i contra la seva pèrdua, destrucció o dany accidental, mitjançant l'aplicació de les mesures tècniques o organitzatives adequades.

Això fa necessari que el responsable i l'encarregat garanteixin la confidencialitat, la integritat i la disponibilitat de les dades.

Per fer-ho, en primer lloc cal identificar i avaluar els riscos existents i, a partir d'aquí determinar les mesures de seguretat necessàries per tal de mitigar-los o, si escau eliminar-los.

7.7.1 El deure de confidencialitat

El responsable del tractament, l'encarregat i totes les persones que actuïn sota la seva autoritat estan obligats a garantir la confidencialitat de la informació a la qual tinguin accés en exercici de les seves funcions, per tal que no sigui revelada, accidentalment o voluntària a persones no autoritzades, llevat que una llei ho exceptuï.

Aquest deure comporta no només la impossibilitat de revelar a tercers la informació en poder del col·legi professional a la qual s'hagi accedit en exercici de les funcions atribuïdes, sinó que obliga també que, dins del col·legi professional, cada treballador pugui accedir només a la informació necessària per exercir les seves funcions.

A aquest efecte, el responsable i l'encarregat han d'adoptar les mesures tècniques i organitzatives necessàries, com ara la implantació de sistemes de control físic de la informació (per exemple, tancaments de dependències i armaris), establir una política i un sistema d'assignació de permisos (per exemple, accés mitjançant claus o certificats), implantar sistemes de control d'accessos, etc.

Per garantir el deure de confidencialitat, es poden incorporar clàusules de confidencialitat en els contractes de treball i en els protocols i regulacions internes. El deure de confidencialitat del personal s'estén fins i tot després que hagi finalitzat la relació laboral.

També s'han d'incloure les previsions oportunes en els contractes i acords d'encàrrec del tractament que se signin, perquè l'encarregat signi aquestes clàusules amb els seus treballadors.

L'obligació de confidencialitat prevista a la normativa de protecció de dades és complementària del deure de secret professional per a determinades professions, de conformitat amb la seva normativa aplicable.



El deure de confidencialitat forma part del secret professional?

Tot i que estan relacionats, no s'ha de confondre. El deure de confidencialitat previst a la normativa de protecció de dades afecta qualsevol persona que intervingui en el tractament de les dades personals i és complementària al deure de secret professional a què estan sotmeses les persones que exerceixen determinades professions.

Qualsevol treballador d'un col·legi professional pot accedir a tota la informació sobre terceres persones de què disposa el col·legi?

Els treballadors només poden tenir accés a la informació necessària per exercir les funcions que tenen atribuïdes.

Una agrupació de persones col·legiades, constituïda en el si del col·legi, pot tenir accés a les dades dels nous col·legiats per facilitar-los informació sobre les activitats que duu a terme l'agrupació?

Atesa la informació que conté el registre de col·legiats i la informació de la guia de col·legiats, es pot considerar habilitada la comunicació de les dades relatives als nous col·legiats (dades identificatives i de contacte –adreça professional-, número de col·legiació i la data d'incorporació al col·legi) a l'agrupació, sense consentiment dels afectats.

Un membre de la junta de govern d'un col·legi professional pot emprar les dades personals que ha conegut en exercici de les seves funcions per fer-ne difusió en un blog personal?

Qualsevol utilització de la informació personal posterior a un accés legítim del membre de la junta de govern ha d'estar, igualment, fonamentada en una finalitat legítima i compatible amb la finalitat que va justificar l'accés. Si l'ús posterior comporta revelar dades personals a terceres persones, com pot ser el fet de publicar informació en un blog sense una base jurídica que ho empari, ens podem trobar davant d'una actuació que no s'adequa a la normativa de protecció de dades, tot i que en origen l'accés es considerés legítim.

Normativa aplicable: art. 5.1.f) RGPD; 5 LOPDGDD.

7.7.2 La integritat de les dades

Es tracta d'una exigència directament lligada amb el principi d'exactitud. La informació no pot patir modificacions no autoritzades. Així, les dades personals s'han de tractar de manera que se'n garanteixi la protecció contra l'alteració, pèrdua, destrucció o dany accidental, mitjançant l'aplicació de les mesures tècniques o organitzatives adequades.

Normativa aplicable: art. 5.1.f) RGPD.

7.7.3 La disponibilitat de les dades

No disposar de la informació necessària per prendre decisions, encara que sigui temporalment, pot comportar conseqüències per als drets, llibertats i interessos de les persones afectades. Per això, és important que el responsable i l'encarregat del tractament adoptin mesures tècniques i organitzatives (com ara les còpies de seguretat o solucions alternatives en cas de fallada del sistema elèctric, etc.) que assegurin la disponibilitat de la informació i els sistemes d'informació de manera continuada.

Normativa aplicable: art. 5.1.f) RGPD.

7.7.4 L'anàlisi de riscos

L'anàlisi de riscos és l'element clau a l'hora de determinar les mesures de seguretat a aplicar (tècniques i organitzatives), atès que han de ser adequades a la probabilitat i la gravetat dels riscos que se'n poden derivar per als drets i llibertats de les persones.

Sens perjudici que l'anàlisi de riscos s'ha de dur a terme abans d'iniciar el tractament, es tracta d'una obligació que afecta tota la vida del tractament. Per això, i atès que els riscos poden variar, s'ha de revisar periòdicament i sempre que es produeixi algun canvi substancial en el tractament.

Sobre aquesta qüestió ens remetem al que ja s'ha exposat a l'apartat 6.3 d'aquesta guia



És recomanable emprar sistemes de missatgeria instantània (SMI), a la llum de les indicacions de la Resolució 280/XI del Parlament de Catalunya?

Els col·legis professionals, com a responsables de tractar dades dels col·legiats i d'altres afectats per complir llurs funcions, han d'assegurar-se que els tercers prestadors de serveis i de sistemes de comunicació compleixen, al seu torn, llurs responsabilitats. Això, ja sigui com a encarregats del tractament o, si escau, com a responsables del tractament de les dades dels usuaris (en el cas dels SMI), atès que el tractament està sotmès a les exigències dels principis i garanties de la normativa europea de protecció de dades.

Així, quan considerin l'elecció d'un determinat sistema de missatgeria instantània (SMI) cal que facin una anàlisi dels riscos existents (probabilitat i gravetat) tenint en compte, especialment: la finalitat de la comunicació; la informació personal que cal tractar; l'existència de consentiment lliurement atorgat pels afectats; les mesures concretes de seguretat aplicades pel sistema de missatgeria; els mecanismes de certificació; les transferències internacionals de dades i la ubicació dels servidors; el dret d'informació i la transparència, en atenció a les previsions de l'RGPD.

