

Pautes de protecció de dades per als centres educatius

Actualització: 2024

Colecció de guies. Núm. 3



© 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
1. Objete	5
2. L'escola i l'RGPD: oportunitat per revisar el compliment.....	5
2.1 <i>Accountability</i> : principi de responsabilitat proactiva	5
2.2 L'enfocament al risc	6
2.3 Protecció de dades des del disseny i per defecte	6
3. Obligacions: Tractament de dades a les escoles	7
3.1 Dades personals	7
3.1.1 Origen de les dades	7
3.1.2 Operacions o gestions en què es tracten dades	8
3.1.3 De qui es tracten les dades?	8
3.1.4 Quines dades es tracten?.....	9
3.1.5 Categories especials de dades. Novetats	9
3.2 Qui tracta les dades personals?.....	10
3.2.1 Responsable del tractament.....	10
3.2.2 Encarregat del tractament	11
3.3 Registre de les activitats de tractament de dades (RAT).....	12
3.3.1 Definició del registre de les activitats de tractament de dades (RAT)	12
3.3.2 Com s'ha d'organitzar el registre d'operacions de tractament?	13
4. Legitimitat. Quan podem tractar dades personals?	13
4.1 Principis. Com complir amb l'RGPD	13
4.1.1 Licitud, lleialtat i transparència	13
4.1.2 Limitació de la finalitat	13
4.1.3 Minimització de les dades	14
4.1.4 Exactitud	14
4.1.5 Limitació del termini de conservació.....	14
4.1.6 Integritat i confidencialitat	14
4.2 Transparència de la informació	15
4.2.1 Informació a la persona interessada	15

4.2.2	Excepcions al dret d'informació	16
4.2.3	On i com cal informar?	16
4.2.4	En quin moment del tractament s'ha de donar la informació?	17
4.3	Bases jurídiques per tractar dades personals	18
4.3.1	LOE: habilitació per al tractament de dades a les escoles	19
4.3.2	Relació contractual. Habilitació del professorat i treballadors dels centres	19
4.3.3	Consentiment: Serveis diferents de la funció docent i orientadora	19
4.3.4	Consentiment: Menores d'edat	20
4.3.5	Consentiment: Xarxes i menors	21
4.3.6	Revocació del consentiment	21
5.	Drets de la persona interessada	21
5.1	Dret de l'autodeterminació informativa	21
5.1.1	Dret d'accés	22
5.1.2	Dret de rectificació	22
5.1.3	Dret de supressió o dret a l'oblit	23
5.1.4	Dret a la limitació del tractament	23
5.1.5	Dret a la portabilitat de les dades	24
5.1.6	Dret d'oposició	24
5.1.7	Dret a no ser objecte de decisions individuals automatitzades	25
5.2	Exercici dels drets	25
5.2.1	Qui pot exercir aquests drets?	25
5.2.2	Procediment. Com es fan efectius els drets?	25
5.2.3	On s'ha de presentar la sol·licitud?	26
5.2.4	Reclamació davant la manca d'atenció dels drets	27
6.	El deure de secret	27
7.	Delegat de protecció de dades	28
7.1	La figura del delegat de protecció de dades a les escoles	28
7.2	Quins requisits o qualificacions ha de tenir?	28
8.	Avaluació d'impacte relativa a la protecció de dades	29
8.1	Com es determina la necessitat de fer una avaluació d'impacte i quin contingut ha de tenir?	29
8.2	Consulta prèvia	30

9. Mesures de seguretat	30
9.1 Com es du a terme una anàlisi de riscos?	30
9.2 Notificació de violacions de seguretat.....	32
9.2.1 Quin és el termini per notificar una violació de seguretat de les dades a l'Autoritat de control?	33
9.2.2 Quin ha de ser el contingut de la notificació d'una violació de la seguretat de les dades a l'Autoritat de control?	33
9.2.3 Quan és probable que una violació de seguretat comporti un risc alt per als drets de les persones afectades?.....	34
9.2.4 Quina és la finalitat de comunicar una violació de seguretat a les persones afectades?	34
9.2.5 Què pot passar si no es notifica una violació de seguretat de les dades?	34

El 27 d'abril de 2016 es va aprovar el Reglament (UE) 2016/679 del Parlament i del Consell, 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, en endavant RGPD), de plena aplicació des del 25 de maig de 2018.

Aquesta nova regulació, que per primera vegada es fa a través d'un reglament europeu, comportarà canvis significatius en la protecció de dades de caràcter personal, tant des del punt de vista dels drets de les persones com de les obligacions de les persones i entitats que tracten dades de caràcter personal.

1. Objete

L'escola té un paper fonamental en la garantia del dret de protecció de dades personals, no només com a subjecte responsable del tractament adequat de la informació de les persones que s'hi relacionen, sinó també com a element essencial en la seva difusió, atès que pot permetre que les persones -menors-, ja des del moment de la seva formació a l'escola, el conegui i l'utilitzi.

Aquest document pretén donar el suport necessari als centres educatius (en endavant les escoles) per establir les polítiques i els procediments necessaris en el tractament de dades que han de dur a terme en el funcionament normal d'un centre. Però sobretot suposa una oportunitat per als centres educatius per revisar les seves pràctiques en matèria de protecció de dades i privacitat.

2. L'escola i l'RGPD: oportunitat per revisar el compliment

2.1 *Accountability*: principi de responsabilitat proactiva

El responsable del tractament, l'escola –en el cas de l'escola pública serà el Departament d'Educació el que haurà d'establir si el responsable és cada centre o el mateix Departament– ha de garantir i poder demostrar que el tractament és conforme a la normativa de protecció de dades i que ha adoptat les mesures més adequades per garantir els drets i les llibertats de les persones de qui tracta les dades.

Aquest nou principi requereix que l'escola analitzi quines dades tracta, amb quines finalitats ho fa i quin tipus d'operacions de tractament du a terme. A partir d'aquest coneixement detallat, ha de valorar el risc que pot generar aquest tractament i, d'acord amb aquesta valoració, adoptar les mesures pertinents. Un dels supòsits que cal analitzar prèviament pels riscos que pot comportar és el tractament de dades de col·lectius vulnerables, en el cas de les escoles, les persones menors d'edat, menors amb necessitats educatives especials o amb discapacitat, entre d'altres.

S'ha de poder demostrar el compliment davant les persones interessades i davant l'Autoritat de protecció de dades.

Cal que l'escola tingui una actitud conscient, diligent i proactiva davant de tots els tractaments de dades personals que dugui a terme.

2.2 L'enfocament al risc

Un altra novetat de la nova regulació és que l'RGPD adopta un enfocament en el risc, i que les mesures concretes a aplicar han de tenir en compte la naturalesa, l'àmbit, el context i les finalitats del tractament, així com el risc per als drets i les llibertats de les persones. És a dir, cada responsable del tractament, atenent les seves característiques, adoptarà les mesures que correspongui en funció dels riscos existents.

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

La major part de les dades tractades a les escoles són dades de menors d'edat. Això fa que, atesa la vulnerabilitat d'aquest col·lectiu i les conseqüències que es poden derivar d'un tractament inadequat de la seva informació, tant en el present com en el futur, les escoles hagin d'extremar, encara més que altres sectors, la diligència en el tractament d'aquesta informació.

Aquests dos elements (l'*accountability* i l'enfocament en el risc) es projecten sobre totes les obligacions de les organitzacions

2.3 Protecció de dades des del disseny i per defecte

El Reglament introdueix els conceptes de privacitat des del disseny i privacitat per defecte. Això implica que el responsable ha d'aplicar, tant en el moment de determinar els mitjans de tractament com en el moment del tractament mateix, les mesures tècniques i organitzatives adequades concebudes per aplicar de manera efectiva els principis de protecció de dades (com per exemple la seudonimització), i integrar les garanties necessàries en el tractament per complir els requeriments del Reglament.