7.7.5 Les mesures de seguretat

L'RGPD no estableix una llista de mesures de seguretat a aplicar. D'acord amb l'anàlisi de riscos realitzada, el responsable i l'encarregat del tractament han de determinar i implementar, cas per cas, les mesures de seguretat apropiades, en funció del risc, per garantir la confidencialitat, la integritat i la disponibilitat de les dades.

S'han de tenir en compte els aspectes següents:

- L'estat de la tècnica.
- Els costos d'aplicació.
- La naturalesa, l'abast, el context i les finalitats del tractament,
- La probabilitat i la gravetat dels riscos per als drets i les llibertats de les persones físiques.

Sempre que exerceixin funcions de naturalesa pública, els col·legis professionals i els ens de naturalesa pública i les fundacions del sector públic que en depenen han d'aplicar, com a mínim, les mesures establertes a l'Esquema Nacional de Seguretat (ENS). En l'exercici de les funcions privades l'aplicació de l'ENS no és obligatòria, tot i que res impedeix que l'anàlisi de riscos també es pugui dur a terme d'acord amb aquest esquema.

La resta d'entitats que depenen dels col·legis professionals poden aplicar també les mesures que es deriven de l'ENS, o unes altres, sempre que siguin adequades per garantir la confidencialitat, integritat i disponibilitat de les dades personals atesos els riscos existents. L'adhesió a un codi de conducta o a un mecanisme de certificació, pot servir d'element per demostrar que es compleix aquesta obligació.

Quan es presten els serveis a través d'un encàrrec del tractament, en el contracte o acte jurídic vinculant també cal assegurar, com a mínim, que s'apliquen les mesures que corresponen adoptar al responsable.

Les mesures de seguretat aplicades s'han d'establir i implementar abans d'iniciar el tractament i s'han de revisar periòdicament i sempre que es produeixi algun canvi substancial en el tractament o en els riscos que se'n deriven.

El responsable i l'encarregat del tractament han de prendre mesures per garantir que qualsevol persona que actua sota la seva autoritat i que té accés a dades personals les tractarà seguint instruccions del responsable, tret que hi estigui obligada en virtut del dret de la Unió o dels estats membres.



Quines mesures de seguretat ha d'implementar un col·legi professional per protegir les dades personals que tracta?

El col·legi professional ha d'implementar qualsevol mesura que resulti necessària atenent els riscos que existeixin. Pel que fa als tractaments automatitzats que dugui a terme en l'exercici de potestats de dret públic, això inclou, com a mínim, les mesures de seguretat que corresponguin de les que preveu l'Esquema Nacional de Seguretat.

Pel que fa a les funcions privades dels col·legis professionals, es pot aplicar l'Esquema Nacional de Seguretat per determinar les mesures de seguretat aplicables als tractaments automatitzats?

Tot i que no és obligatori aplicar l'Esquema Nacional de Seguretat als tractaments relatius a les funcions privades dels col·legis, constitueix un dels estàndars de seguretat que es pot aplicar per determinar-les.

És obligatòria la figura del responsable de seguretat?

Tot i que l'RGPD no fa referència al responsable de seguretat, l'ENS sí que preveu aquesta figura de manera diferenciada del responsable de la informació i del responsable del servei.

El responsable de seguretat determina las decisions per satisfer els requisits de seguretat de la informació, gestiona els riscos que es puguin plantejar i, entre d'altres, signa la declaració d'aplicabilitat, analitza els informes d'auditoria i n'eleva les conclusions al responsable perquè s'adoptin les mesures correctores adequades.

La prestació de serveis en modalitat de teletreball requereix que s'adoptin mesures de seguretat especials?

Sí. El teletreball comporta un increment dels riscos per a les dades personals que es tracten. Per això, cal que prèviament el col·legi estableixi les mesures necessàries i n'informi el personal, per tal de garantir que el tractament es farà de manera segura mitjançant la regulació del règim de sortida de documents en suport físic, el maquinari i programari que es pot emprar, les condicions en què es s'ha de dur a terme l'accés o comunicació de les dades (xifratge, VPN ...), etc.

Sobre aquesta qüestió, podeu consultar la "[Guia ràpida per teletreballar amb seguretat](#)" (Consorti AOC) o les "[Normes de ciberseguretat per a la prestació de serveis en la modalitat de teletreball](#)" de l'Agència de Ciberseguretat de Catalunya.

Normativa aplicable: art. 32 RGPD; art. 77.1.b) i DA 1a LOPDGDD; ENS.

7.7.6 La gestió dels incidents de seguretat

Es considera un incident o violació de seguretat qualsevol violació de la seguretat que ocasiona la destrucció, la pèrdua o l'alteració accidental o il·lícita de dades personals

transmeses, conservades o tractades d'una altra manera, o la comunicació o l'accés no autoritzats a aquestes dades.

Quan es produeix un incident de seguretat, el responsable del tractament ha d'actuar, sense dilació indeguda, per dur a terme les actuacions següents:

- Identificar l'incident, avaluar-ne els riscos i determinar les mesures a aplicar per minimitzar-los o mitigar-los.
- Documentar l'incident de seguretat, inclosos els fets, els efectes i les mesures correctives adoptades.
- Notificar la violació de seguretat a l'Autoritat Catalana de Protecció de Dades, si escau.
- Comunicar la violació de seguretat a les persones afectades, si escau.

Notificació de les violacions de seguretat a l'Autoritat Catalana de Protecció de Dades

El responsable ha de notificar la violació de seguretat a l'Autoritat Catalana de Protecció de Dades sense dilació indeguda i, si és possible, en un termini màxim de 72 hores des que en tingui constància, tret que sigui improbable que constitueixi un risc per als drets i les llibertats de les persones.

Es pot considerar que es té constància d'una violació de seguretat quan hi ha una certesa que s'ha produït i se'n té un coneixement suficient de la naturalesa i l'abast. La mera sospita que hi ha hagut una fallada o la constatació que ha succeït algun tipus d'incident, sense que se'n coneguin mínimament les circumstàncies, encara no hauria de donar lloc a la notificació ja que, en la majoria dels casos, en aquestes condicions no es pot determinar fins a quin punt hi pot haver un risc per als drets i les llibertats de les persones afectades.

En casos de violacions de seguretat que, per les seves característiques, poden tenir un gran impacte, és recomanable contactar amb l'Autoritat Catalana de Protecció de Dades tan aviat com hi hagi evidències que s'ha produït una situació irregular respecte de la seguretat de les dades. Això, sens perjudici que aquests primers contactes es completin amb una notificació formal, més completa, dins del termini legalment previst.

La notificació ha d'incloure, com a mínim:

- La naturalesa de la violació.
- Les categories de dades i de persones afectades.
- El nom i les dades de contacte del delegat de protecció de dades o, si no n'hi ha, de la persona de contacte.
- Les possibles conseqüències de la violació.
- Les mesures adoptades pel responsable per solucionar la violació.
- Si escau, les mesures aplicades per pal·liar els possibles efectes negatius sobre les persones afectades.