Així mateix, el responsable ha d'aplicar les mesures tècniques i organitzatives adequades per garantir que, per defecte, només es tracten les dades personals necessàries per a cada finalitat específica del tractament.

Exemple

Quan es dissenya una aplicació per a ús escolar, el primer que cal fer és valorar com afecta a la privacitat de l'alumnat i dissenyar-la amb el màxim nivell de protecció. És a dir, ja des del disseny i per defecte cal que es garanteixi un nivell alt de protecció de la privacitat per a l'alumnat.

3. Tractament de dades a les escoles

3.1 Dades personals

Dades personals qualsevol informació sobre una persona física identificada o identificable (la persona interessada). S'ha de considerar persona física identificable qualsevol persona la identitat de la qual es pot determinar, 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.

Per complir amb les obligacions establertes per la normativa de protecció de dades, cal identificar les dades que es tractaran i que són susceptibles de protecció i també conèixer els conceptes bàsics, els principis fonamentals i les obligacions establertes per garantir la protecció de la informació de les persones interessades o afectades.

En el cas de les dades de l'alumnat, el tractament de dades a les escoles es produeix per primera vegada amb la petició de la plaça escolar per part dels progenitors o persones tutores en el procés de preinscripció, i es manté com a mínim fins que l'alumne finalitza els estudis en aquell centre. Això comporta el tractament de molta informació, ja sigui facilitada per la família, per les persones professionals que treballen al centre (professorat, persones tutores, professionals de la psicologia, etc.) o pel mateix alumnat.

Les escoles, per exercir les seves funcions, tracten dades de diferents col·lectius i de diferents tipologies. Amb caràcter previ, convé analitzar si la finalitat perseguida es pot assolir sense necessitat de recollir dades que facin identificables persones físiques, ja sigui de forma directa o indirecta.

Per poder realitzar el « mapa » dels tractaments de dades, ens cal establir:

3.1.1 Origen de les dades

- Les dades que rep l'escola, per exemple, quan el Departament envia a l'escola la llista d'admissions.
- Les dades que genera l'escola mateixa, com ara les notes, informes psicopedagògics de l'alumnat, etc.
- Les dades que l'escola envia, per exemple, a proveïdors de serveis de l'escola.
- Les dades que s'envien al nou centre quan l'alumne canvia d'escola, etc.

3.1.2 Operacions o gestions en què es tracten dades

- Matriculació i admissió d'alumnes: publicitat i contacte amb persones interessades a incorporar-se al centre, procés de preinscripció, matriculació.
- Gestió acadèmica.
- Necessitats educatives especials.
- Serveis oferts pel centre educatiu a l'alumnat i que en completen la finalitat educativa: menjador, transport escolar, activitats extraescolars, excursions i colònies, uniformes, etc.
- Gestió del personal docent, administratiu i de serveis.
- Gestió de proveïdors.
- Sistemes de pagament.
- Plataformes virtuals d'ensenyament.
- Sistemes de comunicació/contacte.
- Informació mèdica.
- Serveis a exalumnes.
- Altres.

3.1.3 De qui es tracten les dades?

Persona interessada: qualsevol informació sobre una persona física identificada o identificable.

- Alumnes
- Pares i mares d'alumnes
- Professorat
- Persones tutores
- Proveïdors
- Assistents a activitats
- Monitors i monitores
- Exalumnes
- Altres persones amb les quals es relaciona l'escola

Les dades de caràcter personal que les escoles tracten per dur a terme les seves funcions no pertanyen al centre, sinó a l'alumnat, als seus familiars, al seu personal o a altres persones físiques amb qui es relacionen. Ells i elles en són els autèntics titulars.

3.1.4 Quines dades es tracten?

Totes aquelles dades que permetin identificar una persona.

Algunes dades són útils exclusivament per a identificar les persones; d'altres permeten conèixer aspectes de la seva personalitat, avaluar la persona o conèixer aspectes de la seva història i circumstàncies (estudis, família, vida laboral, salut, etc.).

- Dades identificatives, com el nom, l'adreça, una fotografia o el DNI.
- Dades de característiques personals, com ara lloc de naixement, nacionalitat o sexe.
- Dades de circumstàncies socials, com aficions, estils de vida, situació familiar.
- Dades acadèmiques i professionals, com l'historial acadèmic, l'experiència professional.
- Dades economicofinanceres, dades bancàries, assegurances, subsidis, targetes de crèdit.
- Dades d'ocupació laboral, com el cos, la categoria, el lloc de treball, historial laboral.
- Dades relatives a la comissió d'infraccions penals, com delictes.
- Categories especials de dades: dades de salut, ideologia, afiliació sindical, religió, creences, vida sexual, origen racial.

3.1.5 Categories especials de dades

L'RGPD estableix com a categories especials de dades aquelles que revelin:

- Origen ètnic o racial
- Opinió política
- Conviccions religioses o filosòfiques
- Afiliació sindical
- Dades de salut
- Vida sexual o orientació sexual de la persona
- Dades genètiques
- Dades biomètriques dirigides a identificar la persona

L'RGPD ha inclòs aquestes dues últimes dades en les categories especials de dades:

Dades genètiques: dades personals relatives a les característiques genètiques heretades o adquirides d'una persona física, que proporcionen una informació única sobre la fisiologia o la salut d'aquesta persona, obtingudes en particular de l'anàlisi d'una mostra biològica.

Dades biomètriques: dades personals obtingudes a partir d'un tractament tècnic específic, relatives a les característiques físiques, fisiològiques o conductuals d'una persona física, que permeten o confirmen la identificació única d'aquesta persona (imatges facials, dades dactiloscòpiques, etc.).

Exemples de categories especials de dades

A les escoles es tracten habitualment dades relatives a necessitats educatives especials i dades de salut de l'alumnat, com ara:

- Discapacitat físiques, com ara minusvalideses.
- Al·lèrgies i intoleràncies, per organitzar el servei de menjador.
- Psicopedagògiques, per realitzar informes de l'alumnat.
- Lesions o malalties que poden tenir lloc a l'escola.
- Discapacitats psíquiques, altes capacitat, TDAH, autismes, etc.

El tractament d'aquest tipus d'informació requereix un rigor especial en el compliment dels principis de la protecció de dades i està sotmès a unes condicions especials, tant pel que fa a la forma com s'ha d'obtenir el consentiment, com a les mesures de seguretat aplicables.

Per això, cal establir els protocols necessaris per al tractament adequat d'aquesta informació, tant durant el funcionament normal del centre (estada a les aules, horari d'esbarjo, educació física, menjador, infermeria, avaluació psicopedagògica etc.) com en situacions extraordinàries (substitucions de mestres o persones tutores, celebracions d'aniversaris, sortides, colònies, etc.).

Cal recordar que l'RGPD prohibeix el tractament d'aquest tipus de dades tret que es donin determinades excepcions que es relacionen en l'apartat IV d'aquest document titulat «Legitimitat».

3.2 Qui tracta les dades personals?

3.2.1 El responsable del tractament

El responsable del tractament: la persona física o jurídica, autoritat pública, servei o altre organisme que sol o amb altres, determini els fins i mitjans del tractament (...).

En el cas dels centres educatius públics ens trobem davant de centres que depenen d'un Departament de l'Administració de la Generalitat, però que alhora tenen atribuïda una certa autonomia en la gestió. Per això, el Departament d'Ensenyament serà el que establirà qui és el responsable del tractament.

En el cas de les escoles concertades, el responsable del tractament serà la mateixa escola.

3.2.2 Encarregat del tractament

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

Les escoles, com a responsables dels tractaments, poden encarregar a terceres persones o entitats un tractament de dades personals o una activitat que comporti el tractament de dades de caràcter personal, com ara, per organitzar:

- Les activitats extraescolars
- El servei d'autocar
- El servei de menjador
- Altres serveis externalitzats (natació, activitats extraescolars, assessoria comptable i laboral, destrucció de paper, etc.

En aquest cas, cal tenir present la figura de l'encarregat del tractament.

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

El contracte ha d'establir com a mínim l'objecte, la durada, la naturalesa i la finalitat del tractament, el tipus de dades personals i les categories de persones interessades, així com les obligacions i els drets del responsable. El contracte també ha de preveure si, un cop finalitzada la prestació dels serveis, les dades es tornaran al responsable o es destruiran.

El responsable del tractament ha de triar un encarregat del tractament 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. Per tant, hi ha un deure de diligència a l'hora d'escollir l'encarregat.

Links

Trobareu la informació necessària i models orientatius per realitzar el contracte/acord d'encàrrec de tractament: [Encarregat del tractament](#)



Què passa amb els contractes d'encàrrec formalitzats abans de l'aplicació de l'RGPD?

Els contractes d'encàrrec formalitzats abans de l'aplicació de l'RGPD, el maig de 2018, s'han d'adaptar per respectar-ne el contingut. Tot i que moltes de les obligacions derivades del règim establert a l'RGPD ja estan recollides a la normativa espanyola, cal modificar els contractes existents perquè les clàusules reflecteixin tots els continguts del Reglament, tenint en compte que les remissions genèriques a l'article de l'RGPD que els regula no són vàlides.

D'acord amb la Disposició transitòria segona del Reial Decret Llei 5/2018, de 27 de juliol, de mesures urgents per a l'adaptació del dret espanyol a la normativa de la Unió Europea en matèria de protecció de dades, els contractes i acords d'encàrrec del tractament establerts abans de 25 de maig de 2018 mantenen la seva vigència fins la data de venciment que s'hi assenyala.

Quan es tracti d'encàrrecs amb durada indefinida, mantenen la vigència fins al cap de quatre anys, a comptar des del 25 de maig de 2018 (fins al 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 a allò que estableix l'article 28 de l'RGPD.

3.3 Registre de les activitats de tractament de dades (RAT)

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.

Cal recordar que l'RGPD suprimeix, des del 25 de maig de 2018, la necessitat de crear formalment fitxers i notificar-los al registre de protecció de dades de les autoritats de control.

3.3.1 Registre de les activitats de tractament de dades (RAT)

Els responsables i encarregades del tractament han d'elaborar un registre de les activitats del tractament que duguin a terme.

L'RGPD preveu determinades excepcions a l'elaboració d'aquest registre entre les quals no hi cabrien els tractaments de dades efectuats per les escoles.

Aquest és un instrument fonamental no només per la possible supervisió de l'Autoritat, sinó també per tenir una imatge actualitzada dels tractaments existents a l'escola, essencial per a la gestió de riscos. El registre ha de ser per escrit, inclòs en format electrònic, i s'ha de presentar a petició de l'Autoritat.

3.3.2 Com s'ha d'organitzar el registre d'operacions de tractament?

El registre es pot organitzar al voltant d'operacions de tractament concretes, vinculades a una finalitat bàsica comuna de totes elles (per exemple «gestió acadèmica» o «gestió de recursos humans i nòmines»), o bé d'acord amb altres criteris.

Links

L'APDCAT ha desenvolupat una aplicació senzilla per portar el registre d'activitats de tractament per tal d'ajudar als responsables a organitzar-se. Us la podeu descarregar en aquest enllaç: [Aplicació registre activitats de tractament](#)

4. Legitimitat. Quan podem tractar dades personals?

4.1 Principis. Com complir amb l' RGPD

Els tractaments de dades s'han de dur a terme sempre respectant els principis establerts per l'RGPD. En començar, ja s'ha exposat un dels principis que suposa una important novetat en aquesta regulació, el principi de responsabilitat proactiva.

4.1.1 Licitud, lleialtat i transparència

Les dades s'han de tractar amb licitud, lleialtat i transparència.

Així, per exemple, l'escola ha de facilitar a les persones interessades, la informació sobre el tractament amb suficient antelació d'acord amb els terminis màxims establerts, i quan s'introdueixin canvis en el tractament de les dades, els ha de comunicar a les persones interessades i explicar-los com els afectaran.

4.1.2 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. El tractament posterior de les dades personals amb finalitats d'arxiu en interès públic, amb finalitats de recerca científica i històrica o amb finalitats estadístiques no es considera incompatible amb les finalitats inicials.

En aquest sentit, la mateixa llei orgànica 2/2006, de 3 de maig, d'educació (LOE) estableix que la informació que recullen les escoles en exercici de la seva funció educativa ha de ser

l'estrictament necessària per a la funció docent i orientadora, i no es pot tractar amb finalitats diferents de l'educativa sense consentiment exprés.

4.1.3 Minimització de les dades

Les dades han de ser adequades, pertinents i s'han de limitar al que sigui necessari en relació amb els fins per als quals es tracten.

Cal revisar amb cura les dades que es pretenen recollir perquè només es recullin aquelles que, d'acord amb aquest principi, siguin necessàries per a assolir la finalitat perseguida.

4.1.4 Exactitud

Les dades han de ser exactes i, si fos necessari, han d'estar actualitzades; s'han d'adoptar totes les mesures raonables perquè se suprimeixin o rectifiquin sense dilació aquelles dades personals que siguin inexactes respecte als fins per als quals es tracten.

La manca d'actualització de les dades personals pot afectar la mateixa gestió acadèmica o, fins i tot pot comportar la revelació indeguda de dades a terceres persones (per exemple, si l'adreça no està actualitzada o si l'escola no ha registrat degudament la comunicació dels pares i mares sobre canvis que afecten el règim legal de pàtria potestat o guarda i custòdia sobre els infants i joves).

4.1.5 Limitació del termini de conservació

Les dades s'han de conservar de manera que es permeti la identificació de les persones interessades durant el temps estrictament necessari per als fins del tractament de dades personals. Les dades es poden conservar durant períodes més llargs sempre que es tractin exclusivament amb fins d'arxiu en interès públic, ja sigui per a la recerca científica o històrica o per finalitats estadístiques, sens perjudici de l'aplicació de les mesures tècniques i organitzatives adequades que imposa la normativa de protecció de dades amb la finalitat de protegir els drets i les llibertats de la persona interessada.

4.1.6 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, tal com s'assenyala a l'apartat "IX".

4.2 Transparència de la informació

L'escola ha de ser transparent respecte dels tractaments de dades que es volen dur a terme amb independència que sigui necessari obtenir el consentiment de la persona interessada o es compti amb una altra base jurídica.

Per això, en tots aquells tractaments que l'escola realitzi, caldrà aplicar la màxima transparència, de manera que les persones coneguin en tot moment l'ús que s'està fent de les seves dades. Així per exemple, disposar d'un avís de privacitat a les pàgines web de les entitats clarament visible permetrà a les persones estar informades en tot moment.

4.2.1 Informació a la persona interessada

La transparència en el tractament de les dades es concreta de forma molt clara en el dret d'informació que té la persona interessada tant si les dades es recullen directament com a través de tercers.

Quan les dades es recullen directament de la persona interessada

La informació a la persona interessada es pot facilitar adoptant un model d'informació per capes o nivells: tot donant en un primer nivell la informació bàsica facilitant una adreça electrònica o un altre mitjà que li permeti accedir de forma senzilla i immediata a la resta de la informació.