Quan la notificació d'algun d'aquests aspectes no es pugui fer dins les 72 hores, per exemple a causa de la complexitat de determinar-ne completament l'abast, posteriorment es pot fer una notificació complementària, acompanyada d'una explicació dels motius que han ocasionat el retard.

La notificació es pot fer a través del tràmit electrònic disponible a la seu electrònica de l'Autoritat Catalana de Protecció de Dades.

L'encarregat del tractament ha de notificar al responsable del tractament, sense dilació indeguda, les violacions de la seguretat de les dades personals de les quals té coneixement.

Comunicació de les violacions de seguretat a les persones afectades

El responsable ha de comunicar la violació de seguretat a les persones afectades quan comporti un alt risc pels seus drets (per exemple, si es revela informació confidencial com contrasenyes, si es difonen dades sensibles de forma massiva o si es poden produir perjudicis econòmics per a les persones afectades).

S'ha de comunicar sense dilacions indegudes i en un llenguatge clar i senzill.

L'objectiu d'aquesta comunicació és permetre que les persones afectades puguin prendre mesures per protegir-se de les conseqüències de la violació de seguretat, tan aviat com sigui possible.

No és obligatori fer la comunicació personal en els casos següents:

- Si el responsable ha adoptat mesures de protecció adequades, com ara que les dades no siguin intel·ligibles per persones no autoritzades.
- Si el responsable ha aplicat mesures posteriors que garanteixen que ja no hi ha la probabilitat que es concreti l'alt risc.
- Si suposa un esforç desproporcionat. En aquest cas, cal optar per una comunicació pública o una mesura semblant, que informi les persones afectades de manera igualment efectiva.



Un col·legi professional pateix un robatori d'ordinadors portàtils -no encriptats- que emmagatzemaven en el seu disc dur categories especials de dades relatives a col·legiats (com ara, dades de salut) o dades relatives a infraccions disciplinàries. Cal notificar aquesta violació de seguretat a l'APDCAT?

Sí. El col·legi, com a responsable del tractament de les dades dels col·legiats, té l'obligació de notificar la violació a l'Autoritat sense dilació indeguda, i en un termini màxim de 72 hores des que n'ha tingut constància, ja que hi ha un risc de dany per als col·legiats.

Un empleat del col·legi perd un dispositiu mòbil que conté dades personals de les persones usuàries d'un servei del col·legi, les quals estan encriptades amb un algoritme de tecnologia avançada i la clau de xifrat es manté en possessió segura del responsable. Cal notificar aquesta violació de seguretat a l'APDCAT?

En principi no caldria, però algunes circumstàncies poden fer-ho aconsellable. Així, si el responsable no disposa d'una còpia de seguretat de les dades encriptades o el temps de restauració és significatiu, es produirà una violació de disponibilitat, que podria suposar riscos per a les persones, i per tant, podria ser necessari notificar-la a l'Autoritat. Per altra banda, si més endavant es fa evident que la clau de xifrat s'ha vist compromesa o que el programari o algoritme de xifratge és vulnerable, el risc per als drets i llibertats canviarà i, per tant, en aquest moment pot ser exigible.

Es produeix un breu tall d'energia d'uns minuts de durada en el centre d'atenció telefònica del col·legi, que impedeix al seu personal trucar per telèfon o accedir als seus registres. Cal notificar-ho a l'APDCAT?

No. Això no és una violació de declaració obligatòria, però continua sent un incident que cal documentar i registrar en virtut de l'article 33.5 de l'RGPD.

Un treballador del col·legi envia un correu electrònic a un usuari equivocat, amb informació relativa a un expedient de justícia gratuïta. Cal notificar-ho a l'APDCAT?

Si, en tot cas, atesa la informació personal que contenen aquests tipus d'expedients.

I si el correu electrònic s'ha enviat a un altre treballador del mateix col·legi, que no té permisos per accedir a la informació?

Aquesta circumstància és, com a mínim, un incident que cal documentar i registrar. Ara bé, per determinar si és una violació de seguretat que cal notificar, cal valorar si suposa un risc per als drets i llibertats, especialment atenent a la tipologia de dades que s'hagin traslladat, al nombre de persones afectades, les categories de persones afectades (menors, discapacitats, treballadors...), així com els efectes que pot tenir sobre els drets i llibertats de les persones.

Normativa aplicable: considerants 85 i 86 i arts. 33 i 34 RGPD; D.A 9a LOPDGDD.

7.8 La política de protecció de dades

Atesa l'amplitud de les dades recollides pels col·legis professionals i les conseqüències per als drets i llibertats de les persones que es poden derivar dels tractaments que realitzen, especialment en els que tenen més col·legiats o poden tractar informació més sensible, convé que elaborin un document de política de protecció de dades mitjançant el qual es defineixi i es doni a conèixer d'on s'obtenen, com es tracten i com es protegeixen les dades personals que les persones afectades els facilitin o que el col·legi professional reculli per altres vies.

L'RGPD no estableix el contingut detallat que ha de tenir la política de protecció de dades. En qualsevol cas, entre d'altres, pot fer referència a les qüestions següents:

- Mesures previstes per incorporar la protecció de dades en el disseny i la protecció de dades per defecte.
- Mesures adoptades per complir amb el deure d'informació a les persones afectades i per atendre els seus drets.
- Assignació de responsabilitats (designació i atribució de responsabilitats del responsable del tractament, del delegat de protecció de dades, del responsable de seguretat, del responsable del sistema, etc.).
- Les obligacions del personal.
- Establiment de criteris pel que fa al tractament de dades (per exemple, els criteris per determinar els terminis de conservació de la informació, criteris sobre les dades que es recullen de les persones que visiten al web, o previsions relacionades amb les tecnologies que es poden emprar i la seguretat de les dades, protocols d'assignació de permisos, de gestió de contrasenyes, auditories, etc.).
- Establiment de criteris per a la utilització de les TIC per part del personal al servei del col·legi professional (maquinari, programari, teletreball, ús del correu electrònic o altres serveis de missatgeria, xarxes socials, etc.).
- Establiment de protocols per a la gestió, notificació i comunicació de les violacions de seguretat.
- Establiment de criteris i protocols d'actuació pel que fa a la transparència de la informació pública.
- Adhesió a codis de conducta i certificacions, marques i segells de què es disposi.
- Instruments per fer transferències internacionals.
- Mesures per a la conscienciació i formació del personal.

Correspon al delegat de protecció de dades supervisar l'aplicació de la política de protecció de dades.

Normativa aplicable: considerant 78 i arts. 24.2, 39.1.b) RGPD.

7.9 L'adopció d'altres mesures proactives

L'RGPD estableix un seguit d'obligacions que han de complir els responsables i els encarregats del tractament, a les quals ens hem referit en els apartats precedents. Però més enllà d'això, i en virtut del principi de responsabilitat proactiva, han d'adoptar també qualsevol altra mesura tècnica o organitzativa necessària per garantir i poder demostrar que el tractament és conforme amb la normativa de protecció de dades.

La promoció o l'adhesió a codis de conducta i l'obtenció de certificacions, segells o marques poden ser algunes d'aquestes mesures.

7.9.1 Els codis de conducta

Un codi de conducta és un conjunt de normes que voluntàriament assumeix una organització o entitat amb l'objectiu de facilitar el compliment d'una determinada normativa o aconseguir un comportament ètic, en aquest cas pel que fa al tractament de les dades personals.

Segons l'RGPD els poden elaborar les associacions i altres organismes representatius de categories de responsables i encarregats del tractament. L'LOPDGDD estableix que també els poden promoure, entre d'altres, les corporacions de dret públic.

També es poden adherir a codis de conducta els responsables o encarregats als quals no és d'aplicació l'RGPD, per tal d'oferir les garanties adequades en el marc de les transferències de dades personals a tercers països o a organitzacions internacionals fora de l'Espai Econòmic Europeu.

Els responsables o els encarregats han d'assumir compromisos vinculants i exigibles, ja sigui per via contractual o mitjançant altres instruments jurídicament vinculants, per aplicar aquestes garanties adequades, incloses les relatives als drets de les persones afectades.

El contingut del codi de conducta ha d'especificar l'aplicació de la normativa de protecció de dades pel que fa, per exemple, a:

- El tractament lleial i transparent.
- Els interessos legítims perseguits pels responsables en contextos específics.
- La recollida de dades personals.
- La pseudonimització de dades personals.
- La informació proporcionada a les persones afectades.
- L'exercici dels drets de les persones afectades.
- La informació que es proporciona als nens i la protecció d'aquests, així com la manera d'obtenir el consentiment dels titulars de la potestat parental o de la tutela sobre el nen.
- Les mesures i els procediments relatius a les polítiques de protecció de dades, la protecció de dades en el disseny i la protecció de dades per defecte, l'anàlisi de riscos i les mesures per garantir la seguretat del tractament.
- La notificació de violacions de seguretat a l'autoritat de control i la comunicació d'aquestes violacions a les persones afectades.
- La transferència de dades personals a tercers països o a organitzacions internacionals.

Els procediments extrajudicials i altres procediments de resolució de conflictes per resoldre les controvèrsies entre els responsables del tractament i les persones afectades respecte del tractament.

Els col·legis, consells de col·legis o associacions de col·legis que promoguin el codi han de presentar-ne el projecte o, si escau, la modificació o ampliació a l'Autoritat Catalana de Protecció de Dades. L'Autoritat ha de dictaminar si el projecte de codi o la modificació o ampliació és conforme a la normativa vigent i, si escau, aprovar-lo, registrar-lo i publicar-lo, sempre que el codi afecti només activitats de tractament en un estat membre.

L'Autoritat Catalana de Protecció de Dades ofereix el seu assessorament durant la fase d'elaboració del projecte de codi, per tal de facilitar-ne la tramitació posterior.

Normativa aplicable: art. 40 RGPD; 38 i 77.1.g) LOPDGDD.

7.9.2 Les certificacions, segells i marques

La finalitat principal de les certificacions, segells i marques és demostrar que els responsables i encarregats del tractament compleixen l'RGPD. Aquests instruments no en limiten les responsabilitats pel que fa al compliment de l'RGPD, però serveixen per avaluar més ràpidament el nivell de protecció de dades de productes i serveis. També pot actuar com a mecanisme a tenir en compte a l'hora d'acreditar que se selecciona un encarregat del tractament que ofereix garanties adequades; també a l'hora de fer transferències internacionals; o per graduar eventuais sancions per incompliment.

Aquests instruments poden proporcionar directrius als responsables i als encarregats del tractament, tant respecte de la identificació i la mitigació dels riscos com respecte del compliment del deure de transparència.

La certificació és voluntària, ha d'estar disponible a través d'un procés transparent i pot ser expedida al responsable o l'encarregat del tractament per un període màxim de tres anys, renovables en les mateixes condicions, sempre que es continuïn complint els requisits pertinents. La certificació la pot expedir una autoritat de control o un organisme de certificació acreditat.

Sobre aquesta qüestió, es recomana consultar les **Directrius** 1/2018 del Comitè Europeu de Protecció de Dades (CEPD), sobre certificació i criteris de certificació d'acord amb els articles 42 i 43 del Reglament 2016/679, disponible a la web de l'APDCAT.

Normativa aplicable: considerants 77, 100 i arts. 42, 43, 57.1.n) RGPD; 39 LOPDGDD.

8. Obligacions del responsable un cop finalitza el tractament; la conservació de les dades

El principi de minimització, i la seva manifestació concretada en el principi de limitació del termini de conservació, obliguen a cessar en el tractament i suprimir i bloquejar les dades un cop deixen de ser necessàries per a la finalitat per a la qual es van recollir.

8.1 Limitació del termini de conservació

Les dades s'han de conservar de manera que només es permeti la identificació de les persones afectades durant el temps estrictament necessari per als fins del tractament de les dades. Quan les dades deixin de ser necessàries o pertinents, s'han de suprimir.

Únicament es poden conservar per un termini superior si les dades es conserven anonimitzades, o bé es conserven amb finalitats d'arxiu en interès públic, de recerca científica o històrica o finalitats estadístiques. Això, sempre que s'apliquin mesures tècniques i organitzatives adequades per protegir els drets i les llibertats de la persona afectada.

No obstant això, cal tenir en compte que la supressió no equival a la destrucció, atès que la normativa de protecció de dades preveu el deure de bloqueig de les dades suprimides. Sobre això, ens remetem a l'apartat següent.

Cal informar la persona afectada respecte del termini de conservació de les dades i, si no és possible concretar-lo, se l'ha d'informar sobre quins són els criteris utilitzats per determinar-lo.

D'acord amb la legislació d'arxius, aplicable també a les corporacions de dret públic, els documents de les administracions públiques s'han de sotmetre a una avaluació, en la qual se n'ha de determinar el termini de conservació (atenent al seu valor cultural, informatiu o jurídic) o bé l'eliminació, d'acord amb el procediment establert reglamentàriament.

El termini de conservació s'estableix a través de les Taules d'Accés i Avaluació Documental (TAAD), aprovades pel Departament de Cultura a proposta de la Comissió Nacional d'Accés, Avaluació i Tria Documental (CNAATD). Al [web del Departament de Cultura](#) es poden consultar les TAAD aprovades per a les diferents sèries documentals avaluades.

Tot i que es tracta d'una qüestió diferent, perquè en aquest cas només s'ha de limitar el tractament, però no suprimir les dades, també cal tenir en compte la necessitat de limitar el temps d'exposició al públic, en particular a través d'internet, de determinades informacions. Així, si s'ha establert un termini, la informació només ha d'estar publicada fins que aquest termini transcorri. Si no hi ha un termini d'exposició establert, cal cessar en la publicació quan s'hagi assolit la finalitat per a la qual es va publicar.