Es concreta de la manera següent:

Primer nivell. Informació bàsica que permeti tenir un coneixement general del tractament.

- La identitat del responsable del tractament.
- La finalitat del tractament.
- La possibilitat d'exercir els drets d'autodeterminació informativa, el dret d'accés, rectificació, supressió, i oposició, així com el dret a la limitació del tractament, a la portabilitat de les dades o a impugnar valoracions.

Segon nivell. Resta de la informació.

- 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 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.

- La intenció de transferir les dades a un tercer país o a una organització internacional i la base per fer-ho, 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 i l'oposició al tractament i la portabilitat de les dades.
- El dret a retirar en qualsevol moment el consentiment que s'ha prestat.
- Si la comunicació de dades és un requisit legal o contractual o un requisit necessari per subscriure un contracte, i si la persona interessada està obligada a facilitar les dades i les conseqüències de no facilitar-les.
- 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.

Quan les dades no es recullen directament de la persona interessada

A més dels aspectes que s'acaben de relacionar, cal indicar:

- Les categories de dades personals tractades.
- La font de la qual procedeixen les dades i si són fonts d'accés públic.

4.2.2 Excepcions al dret d'informació

No cal informar quan:

- Les dades es recullen de la persona interessada i aquesta ja disposa de la informació.
- Les dades no es recullen de la persona interessada i hi concorre alguna de les circumstàncies següents:
 - La persona interessada ja disposa de tota la informació legalment exigible.
 - La comunicació resulta impossible o suposa un esforç desproporcionat.
 - L'obtenció o la comunicació està expressament establerta pel Dret de la Unió Europea o dels Estats Membres.
 - Les dades han de continuar tenint caràcter confidencial per una obligació legal de secret professional, inclosa una obligació de secret de naturalesa estatutària.

4.2.3 On i com cal informar?

L'obligació d'informar s'ha de complir sense necessitat de cap requeriment i el responsable ha de poder acreditar amb posterioritat que l'ha complert.

En qualsevol cas, la informació a les persones interessades s'ha de proporcionar:

- En un llenguatge clar i senzill.
- De forma concisa, transparent, intel·ligible i de fàcil accés.
- Equilibrant la concisió i precisió, tot evitant circumloquis, explicacions innecessàries o detalls confusos.
- Tot evitant l'abús de cites legals innecessàries i de termes ambigus o amb escàs sentit per a les persones destinatàries.
- Mitjançant un llenguatge adequat al seu nivell de comprensió, en cas que els destinataris siguin menors.

Si ho sol·licita la persona interessada, la informació també es pot facilitar verbalment.

4.2.4 En quin moment del tractament s'ha de donar la informació?

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

- Si la informació s'obté de la mateixa persona interessada, en el moment en què se sol·liciten les dades.
- Si la informació no s'obté de la mateixa persona interessada, en un termini raonable, però en qualsevol cas en el termini d'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 interessada, cal informar-ne abans o en la primera comunicació amb ella.
 - Si és previst comunicar-les a un altre destinatari, cal informar-ne abans o en el moment d'aquesta comunicació.
 - Si posteriorment es pretén utilitzar les dades per a una finalitat diferent d'aquella per a la qual es van recollir, cal proporcionar prèviament la informació necessària vinculada a aquesta nova finalitat.

Links

Al web de l'Autoritat, trobareu la Guia per al compliment del deure d'informar que ofereix directrius i orientacions per complir amb aquesta obligació: [Guia per al compliment del deure d'informar](#)



Cal tornar a informar les persones afectades que ja ho dels nous aspectes que exigeixen els articles 13 i 14 de l'RGPD??

L'RGPD amplia les qüestions sobre les quals cal informar les persones afectades i modifica alguns aspectes de la manera com s'ha de proporcionar aquesta informació. No obstant això, pel que fa a les dades recollides abans del 25 de maig de 2018, no és preceptiu informar novament amb els requisits establerts a l'RGPD. L'obligació d'informar segons el que estableix l'RGPD és exigible només per a les dades recollides després d'aquesta data. Tanmateix, si les circumstàncies ho permeten, una bona pràctica recomanable és aprofitar els actes de comunicació amb les persones afectades per informar-les dels nous aspectes que estableix l'RGPD.

4.3 Bases jurídiques per tractar dades personals

Les escoles, per a exercir les seves funcions, han de tractar un gran volum de dades personals. El tractament només és lícit si es compleix, almenys, una de les condicions que es detallen a continuació:

- Quan la persona interessada ha donat el seu consentiment.
- Quan és necessari per executar un contracte o aplicar mesures precontractuals.
- Per complir una obligació legal.
- Per protegir interessos vitals de la persona interessada o d'una altra persona física.
- Per complir una missió realitzada en interès públic o en l'exercici de poders públics conferits al responsable del tractament.
- Per satisfer interessos legítims perseguits per al responsable del tractament o per un tercer, sempre que no hi prevalguin els interessos o els drets i les llibertats fonamentals de la persona interessada que requereixen la protecció de dades personals, especialment si la persona interessada és un infant. (Aquest paràgraf no s'aplica al tractament efectuat per les autoritats públiques en l'exercici de les seves funcions).

Per al cas de les categories especials de dades, no n'està permès el tractament excepte si concorre alguna de les circumstàncies establertes a l'RGPD com per exemple:

- La persona interessada ha donat el seu consentiment explícit per al tractament d'aquestes dades personals per a una o més de les finalitats especificades.
- El tractament és necessari per a protegir interessos vitals de la persona interessada o d'una altra persona física, en el supòsit que la persona interessada no estigui capacitada físicament o jurídicament per donar el consentiment.
- O també altres circumstàncies, com ara quan el tractament es refereix a dades personals que la persona interessada ha fet manifestament públiques, quan és necessari per a finalitats de medicina preventiva o laboral, etc.

Qualsevol tractament de dades, per tant, també la comunicació de dades a tercers han d'estar sustentades en alguna de les bases jurídiques anteriors.

Alguns exemples de comunicacions poden ser:

- Comunicacions de dades per a finalitats acadèmiques.
- Comunicacions extraacadèmiques.
- Comunicacions amb finalitats administratives.
- Comunicacions a administracions públiques.

4.3.1 LOE: habilitació per al tractament de dades a les escoles

Les escoles, siguin de titularitat pública o privada, poden tractar les dades personals del seu alumnat que siguin necessàries per a l'exercici de la seva funció educativa i orientadora. Així ho estableix la LOE que habilita el tractament de les dades de l'alumnat amb aquesta finalitat des del moment que l'alumne s'incorpora a l'escola. La LOE també habilita l'escola, si escau, perquè cedeixi dades de l'alumnat, com ara del centre on hagi estat escolaritzat anteriorment cap al nou centre on l'alumne segueixi els seus estudis.

Així mateix, la LOE habilita les escoles per al tractament de dades de categories especials, el coneixement de les quals sigui necessari per a l'educació i orientació de l'alumnat.

Per totes aquelles altres funcions que no formin part de la funció docent i orientadora dels centres, caldrà buscar la base jurídica per a tractar-les (consentiment, contracte, interès públic, etc.)

4.3.2 Relació Contractual. Habilitació Professorat i personal dels centres

Pel que fa a les dades relatives al seu personal, les escoles poden tractar les seves dades sense necessitat del seu consentiment, quan es tracta de dades necessàries per mantenir o complir la relació laboral o administrativa que mantinguin amb el centre.