En els cas dels col·legiats, cal tenir en compte que per a determinats professionals la normativa aplicable estableix un determinat període de conservació mínima obligatòria, com per exemple en el cas de la normativa aplicable a la conservació de la història clínica. En aquest cas, la informació es pot haver de conservar fins i tot més enllà de la jubilació o de la mort d'un professional autònom. Per fer front a aquests supòsits de cessament de la activitat, i per garantir la confidencialitat i també la disponibilitat de les dades, pot ser d'utilitat que el col·legi professional prevegi un servei de custòdia d'aquesta documentació. Aquest servei, contractat pel mateix professional o pels seus hereus, comportaria que el col·legi fos responsable de la custòdia dels expedients, com també de l'atenció dels drets de les persones afectades.



El col·legi ha de destruir totes les dades de què disposa sobre un col·legiat quan el col·legiat es dona de baixa? Quant de temps han de conservar les dades els col·legis professionals?

Els col·legis professionals han de conservar la informació personal de la qual disposen mentre resulti necessària per exercir les funcions que legalment tenen atribuïdes, o siguin necessàries per mantenir les relacions jurídiques establertes amb les persones col·legiades. Quan les dades deixin de ser necessàries, s'han de suprimir.

Les dades personals s'han de suprimir un cop deixen de ser necessàries per a la finalitat per a la qual es van recollir o, si escau, un cop finalitzats els terminis de conservació establerts per la llei o a les taules d'avaluació documental aprovades d'acord amb la Llei 10/2001, de 13 de juliol, d'arxius i documents. La supressió comporta el bloqueig de les dades durant els terminis de prescripció en què es pugui exigir algun tipus de responsabilitat derivada del tractament. Acomplert aquest termini, el qual pot variar segons la informació tractada i les responsabilitats que es poden generar, s'ha de procedir a l'eliminació efectiva de la informació personal.

Les dades només es poden conservar per un termini superior si es conserven anonimitzades, o bé si es conserven amb finalitats d'arxiu en interès públic, de recerca científica o històrica o finalitats estadístiques. Això, sempre que s'apliquin mesures tècniques i organitzatives adequades per protegir els drets i les llibertats de la persona afectada.

Es compleix amb l'obligació de suprimir 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 reidentificar el titular, compleix l'obligació de supressió, sens perjudici del deure de bloqueig.

Un col·legi de metges es pot fer càrrec de les històries clíniques que eren responsabilitat d'un metge col·legiat que ha cessat en la seva activitat?

Sí. En aquest cas, el col·legi professional és responsable de la custòdia dels expedients, com també de l'atenció dels drets d'accés, rectificació, supressió, oposició, limitació del tractament i portabilitat de les persones afectades.

Un col·legi professional està legitimat per acceptar la donació d'un fons documental?

D'acord amb la normativa d'arxius, i amb la normativa reguladora de col·legis professionals, pot haver-hi suficient habilitació en normes amb rang de llei perquè el col·legi es pugui fer càrrec d'un fons documental relacionat amb les seves funcions, sense haver de disposar del consentiment dels afectats. A partir del marc normatiu aplicable i del principi de limitació de finalitat, el col·legi, com a responsable, ha de determinar, quines dades del fons documental poden ser pertinents, adequades i limitades al mínim necessari per a la finalitat històrica, estadística o científica prevista i, en conseqüència, quines es poden conservar per posteriors sol·licituds d'accés de tercers i quines no.

Normativa aplicable: art. 5.1.e), 13 i 14 RGPD; art. 32 LOPDGDD; art. 9 LAD; art. 8 Decret 13/2008.

8.2 El deure de bloqueig

El responsable del tractament està obligat a bloquejar les dades quan les rectifiqui o les suprimeixi.

Es tracta d'una figura que no està prevista a l'RGPD però sí a l'LOPDGG i que s'ha d'aplicar tant quan se suprimeixen com quan es rectifiquen les dades.

El bloqueig consisteix en la identificació i la reserva de les dades, amb mesures tècniques i organitzatives per impedir-ne el tractament, inclosa la visualització, excepte per posar-les a disposició dels jutges i tribunals, el ministeri fiscal o les administracions públiques competents, en particular de les autoritats de protecció de dades, per exigir possibles responsabilitats derivades del tractament i només durant el termini de prescripció d'aquestes responsabilitats. Les dades bloquejades no es poden tractar amb cap altra finalitat.

Transcorregut aquest termini les dades s'han de destruir.

Quan la configuració del sistema d'informació no permeti el bloqueig o calgui una adaptació que impliqui un esforç desproporcionat, s'ha de fer una còpia segura de la informació de manera que consti una evidència digital, o d'una altra naturalesa, que permeti acreditar que la còpia és autèntica, la data del bloqueig i que les dades no s'han manipulat durant aquest període.

L'obligació de bloqueig no és d'aplicació:

- A les dades dels sistemes de videovigilància.
- A les dades incorporades a sistemes de denúncies internes que no s'hagin cursat.
- Quan l'Autoritat Catalana de Protecció de Dades n'hagi establert l'exempció en algun d'aquests supòsits:

- Quan per la naturalesa de les dades o pel nombre elevat d'afectats, conservar-les pugui suposar un risc elevat per a les persones afectades.
- Quan conservar les dades bloquejades pot suposar un esforç desproporcionat per al responsable del tractament.



Davant l'exercici d'un dret de supressió, s'han de bloquejar les dades? Cal informar del bloqueig la persona afectada?

Sí. El responsable del tractament està obligat a bloquejar les dades quan les rectifiqui o les suprimeixi, llevat que es tracti de dades obtingudes amb sistemes de videovigilància, dades incorporades a sistemes de denúncies internes que no s'hagin cursat o si l'Autoritat Catalana de Protecció de Dades n'ha establert l'exempció, en algun dels supòsits de l'article 32.5 de l'LOPDGDD.

En la resolució del dret de supressió, convé informar que les dades es conservaran bloquejades i que no es podran tractar per a cap finalitat, excepte per posar-les a disposició dels jutges i tribunals, el ministeri fiscal o les administracions públiques competents, en particular de les autoritats de protecció de dades, per exigir possibles responsabilitats derivades del tractament i només durant el termini de prescripció d'aquestes responsabilitats.

Normativa aplicable: arts. 22.3, 24.4 i 32 LOPDGDD.

9. Règim de responsabilitat

La vulneració del dret a la protecció de dades genera responsabilitats, que es poden exigir mitjançant una reclamació o una denúncia davant l'APDCAT o mitjançant una reclamació de responsabilitat per danys davant el col·legi professional o el consell de col·legis responsable o encarregat del tractament o, si escau, mitjançant l'exercici d'accions davant els òrgans jurisdiccionals.