4.3.3 Consentiment: Serveis diferents de la funció docent i orientadora

Per a altres casos en què es necessiti tractar les dades amb finalitats diferents a la funció docent i orientadora, com ara la publicació de fotografies al web de l'escola, o el lliurament de dades a cases de colònies, museus o altres establiments que es visitin, es necessita el consentiment del titular de les dades, o del seu representant en el cas de menors.

El consentiment ha de ser una manifestació de voluntat per la qual la persona interessada accepta el tractament de les seves dades personals, ja sigui mitjançant una declaració o una clara acció afirmativa. Aquesta manifestació de voluntat ha de ser:

- **Lliure**, la persona ha de tenir la possibilitat de rebutjar lliurement que es tractin les seves dades.
- **Específica**, el consentiment es refereix a tractaments concrets i per a una finalitat determinada, explícita i legítima del responsable del tractament, sense que es puguin fer habilitacions genèriques.
- **Informada**, cal informar les persones interessades perquè amb antelació al tractament, en puguin conèixer l'existència i les finalitats.
- **Inequívoca**, la sol·licitud i l'atorgament del consentiment s'han de produir de forma clara

L'RGPD requereix que la persona interessada presti el consentiment mitjançant una declaració inequívoca o una acció afirmativa clara per a cada una de les finalitats per a les quals es demana el consentiment. Així, als efectes de l'RGPD, les caselles ja marcades, el consentiment tàcit o la inacció no constitueixen un consentiment vàlid.

Correspon al responsable del tractament la prova de l'obtenció del consentiment de la persona interessada per a un tractament específic.



Es poden continuar fent els tractaments basats en el consentiment tàcit iniciats abans de 25 de maig de 2018?

L'RGPD estableix que el consentiment ha de consistir en una declaració o un acte afirmatiu clar, que reflecteixi una manifestació de voluntat lliure, específica, informada i inequívoca de la persona interessada d'acceptar el tractament de dades de caràcter personal que l'afecten. Per tant, el silenci, les caselles ja marcades o la inacció (com, per exemple; el consentiment tàcit) no constitueixen un consentiment vàlid d'acord amb l'RGPD.

D'acord amb això, cal que els tractaments de dades iniciats abans del 25 de maig de 2018 basats en un consentiment tàcit, s'ajustin als requisits de l'RGPD abans d'aquesta data, ja sigui mitjançant l'obtenció d'un nou consentiment que reuneixi els requisits establerts per l'RGPD, ja sigui mitjançant alguna altra de les bases jurídiques establertes per l'RGPD.

4.3.4 Consentiment: Menores d'edat

Les escoles normalment tractaran dades de menors d'edat. Per aquells tractaments que requereixin el consentiment, és a dir, aquells no inclosos en la funció docent i orientadora dels centres, caldrà el consentiment dels pares, mares o persones tutores quan l'alumne sigui menor de 14 anys.

L'alumnat major de 14 anys podran consentir per sí mateixos, amb l'excepció d'aquells supòsits en què la llei exigeixi l'assistència dels titulars de la pàtria potestat o tutela.

La protecció de menors es concreta també en l'exigència que la informació que se'ls proporciona sigui en un llenguatge que els resulti fàcilment comprensible.

4.3.5 Consentiment: Xarxes i menors

L'escola ha de ser conscient de la seva responsabilitat en un ús o difusió inapropiat de les imatges de menors. La normativa de protecció de dades regula especialment la protecció de menors a Internet, i estableix que la utilització i difusió d'imatges i informació personals de menors a les xarxes socials que puguin implicar una intromissió il·legítima en els seus drets fonamentals determinarà la intervenció del ministeri fiscal que podrà instar les mesures cautelars i de protecció que determini la llei.

Les escoles, i qualsevol persona que realitzi activitats on hi participin menors d'edat i on es tractin les seves dades (imatges, veu, ...) han de garantir la protecció de l'interès superior de l'infant i dels seus drets i llibertats fonamentals. En aquest cas, especialment el dret a la protecció de dades personals, en el moment de la publicació o difusió de les seves dades personals a través dels serveis de la societat de la informació.

Caldrà que l'escola compti amb el consentiment dels infants o dels seus pares, mares o persones tutores abans de dur a terme qualsevol publicació o difusió de les dades de l'alumnat al web de l'escola o a la intranet de l'escola.

4.3.6 Revocació del consentiment

La persona afectada pot revocar el consentiment atorgat en qualsevol moment, sense efectes retroactius. Abans de donar el seu consentiment s'haurà d'informar a la persona interessada d'aquesta possibilitat. Ha de ser tan fàcil retirar el consentiment com donar-lo.

5. Drets de la persona interessada

5.1 Dret de l'autodeterminació informativa

Aquest drets són personalíssims i els ha d'exercir la mateixa persona interessada o un tercer per representació, davant el responsable del tractament.

Les persones titulars de la pàtria potestat podran exercir sempre aquests drets, en nom i representació dels infants menors de 14 anys.

5.1.1 Dret d'accés

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

- Les finalitats del tractament, les categories de dades personals que es tracten i 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 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 interessada.
- 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.

La persona interessada té dret a obtenir una còpia gratuïta de les dades objecte del tractament. Per a còpies posteriors, es pot establir un cànon segons els costos administratius. Si se sol·licita per mitjans electrònics, la persona interessada té dret a rebre la informació en aquest mateix format.

Si les sol·licituds són manifestament infundades o excessives, especialment a causa del seu caràcter repetitiu, el responsable del tractament pot cobrar un cànon raonable, d'acord amb els costos administratius que s'han afrontat per facilitar la informació o la comunicació, o per dur a terme l'actuació sol·licitada, o bé, negar-se a actuar respecte de la sol·licitud. El responsable del tractament és qui haurà de demostrar el caràcter manifestament infundat o excessiu de la sol·licitud.

5.1.2 Dret de rectificació

La persona interessada té dret a rectificar les seves dades personals inexactes i que es completin les seves dades personals incompletes, fins i tot mitjançant una declaració addicional.

Cal que la persona interessada indiqui de forma clara i detallada el que es demana, a quines dades es refereix i quina correcció s'ha de fer. La sol·licitud ha d'anar acompanyada de la documentació que justifica la rectificació, si escau.

El responsable ha de comunicar la rectificació a cadascun dels destinataris, tret que sigui impossible o exigeixi esforços desproporcionats. Si la persona interessada ho sol·licita, el responsable ha d'identificar les persones destinatàries.

5.1.3 Dret de supressió o dret a l'oblit

Les persones interessades tenen dret a obtenir la supressió de les dades («dret a l'oblit»), quan:

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

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

El responsable ha de comunicar la supressió a cadascuna de les persones destinatàries, tret que sigui impossible o exigeixi esforços desproporcionats. Si la persona interessada ho sol·licita, el responsable ha d'identificar els destinataris.

Es preveuen algunes excepcions a l'exercici d'aquest dret:

- L'exercici del dret a la llibertat d'expressió i informació.
- El compliment d'una obligació legal.
- 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.

5.1.4 Dret a la limitació del tractament

La limitació de tractament suposa que, a petició de la persona interessada, no s'aplicaran a les seves dades personals les operacions de tractament que en cada cas correspondrien.

La limitació es pot sol·licitar quan:

- La persona interessada ha exercit els drets de rectificació o oposició i mentre el responsable determina, si escau, atendre la sol·licitud.

- El tractament és il·lícit, cosa que determinaria l'esborrat de les dades, però la persona interessada s'hi oposa.
- Les dades ja no són necessàries per al tractament, la qual cosa novament en determinaria l'esborrat, però la persona interessada sol·licita la limitació perquè les necessita per formular, exercir o defensar reclamacions.

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

- Amb el consentiment la persona interessada.
- Per formular, exercir o defensar reclamacions.
- Per protegir els drets d'una altra persona física o jurídica.
- Per raons d'interès públic important de la Unió Europea o d'un Estat Membre.

El responsable ha de comunicar la limitació a cadascun dels destinataris, tret que sigui impossible o exigeixi esforços desproporcionats. Si la persona interessada ho sol·licita, el responsable ha d'identificar els destinataris.

5.1.5 Dret a la portabilitat de les dades

El dret a la portabilitat de les dades és una forma avançada del dret d'accés, pel qual la persona interessada té dret a rebre les dades personals que l'afecten en un format estructurat, d'ús comú i de lectura mecànica, si es compleixen els requisits següents:

- El tractament està basat en el consentiment o en un contracte.
- El tractament es fa per mitjans automatitzats.

La persona interessada pot sol·licitar al responsable les dades que ha proporcionat i que l'afecten, incloses les dades derivades de l'activitat de la persona interessada.

El dret a la portabilitat de dades inclou el dret que aquestes es transmetin directament de responsable a responsable, si és tècnicament possible.

No es pot exercir aquest dret quan el tractament es fonamenta en el compliment d'una missió d'interès públic o inherent a l'exercici del poder públic.

5.1.6 Dret d'oposició

La persona interessada té dret a oposar-se al tractament de les seves dades personals:

- Quan el tractament es basa en l'interès públic o l'exercici de poders públics conferits al responsable, o en l'interès legítim perseguit per al 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 un interès legítim imperiós que prevalgui sobre el de la persona interessada o sigui necessari per exercir o defensar reclamacions.

- 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.
- Quan el tractament té per objecte el màrqueting directe, inclosa l'elaboració de perfils relacionats amb aquest màrqueting. Ho podrà fer en qualsevol moment, sense necessitat de fonamentar la seva petició.

5.1.7 Dret a no ser objecte de decisions individuals automatitzades

La persona interessada 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 produeix efectes jurídics sobre ell o que l'afecti significativament, tret que la decisió:

- S' sigui necessària per formalitzar o executar un contracte entre la persona interessada i un responsable del tractament.
- Es basi en el consentiment explícit de la persona interessada.
- Estigui autoritzada pel dret de la Unió Europea o d'un Estat Membre.

Convé recordar que, en cas que es prenguin aquest tipus de decisions, caldrà informar-ne la persona interessada.

5.2 Exercici dels drets

5.2.1 Qui pot exercir aquests drets?

La persona afectada o una persona representant en nom seu, si es tracta de menors de 14 anys, persones discapacitades, persones més grans de 14 anys si la llei ho exigeix, o quan la persona afectada designi voluntàriament algú que la representi.

5.2.2 Procediment. Com es fan efectius els drets?

- El responsable del tractament ha de respondre a la interessada d'una manera concisa, transparent, intel·ligible i de fàcil accés, amb un llenguatge clar i senzill, especialment si la informació s'adreça específicament a un infant.
- Ha de facilitar la resposta per escrit o per altres mitjans, inclosos, si escau, per mitjans electrònics. Si la persona interessada ho sol·licita, se li pot donar resposta verbalment si demostra la seva identitat per altres mitjans.

- El responsable del tractament ha de facilitar a la persona interessada l'exercici dels seus drets, i no s'ha de negar a actuar a petició d'ella excepte que pugui demostrar que no està en condicions d'identificar la persona interessada.
- El responsable del tractament ha de facilitar a la persona interessada informació relativa a les seves actuacions, si la sol·licitud s'ha fet d'acord amb l'RGPD i, en qualsevol cas, en el termini d'un mes a partir de la recepció de la sol·licitud. aquest termini es pot prorrogar dos mesos més, en cas necessari, tenint en compte la complexitat i el nombre de sol·licituds.
El responsable ha d'informar la persona interessada de qualsevol d'aquestes prorroques en el termini d'un mes a partir de la recepció de la sol·licitud, indicant els motius de la dilació. Quan la persona interessada presenti la sol·licitud per mitjans electrònics la informació s'ha de facilitar, sempre que sigui possible, per aquests mateixos mitjans, tret que la persona interessada sol·liciti que es faci d'una altra manera.
- La informació facilitada ha de ser gratuïta. Si les sol·licituds són manifestament infundades o excessives, especialment a causa del seu caràcter repetitiu, el responsable del tractament pot:
 - Cobrar un cànon raonable, d'acord amb els costos administratius que s'han afrontat per facilitar la informació o la comunicació, o per dur a terme l'actuació sol·licitada.
 - Negar-se a actuar respecte de la sol·licitud.
- El responsable del tractament ha de suportar la càrrega de demostrar el caràcter manifestament infundat o excessiu de la sol·licitud.
- Quan el responsable del tractament tingui dubtes raonables sobre la identitat de la persona física que presenta la sol·licitud, podrà sol·licitar la informació addicional necessària per confirmar la identitat de la persona interessada.

5.2.3 On s'ha de presentar la sol·licitud?

La persona interessada ha de presentar la sol·licitud davant el responsable del tractament, ja sigui l'escola que tracta les seves dades o el Departament.

Els drets també es poden exercir davant de l'encarregat del tractament. En aquest cas, l'encarregat (per exemple l'empresa que presta el servei de menjador) ha de traslladar la sol·licitud al responsable perquè la resolgui, llevat dels casos en què el contracte d'encàrrec del tractament l'habiliti per resoldre les sol·licituds per compte del responsable.

Si el responsable o en el seu cas l'encarregat del tractament no tramiten la sol·licitud de la persona interessada, sense dilació i com a màxim al cap d'un mes, s'ha d'informar a la persona interessada que s'ha rebut la seva sol·licitud, dels motius pels quals no s'ha atès, i de la possibilitat de presentar una reclamació davant l'Autoritat Catalana de Protecció de Dades i d'exercir accions judicials.

5.2.4 Reclamació davant la manca d'atenció dels drets

Les persones interessades a les quals es denegui en part o totalment l'exercici dels drets d'autodeterminació informativa, o que entenguin que la seva sol·licitud s'ha desestimat perquè no s'ha atès dins del termini establert, poden presentar una reclamació davant l'Autoritat Catalana de Protecció de Dades. L'Autoritat, a través de la tramitació d'un procediment de tutela de drets, resoldrà si la denegació és procedent o improcedent.

6. El deure de secret

El responsable del tractament i totes les persones que poden intervenir en qualsevol de les fases del tractament de dades de caràcter personal estan obligades a guardar secret respecte d'aquestes dades. En aquest sentit, la LOE estableix que el professorat i la resta del personal que, en l'exercici de les seves funcions, accedeixi a dades personals i familiars o que afectin l'honor i la intimitat dels infants i joves o les seves famílies queda subjecte al deure de sigil.

Els centres escolars, pel desenvolupament de les seves funcions, necessiten la col·laboració no només del professorat, sinó també de diferents professionals dels àmbits següents: psicologia, pedagogia, logopèdia, educació especial o educació social. Els centres també compten amb personal administratiu i altres serveis auxiliars com ara el de manteniment o el menjador. Tots ells accedeixen o poden accedir en algun moment als sistemes d'informació o documentació que contenen dades de caràcter personal de l'alumnat.

Per garantir el compliment d'aquest deure, en una relació jurídica que comporti el tractament de dades de caràcter personal, cal incorporar-lo i definir-lo en els contractes laborals, en els protocols interns, en les activitats formatives i en les regulacions específiques que recullen els drets i les obligacions de les parts. Aquesta obligació subsisteix fins i tot un cop finalitzi la relació amb el responsable.