En determinats casos, pot donar lloc també a l'exigència de responsabilitats penals a les persones que hagin comès algun delictes contra els drets de les persones, en especial delictes contra la intimitat.

9.1 Reclamacions davant l'Autoritat Catalana de Protecció de Dades

Es pot reclamar davant l'Autoritat Catalana de Protecció de Dades per denunciar fets que constitueixin una infracció de la normativa de protecció de dades o en casos en què el responsable del tractament desatengui els drets d'accés, rectificació, supressió, oposició i portabilitat, així com del dret a la limitació del tractament i el dret a no ser objecte de decisions automatitzades. La reclamació també pot tenir per objecte ambdues qüestions a la vegada.

L'Autoritat Catalana de Protecció de Dades ha d'informar les persones afectades sobre el curs o el resultat de la reclamació presentada en el termini de tres mesos.

Reclamacions per denunciar infraccions de la normativa de protecció de dades

Qualsevol persona pot presentar una reclamació davant l'Autoritat Catalana de Protecció de Dades per comunicar fets que poden ser constitutius d'una infracció de la normativa de protecció de dades.

El règim sancionador previst a la normativa de protecció de dades és aplicable:

- Als responsables dels tractaments.
- Als encarregats dels tractaments.
- Als representants dels responsables o encarregats dels tractaments no establerts al territori de la Unió Europea.
- A les entitats de certificació.
- A les entitats acreditades de supervisió dels codis de conducta.

En canvi, no és aplicable al delegat de protecció de dades.

La tipificació de les infraccions i les sancions està prevista amb caràcter general als articles 83 i 84 de l'RGPD i als articles 71 a 76 de l'LOPDGDD.

Les sancions aplicables s'han de graduar d'acord amb les circumstàncies previstes a l'article 83.2 de l'RGPD.

Pel que fa als tractaments dels col·legis professionals relatius a l'exercici de potestats públiques, s'ha de tenir en compte que se'ls aplica el règim sancionador especial previst a l'LOPDGDD. En virtut d'aquest règim, si s'ha comès alguna infracció, l'Autoritat ha de dictar una resolució que sancioni amb una amonestació i, si escau, imposi les mesures a adoptar perquè cessi la conducta o es corregeixin els efectes de la infracció.

En aquests casos, la resolució s'ha de notificar al responsable o l'encarregat del tractament, a l'òrgan del qual depengui jeràrquicament, si escau, i als reclamants que tinguin la condició d'interessat, si escau.

Les actuacions i les resolucions sancionadores que es dictin en relació amb l'exercici de potestats públiques també s'han de comunicar al Síndic de Greuges.

A més, l'autoritat de protecció de dades ha de proposar la iniciació d'actuacions disciplinàries quan hi hagi indicis suficients per fer-ho. En aquest cas, el procediment i les sancions que ha d'aplicar el col·legi professional són els que estableix la legislació sobre règim disciplinari o sancionador que sigui aplicable.

Així mateix, quan les infraccions siguin imputables a autoritats i directius, i s'acrediti que hi ha informes tècnics o recomanacions per al tractament que no s'hagin atès degudament, com ara que no s'hagin atès els informes del delegat de protecció de dades, cal incloure a la resolució en què s'imposa la sanció una amonestació amb la denominació del càrrec responsable i se n'ha d'ordenar la publicació al butlletí oficial que correspongui.

A les infraccions comeses relatives a la resta de tractaments duts a terme pel col·legi en exercici de funcions que no tinguin caràcter públic, així com les comeses pels encarregats del tractament de dret privat que actuen respecte de tractaments dels quals és responsable el col·legi, els és d'aplicació el règim sancionador general.

Els terminis de prescripció de les infraccions són els següents:

- Per a les infraccions considerades molt greus, tres anys.
- Per a les infraccions considerades greus, dos anys.
- Per a les infraccions considerades lleus, un any.

La prescripció s'interromp quan s'inicia, amb coneixement de l'interessat, el procediment sancionador. El termini de prescripció es reinicia si l'expedient sancionador està paralitzat durant més de sis mesos per causes no imputables al presumpte infractor.

Els terminis de prescripció de les sancions, són els següents:

- Les sancions per import igual o inferior a 40.000 euros, al cap d'un any.
- Les sancions per import comprès entre 40.001 i 300.000 euros, al cap de dos anys.
- Les sancions per import superior a 300.000 euros, al cap de tres anys.

El termini de prescripció de les sancions es comença a comptar des de l'endemà del dia en què la resolució per la qual s'imposa la sanció és executable o hagi transcorregut el termini per recórrer-la. S'interromp per la iniciació, amb coneixement de l'interessat, del procediment d'execució, i torna a transcórrer si està paralitzat durant més de sis mesos per causa no imputable a l'infractor.

Normativa aplicable: arts. 83 i 84 RGPD; art. 70 a78 LOPDGDD; arts. 21 a 25 i DT 2a LACPD.

Reclamacions davant la desatenció de sol·licituds d'exercici de drets

A més, les persones afectades poden presentar una reclamació davant l'Autoritat Catalana de Protecció de Dades quan se'ls denegui, en part o totalment, l'exercici dels drets d'accés, de rectificació, de supressió, de limitació del tractament, de portabilitat o d'oposició, o no en rebin resposta.

Per fer-ho, cal haver exercit prèviament el dret davant del responsable del fitxer i que l'hagi denegat, o hagi transcorregut el termini per fer-ho sense que se li hagi notificat la resposta.

L'Autoritat, a través de la tramitació d'un procediment de tutela de drets, resoldrà en el termini de sis mesos, si la denegació és procedent o improcedent. Si en el termini de sis mesos l'Autoritat no ha notificat la resolució de la reclamació de tutela de drets, la persona afectada pot considerar que s'ha desestimat.

Contra aquesta resolució o davant la manca de resolució en el termini esmentat, es pot presentar un recurs potestatiu de reposició davant la directora de l'Autoritat, o directament recurs contenciós administratiu davant el jutjat contenciós administratiu de Barcelona.

Si s'han vulnerat altres drets o hi ha hagut actuacions contràries a la normativa de protecció de dades, es pot presentar una denúncia davant l'Autoritat.



Davant una vulneració del dret a la protecció de dades que hagi provocat un dany o perjudici, la persona afectada pot reclamar simultàniament davant l'APDCAT i per via judicial?

Sí. La persona afectada pot denunciar la infracció davant l'Autoritat Catalana de Protecció de Dades, per via administrativa i simultàniament o posteriorment (tenint en compte els diferents terminis per fer-ho) també pot presentar demanda per via judicial, per reclamar la indemnització per danys i perjudicis.

Normativa aplicable: art. 77 RGPD; art. 16 LACPD.

9.2. Reclamacions davant els òrgans jurisdiccionals

Les persones afectades poden interposar recurs contenciós administratiu contra una resolució de l'Autoritat que els afecti o davant la manca de resolució en el termini de sis mesos d'una reclamació per la tutela drets.

A més, qualsevol persona afectada també té dret a interposar un recurs contenciós administratiu si l'Autoritat Catalana de Protecció de Dades no tramita una reclamació o no informa la persona afectada sobre el curs o el resultat de la reclamació presentada, en el termini de tres mesos.

Normativa aplicable: art. 78 RGPD.

9.3. Indemnització per danys i perjudicis

Qualsevol persona que hagi sofert danys i perjudicis, materials o immaterials, com a conseqüència d'una infracció de la normativa sobre protecció de dades, té dret a percebre una indemnització del responsable o de l'encarregat del tractament.

Si el dany o perjudici es produeix en el marc de les funcions públiques del col·legi professional, la responsabilitat s'exigeix d'acord amb el règim de responsabilitat patrimonial previst a l'LRJSP.

Si el dany es produeix en el marc de la resta de funcions del col·legi professional, la responsabilitat s'exigeix davant dels òrgans de la jurisdicció ordinària, és a dir, davant dels jutges i tribunals competents en l'ordre civil.

L'encarregat únicament ha de respondre dels danys i perjudicis causats pel tractament quan no hagi complert les obligacions de la normativa de protecció de dades adreçades específicament als encarregats o quan hagi actuat al marge o en contra de les instruccions legals del responsable.

Quan més d'un responsable o d'un encarregat del tractament, o quan un responsable i un encarregat hagin participat en la mateixa operació de tractament i siguin responsables del dany o perjudici causat, hi responen solidàriament, sens perjudici del dret a reclamar als altres responsables o encarregats la part que correspongui a la seva part de responsabilitat.



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

Sí, poden exercir una acció de reclamació de responsabilitat o, si escau, en el cas de les funcions públiques del col·legi, una reclamació de responsabilitat patrimonial d'acord amb la normativa reguladora del règim de responsabilitat patrimonial de les administracions públiques, davant del col·legi professional o, si escau, davant dels òrgans jurisdiccionals.

Normativa aplicable: art. 82 RGPD.

10. Autoritat de control: l'Autoritat Catalana de Protecció de Dades.

10.1 Naturalesa i objecte

És l'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.

L'APDCAT vetlla perquè les entitats del sector públic de Catalunya que tracten les dades personals dels ciutadans respectin el dret a la protecció de dades personals, informa les persones sobre els seus drets, com s'exerceixen, què poden fer si no es respecten, i atén les seves reclamacions.

Normativa aplicable: arts. 1 i 2 LACPD.

10.2 Àmbit d'actuació

Els ens que estan dins l'àmbit d'actuació de l'APDCAT són:

- Les institucions públiques de Catalunya.
- L'Administració de la Generalitat.
- Els col·legis professionals.
- 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 compleixen, com a mínim, un dels tres requisits següents amb relació a la Generalitat, als ens locals o als ens que en depenen:
 - El seu capital pertany majoritàriament als ens públics esmentats.
 - Els seus ingressos pressupostaris provenen majoritàriament dels ens públics esmentats.
 - En els seus òrgans directius, els membres designats per aquests ens públics són 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 col·legis professionals, si es tracta de fitxers o tractaments destinats a exercir 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.

Per tant, pel que fa als col·legis professionals, els consells de col·legis i els ens o organismes que hi estan vinculats o en depenen que exerceixen les seves funcions exclusivament a Catalunya, l'APDCAT és l'autoritat de control competent respecte dels tractaments que duen a terme, tant si és en l'exercici de les funcions públiques que tenen atribuïdes o d'altres funcions.



La delegació a Catalunya d'un col·legi d'àmbit estatal, està inclosa en l'àmbit d'actuació de l'Autoritat Catalana de Protecció de Dades?

No. L'àmbit d'actuació de l'Autoritat Catalana de Protecció de Dades es limita als col·legis i consells de col·legis que compleixen les seves funcions exclusivament en l'àmbit territorial de Catalunya.

Normativa aplicable: art. 156 EAC; 3 LACPD.

10.3 Organització

L'Autoritat disposa de dos òrgans:

- El director o directora, 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.

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

10.4 Funcions i potestats

L'RGPD atribueix a totes les autoritats de protecció de dades les funcions següents:

- Controlar i garantir l'aplicació de la normativa de protecció de dades.
- Promoure la sensibilització i la comprensió del públic respecte dels riscos, les normes, les garanties i els drets relacionats amb el tractament. Les activitats adreçades específicament als nens han de ser objecte d'una atenció especial.
- Assessorar, de conformitat amb el dret dels estats membres, el parlament nacional, el govern i altres institucions i organismes, sobre les mesures legislatives i administratives relatives a la protecció dels drets i les llibertats de les persones físiques pel que fa al tractament.
- Promoure la sensibilització dels responsables i els encarregats del tractament sobre les obligacions que els corresponen d'acord amb la normativa de protecció de dades.

- Prèvia sol·licitud, facilitar informació a qualsevol persona afectada sobre l'exercici dels seus drets, i si escau cooperar amb les autoritats de control d'altres estats membres amb aquesta finalitat.
- Tramitar les reclamacions presentades per una persona afectada, per un organisme, una organització o una associació; així mateix, investigar el motiu de la reclamació i informar el reclamant sobre el curs i el resultat de la investigació en un termini raonable.
- Cooperar amb altres autoritats de control, en particular compartint informació, i prestar assistència mútua amb la finalitat de garantir la coherència en l'aplicació i l'execució de l'RGPD.
- Dur a terme investigacions sobre l'aplicació de l'RGPD, en particular d'acord amb la informació rebuda d'una altra autoritat de control o d'una altra autoritat pública.
- Fer un seguiment de canvis rellevants que tenen incidència en la protecció de dades personals, en particular els relatius al desenvolupament de les tecnologies de la informació i la comunicació i a les pràctiques comercials.
- Adoptar les clàusules contractuals tipus per a encarregats del tractament.
- Elaborar i mantenir una llista relativa al requisit de l'avaluació d'impacte relativa a la protecció de dades.
- Oferir assessorament sobre les operacions de tractament sotmeses a consulta prèvia.
- Encoratjar l'elaboració de codis de conducta i dictaminar i aprovar els codis de conducta que ofereixen garanties suficients.
- Fomentar la creació de mecanismes de certificació de la protecció de dades i de segells i marques de protecció de dades, i aprovar els criteris de certificació.
- Dur a terme, si escau, una revisió periòdica de les certificacions expedides.
- Elaborar i publicar els criteris per acreditar els organismes de supervisió dels codis de conducta i dels organismes de certificació.
- Acreditar els organismes de supervisió dels codis de conducta i els organismes de certificació.
- Autoritzar les clàusules contractuals i les disposicions a què es refereix l'article 46, apartat 3, de l'RGPD.
- Aprovar normes corporatives vinculants.
- Contribuir a les activitats del Comitè Europeu de Protecció de Dades.
- Portar registres interns de les infraccions de l'RGPD i de les mesures que s'han adoptat.
- Dur a terme qualsevol altra funció relacionada amb la protecció de les dades personals.