El compliment del deure de secret és encara més important en un àmbit com l'educatiu, en què sovint es pot tractar informació que ha de ser especialment protegida, com ara la informació obtinguda per part de professionals de les àrees d'orientació, psicologia, pedagogia, logopèdia, educació especial i educació social, i que pot incloure diagnòstics, valoracions i dictàmens professionals sobre l'estat de salut física o psíquica de l'alumnat o valoracions sobre la seva vida personal i familiar.

7. Delegat de protecció de dades

7.1 La figura del delegat de protecció de dades a les escoles

Les escoles estan obligades a designar un delegat de protecció de dades (DPD). Aquesta obligació s'estendria també a l'escola concertada i a l'escola privada en el marc del projecte de la Llei orgànica de protecció de dades de caràcter personal, publicat al Butlletí oficial de les Corts Generals núm.13- 1, de 24 de novembre de 2017.

El delegat de protecció de dades podrà formar part de la plantilla o bé actuar en el marc d'un contracte. El delegat de protecció de dades d'una escola també ho pot ser d'altres escoles o bé, diferents escoles poden tenir un mateix delegat per a totes elles.

Les escoles hauran de publicar les dades de contacte del delegat de protecció de dades i comunicar a l'Autoritat catalana de protecció de dades les designacions, els nomenaments i els cessaments d'aquesta persona en un termini de 10 dies.

El delegat de protecció de dades té, entre d'altres, les funcions següents:

- Informar i assessorar el centre o l'encarregat i el personal sobre les obligacions que imposa la normativa de protecció de dades.
- Supervisar el compliment de la normativa.
- Assessorar respecte de l'avaluació d'impacte relativa a la protecció de dades.
- Ser l'interlocutor del centre escolar amb l'Autoritat de protecció de dades.

La posició del DPD a les organitzacions ha de complir els requisits que estableix expressament l'RGPD. Entre aquests requisits hi ha la total autonomia en l'exercici de les seves funcions, la necessitat que es relacioni amb el nivell superior de la direcció o l'obligació que el responsable o encarregat li facilitin tots els recursos necessaris per desenvolupar la seva activitat.

7.2 Quins requisits o qualificacions ha de tenir el delegat de protecció de dades?

El DPD s'ha de nomenar tenint en compte les seves qualificacions professionals i, en particular, el seu coneixement de la legislació i la pràctica de la protecció de dades. Això no significa que el DPD hagi de tenir una titulació específica. Tenint en compte que entre les seves funcions s'inclou l'assessorament al responsable o encarregat en tot el que fa referència a la normativa sobre protecció de dades, els coneixements jurídics en la matèria són, sens dubte, necessaris; però també cal que compti amb coneixements aliens a l'àmbit estrictament jurídic, com per exemple en matèria de tecnologia aplicada al tractament de dades o en relació amb l'àmbit d'activitat de l'organització en la qual exerceix la seva tasca.

8. Avaluació d'impacte relativa a la protecció de dades

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

8.1 Com es determina la necessitat de fer una avaluació d'impacte i quin contingut ha de tenir?

L'RGPD conté una llista indicativa de tres supòsits en els quals es considera que els tractaments comporten un alt risc:

- Elaboració de perfils sobre la base dels quals es prenen decisions que produeixen efectes jurídics sobre les persones interessades o que les afecten significativament de manera similar.
- Tractament a gran escala de categories especials de dades.
- Observació sistemàtica a gran escala d'una zona d'accés públic.

En les directrius sobre l'avaluació d'impacte en la protecció de dades, AIPD (WP248), el Grup de l'Article 29 considera que per valorar si el tractament es fa a gran escala s'ha de tenir en compte el següent:

- El nombre de persones interessades 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.

Links

Per a la delimitació de la noció d'alt risc als efectes de l'obligatorietat de fer una avaluació d'impacte i sobre els criteris per fer-la, es recomana consultar la Guia d'avaluació d'impacte en la protecció de dades (AIPD) de l'Autoritat. [Guia d'avaluació d'impacte en la protecció de dades](#)



Què succeeix amb els tractaments iniciats abans del 25 de maig de 2018 als quals amb la nova normativa els sigui exigible l'avaluació d'impacte sobre la protecció de dades (AIPD)?

Si aquests tractaments es perllonguen més enllà del 25 de maig de 2018 i l'anàlisi de risc que les organitzacions duen a terme sobre els tractaments iniciats amb anterioritat indica que aquests tractaments presenten alt risc per als drets o les

llibertats de les persones interessades, la Guia per a l'avaluació de l'impacte en la protecció de dades també recomana fer una AIPD.

8.2 Consulta prèvia

En els casos en què les AIPD identifiquin un alt risc que a parer del responsable del tractament no es pugui mitigar per mitjans raonables en termes de tecnologia disponible i costos d'aplicació, el responsable ha de consultar l'Autoritat catalana de protecció de dades. La consulta ha d'anar acompanyada de la documentació que preveu l'RGPD, inclosa la mateixa avaluació d'impacte.

Links

Per sol·licitar una consulta prèvia, cal seguir els passos que indiquem a la nostra seu electrònica: [Consulta prèvia](#)

L'Autoritat Catalana de Protecció de Dades ha d'assessorar per escrit el responsable i, si escau, l'encarregat. L'Autoritat pot fer ús de tots els poders que li confereix el Reglament, entre els quals hi ha prohibir l'operació de tractament.

9. Mesures de seguretat

A diferència de la normativa actual, el Reglament no estableix una llista de les mesures de seguretat que són d'aplicació d'acord amb la tipologia de dades objecte de tractament, sinó que estableix que el responsable i encarregat del tractament han d'aplicar mesures tècniques i organitzatives adequades al risc que comporta el tractament. Això implica haver de fer una avaluació dels riscos que comporta cada tractament per tal de determinar les mesures de seguretat que cal implementar.

9.1 Com es du a terme una anàlisi de riscos?

Des del punt de vista de la seguretat de la informació una anàlisi de riscos requereix identificar les amenaces (per exemple, accés no autoritzat a les dades personals), valorar quina és la probabilitat que es produeixi i l'impacte que tindria en les persones afectades.

El tipus d'anàlisi varia segons:

- Els tipus de tractament.
- La naturalesa de les dades que es tracten.
- El nombre de persones interessades afectades.

- La quantitat i varietat de tractaments que fa una mateixa organització.
- Les tecnologies utilitzades.

Com a norma general, en les grans organitzacions aquesta anàlisi de riscos i la determinació de les mesures o controls a implantar es pot dur a terme utilitzant alguna de les metodologies o estàndards d'anàlisi de risc existents: MAGERIT, ISO, etc. En responsables de dimensions menors i amb tractaments de poca complexitat, aquesta anàlisi pot ser el resultat d'una reflexió documentada, sobre les implicacions dels tractaments en els drets i les llibertats de les persones interessades. Aquesta reflexió ha d'analitzar el context en què es du a terme el tractament (mitjans, instal·lacions, usuaris, etc.) i ha de donar resposta a qüestions com les següents:

- Es tracten categories especials de dades?
- Es tracten dades de col·lectius vulnerables (per exemple, menors)?
- Es tracten dades d'una gran quantitat de persones?
- Les dades tractades permeten l'elaboració de perfils?
- La revelació, alteració o pèrdua de les dades pot tenir conseqüències importants per les persones afectades?
- Es tracten les dades fora dels equips o instal·lacions del responsable?
- Tenen accés a les dades terceres persones que presten serveis per compte del responsable?
- S'utilitzen tecnologies especialment invasives per a la privacitat, (geolocalització, videovigilància, internet de les coses etc.) ?