A més, l'LACPD també estableix, entre d'altres, les funcions següents:

- Respondre les consultes que formulen les entitats del seu àmbit d'actuació sobre la protecció de dades personals en poder de les administracions públiques i col·laborar

amb aquestes entitats, en la difusió de les obligacions derivades de la legislació reguladora d'aquestes matèries.

- Emetre l'informe preceptiu sobre les disposicions que afecten la protecció de dades personals de la Generalitat. En el cas dels col·legis professionals, aquest informe és potestatiu.
- Elaborar plans d'auditoria.

El responsable i l'encarregat del tractament han de cooperar amb l'APDCAT quan els ho sol·liciti en exercici de les seves funcions.

Per exercir aquestes funcions, l'APDCAT compta amb les potestats següents:

Poders d'investigació:

- Ordenar al responsable i a l'encarregat del tractament, i si escau al seu representant, que facilitin qualsevol informació que necessiti per complir les seves funcions.
- Dur a terme investigacions en forma d'auditories de protecció de dades.
- Revisar les certificacions que s'expedeixen en virtut del que disposa l'article 42, apartat 7, de l'RGPD.
- Notificar al responsable o a l'encarregat del tractament les presumptes infraccions de la normativa de protecció de dades.
- Obtenir del responsable i de l'encarregat del tractament l'accés a totes les dades personals i a tota la informació necessària per exercir les seves funcions.
- Obtenir l'accés a tots els locals del responsable i de l'encarregat del tractament, inclosos qualssevol equips i mitjans de tractament de dades, de conformitat amb el dret processal de la Unió o dels estats membres.

Poders correctius:

- Adreçar a qualsevol responsable o encarregat del tractament una advertència, si les operacions de tractament previstes poden infringir el que disposa la normativa de protecció de dades.
- Adreçar a qualsevol responsable o encarregat del tractament una amonestació, si les operacions de tractament han infringit el que disposa l'RGPD.
- Ordenar al responsable o a l'encarregat del tractament que atengui les sol·licituds d'exercici dels drets de la persona afectada, en virtut del que disposa l'RGPD.
- Ordenar al responsable o l'encarregat del tractament que les operacions de tractament s'ajustin a les disposicions de l'RGPD i l'LOPDGDD, d'una determinada manera i dins d'un termini especificat, si escau.
- Ordenar al responsable del tractament que comuniqui a la persona afectada les violacions de la seguretat de les dades personals.
- Imposar una limitació temporal o definitiva del tractament, inclosa la prohibició.

- Ordenar la rectificació o la supressió de dades personals o la limitació de tractament, i la notificació d'aquestes mesures als destinataris als quals s'han comunicat dades personals.
- Retirar o ordenar a l'organisme de certificació que retiri una certificació emesa, o ordenar a l'organisme de certificació que no l'emeti, si no es compleixen els requisits per la certificació o si es deixen de complir.
- Imposar una multa administrativa, a més de les mesures esmentades en aquest apartat o en lloc d'aquestes mesures, segons les circumstàncies de cada cas particular.
- Ordenar la suspensió dels fluxos de dades cap a un destinatari situat en un tercer país o cap a una organització internacional.

Poders d'autorització i consultius:

- Assessorar el responsable del tractament, mitjançant la consulta prèvia.
- Emetre, per iniciativa pròpia o prèvia sol·licitud, dictàmens destinats als ens que estan dins l'àmbit d'actuació de l'Autoritat, sobre qualsevol assumpte relacionat amb la protecció de les dades personals.
- Autoritzar el tractament quan es requereixi l'autorització prèvia.
- Emetre un dictamen i aprovar projectes de codis de conducta.
- Acreditar els organismes de certificació.
- Expedir certificacions i aprovar criteris de certificació.
- Adoptar les clàusules tipus de protecció de dades per a l'encarregat del tractament.
- Autoritzar les clàusules contractuals esmentades a l'article 46.3.a) de l'RGPD.
- Autoritzar els acords administratius que preveu l'article 46.3.b) de l'RGPD.
- Aprovar normes corporatives vinculants.

Normativa aplicable: arts. 31, 57 i 58 RGPD; arts. 5 i 15 i s. LACPD; arts. 57 a 62 LOPDGDD.

Abreviatures

EAC: Estatut d'autonomia de Catalunya.

EBEP: Text refós de la Llei de l'Estatut bàsic de l'empleat públic, aprovat pel Reial decret legislatiu 5/2015, de 30 d'octubre.

ENS: Esquema Nacional de Seguretat, aprovat pel Reial decret 311/2022, de 3 de maig.

ET: Text refós de l'Estatut dels treballadors, aprovat pel Reial decret legislatiu 2/2015, de 23 de octubre.

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

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

LCSP: Llei 9/2017, de 8 de novembre, de contractes del sector públic, per la qual es transposen a l'ordenament jurídic espanyol les directives del Parlament Europeu i del Consell 2014/23/UE i 2014/24/UE, de 26 de febrer de 2014.

LEC: Llei 23/1998, de 30 de desembre, d'estadística de Catalunya.

Llei 7/2006: Llei 7/2006, de 31 de maig, de l'exercici de professions titulades i dels col·legis professionals.

Llei 2/1974: Llei 2/1974, de 13 de febrer, de col·legis professionals.

Llei 2/2007: Llei 2/ 2007, de 15 de març, de societats professionals.

Llei orgànica 7/2021: Llei orgànica 7/2021, de 26 de maig, de protecció de dades personals tractades per a fins de prevenció, detecció, investigació i enjudiciament d'infraccions penals i d'execució de sancions penals.

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

LOPDGDD: Llei orgànica 3/2018, de 5 de de desembre, de protecció de dades personals i garantia dels drets digitals.

LOVFCs: 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.

LRJSP: Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic.

LT: Llei 19/2013, de 9 de desembre, de transparència, accés a la informació pública i bon govern.

LTC: Llei 19/2014, del 29 de desembre, de transparència, accés a la informació pública i bon govern.

RGPD: Reglament (UE) núm. 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE.

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.

Annexos

Annex 1: Model de clàusula informativa per a documents de recollida de dades pel col·legi professional.

Annex 2: Model de clàusula informativa per actualitzar les dades que apareixen a la llista o guia de persones col·legiades.

Annex 3: Model per exercir el dret d'accés.

Annex 4: Model per exercir el dret de rectificació i, si escau, el de limitació del tractament.

Annex 5: Model per exercir el dret de supressió.

Annex 6: Model per exercir el dret d'oposició i, si escau, el de limitació del tractament.

Annex 7: Model per exercir el dret de limitació del tractament.