Són moltes les qüestions que poden impactar de forma negativa en els drets i llibertats de les persones si es tracten inadequadament les dades. Per tant, és molt important, que si no s'utilitza una metodologia estàndard, fàcilment auditable i objectivable, es documentin detalladament les qüestions que s'han tingut en compte a l'hora de determinar el nivell de risc existent i concretar les mesures de seguretat que cal aplicar. Això ens servirà per complir amb el principi de responsabilitat proactiva.

En qualsevol cas, és obvi que com més gran és el nombre de respostes afirmatives, més elevat és el risc que es pot derivar del tractament.

Aquest canvi d'enfocament de l'RGPD comporta que les mesures que una entitat aplicava seguint l'RLOPD no són correctes? No. Potser són les adequades, però cal, en tot cas, fer l'anàlisi de riscos per determinar si les mesures implementades són correctes o si hi ha alguna mancança.

En qualsevol cas, les mesures concretes a aplicar han de garantir:

- La confidencialitat, la integritat, la disponibilitat i la resiliència permanents dels sistemes i dels serveis de tractament.

- La capacitat de restaurar la disponibilitat i l'accés a les dades personals de manera ràpida, en cas d'incident físic o tècnic.
- L'existència d'un procés per verificar i avaluar regularment l'eficàcia de les mesures tècniques i organitzatives establertes per garantir la seguretat del tractament



Es poden continuar aplicant les mesures de seguretat que preveia l'RLOPD?

L'RGPD no estableix cap llista de mesures de seguretat basada en els nivells de seguretat bàsic, mitjà i alt, com preveia l'RLOPD. Deixa a criteri del responsable i l'encarregat, prèvia avaluació dels riscos, determinar quines mesures de seguretat cal implementar en cada supòsit.

En qualsevol cas, s'han d'establir les mesures de seguretat tècniques i organitzatives adients per garantir un nivell de protecció adequat al risc. Les mesures previstes a l'RLOPD que ja estiguin implantades poden ser útils, però cal analitzar en cada cas si són suficients o si cal modificar-les.

9.2 Notificació de violacions de seguretat de les dades

Violacions de seguretat de les dades personals: Tota 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.

Situacions com la pèrdua o robatori d'un ordinador portàtil, l'accés no autoritzat a la base de dades (fins i tot per part del propi personal), l'enviament d'informació personal a una persona destinatària errònia, l'alteració de dades sense autorització o la pèrdua de disponibilitat de les dades (per exemple, per haver patit un atac als sistemes amb un programari de segrest, *ransomware*, que xifra les dades) constitueixen violacions de seguretat de les dades i han de ser tractades d'acord amb el que disposen els articles 33 i 34 de l'RGPD.

Si es produeix una violació de la seguretat de les dades, el responsable del tractament l'ha de notificar a l'autoritat de control sense dilació indeguda i, si és possible, en un termini màxim de 72 hores, tret que sigui improbable que constitueixi un risc per als drets i les llibertats de les persones (art 33. RGPD).

A més, quan sigui probable que la violació comporti un alt risc per als drets de les persones, el responsable l'ha de comunicar a les persones afectades sense dilacions indegudes i en un llenguatge clar i senzill, tret que:

- El responsable hagi adoptat mesures de protecció adequades, com ara que les dades no siguin intel·ligibles per a persones no autoritzades.

- El responsable hagi aplicat mesures posteriors que garanteixen que ja no hi ha la probabilitat que es concreti l'alt risc.
- Suposi un esforç desproporcionat (art 34. RGPD).

9.2.1 Quin és el termini per notificar una violació de seguretat de les dades a l'autoritat de control?

La notificació de la violació de seguretat a les autoritats s'ha de produir sense dilació indeguda i, si és possible, dins de les 72 hores següents que el responsable n'ha tingut constància. Aquest criteri pot ser objecte d'interpretacions diverses. En general, es considera que es té constància d'una violació de seguretat quan hi ha una certesa raonable que s'ha produït un incident de seguretat que ha compromès les dades personals i se'n té un coneixement suficient de la naturalesa i l'abast. La mera sospita que hi ha hagut una violació, sense que se'n coneguin mínimament les circumstàncies, encara no haurien 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.

No obstant això, en casos de violacions que per les seves característiques puguin tenir un gran impacte, sí que pot ser recomanable contactar amb l'autoritat de supervisió tan aviat com hi hagi evidències que s'ha produït una situació irregular respecte de la seguretat de les dades. Això, sense perjudici que aquests primers contactes es completin amb una notificació formal, més completa, dins del termini legalment previst.

Si la notificació a l'autoritat de control no es produeix en el termini de les 72 hores, haurà d'anar acompanyada d'una explicació dels motius que han ocasionat el retard.

9.2.2 Quin ha de ser el contingut de la notificació d'una violació de la seguretat de les dades a l'autoritat de control?

La notificació ha de contenir uns elements mínim que el mateix RGPD estableix (art. 33 RGPD) i que inclou la naturalesa de la violació, les categories i nombre aproximat de dades afectades, les mesures adoptades pel responsable per solucionar la violació i, si escau, les mesures aplicades per pal·liar els possibles efectes negatius sobre les persones afectades.

Si no és possible facilitar simultàniament tota la informació, es pot fer de manera gradual, sense dilació indeguda.

Links

Per comunicar una violació de seguretat cal seguir els passos que indiquem a la nostra seu electrònica o al lloc web APDCAT:

- [A la seu de l'APDCAT](#)
- [Al web de l'APDCAT](#)

Amb independència de la notificació a les autoritats, els responsables han de documentar totes les violacions de seguretat. Es tracta d'una obligació que estableix l'RGPD i que s'aproxima molt al registre d'incidències que preveia l'RLOPD.

9.2.3 Quan és probable que una violació de seguretat comporti un risc alt per als drets de les persones afectades?

El criteri de l'alt risc que esmenta l'RGPD s'ha d'entendre en el sentit que sigui probable que la violació de seguretat ocasioni danys importants a les persones interessades. Això pot succeir, per exemple, si es revela informació confidencial, com contrasenyes o la participació en determinades activitats, si es difonen dades sensibles o si es poden produir perjudicis econòmics per a les persones afectades.

9.2.4 Quina és la finalitat de comunicar una violació de seguretat a les persones afectades?

L'objectiu d'aquesta comunicació ha de ser permetre que les persones afectades puguin prendre mesures per protegir-se de les conseqüències de la violació de seguretat. Per això, l'RGPD requereix que se'ls comuniqui sense dilació indeguda i sense fer referència ni al moment en què se'n té constància ni tampoc a la possibilitat d'efectuar la comunicació dins d'un termini de 72 hores. El propòsit és sempre que la persona interessada afectada pugui reaccionar tan aviat com sigui possible.

Pels mateixos motius, l'RGPD afegeix als continguts de la notificació que en cas que s'escaigui caldrà establir recomanacions sobre les mesures que poden prendre les persones afectades per fer front a les conseqüències de la violació.

9.2.5 Què pot passar, si no es notifica una violació de seguretat de les dades?

Si una violació de seguretat no es notifica a l'autoritat de control, es pot incórrer en la vulneració d'una obligació prevista a l'RGPD, tret que sigui improbable que la violació comporti un risc per als drets i les llibertats de les persones físiques.

També pot constituir una vulneració de l'RGPD el fet de notificar la violació de seguretat de dades més enllà de les 72 hores, si no hi ha raons que ho justifiquin. Aquestes vulneracions poden comportar que s'exerceixin poders d'investigació i correctius, inclosa la imposició d'una multa, si escau.

Per contra, no hi ha cap penalització si es notifica a l'autoritat un incident de seguretat que no arriba a tenir la consideració de violació de seguretat de dades personals de notificació obligada.