GUIA INFORMATIVA

Principals canvis en la nova normativa de protecció de dades: la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals (LQPD)

AGÈNCIA ANDORRANA DE PROTECCIÓ DE DADES

28 de gener de 2022

Agència Andorrana de Protecció de dades

ÍNDEX

1) Introducció

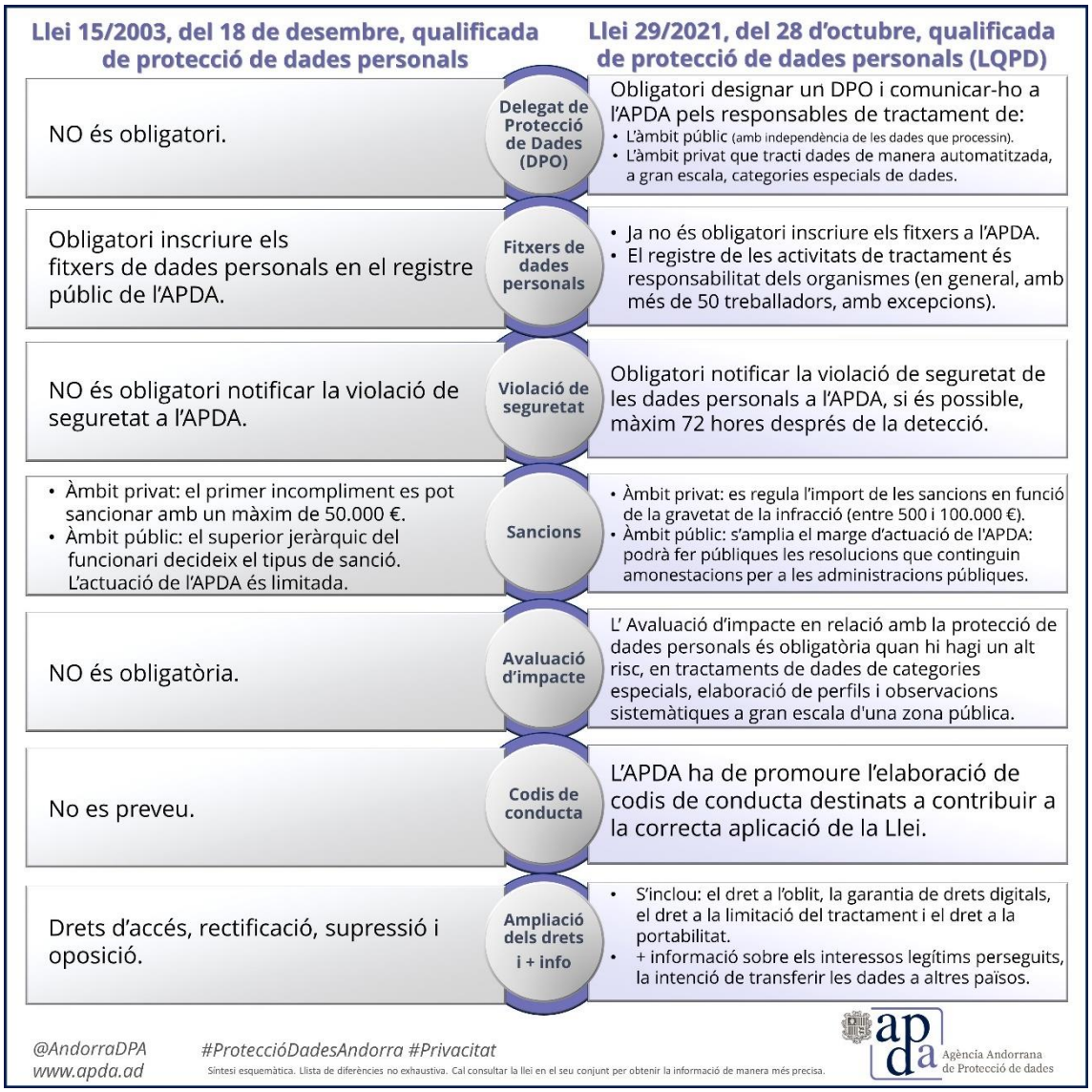
El 28 de gener se celebra el Dia de la Protecció de Dades, data proclamada per la Comissió Europea, el Consell d'Europa i les autoritats de Protecció de Dades dels països signants de la Convenció 108, amb l'objectiu d'impulsar el coneixement entre els ciutadans dels drets que tenen en matèria de protecció de dades, de manera que es puguin familiaritzar amb un dret fonamental, que malgrat que sigui menys conegut, és present en totes les facetes de la vida quotidiana.

El 26 d'abril del 2006 el Consell d'Europa va establir el 28 de gener com a data per celebrar, amb caràcter anual, del Dia de la protecció de dades a Europa, i commemorar així, l'aniversari de la signatura del Conveni 108 del Consell d'Europa per la protecció de les persones pel que fa al tractament automatitzat de dades de caràcter personal.

A ningú se li escapa la constant i imparable evolució tecnològica de la nostra societat i com configura i provoca canvis socials amb els quals les noves tecnologies passen a formar part intrínseca de la nostra vida. Aquesta constant evolució obliga no només els ciutadans sinó també els legisladors a actualitzar-se i a proposar canvis que garanteixin un màxim respecte a les nostres llibertats i als drets individuals. Així, l'any 2021 es va publicar la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals (LQPD) a Andorra que entrarà en vigor a partir del mes de maig del 2022. Aquest nou text normatiu fa que el Dia de Protecció de Dades d'enguany sigui especialment rellevant, ja que la LQPD introdueix noves obligacions que hauran de complir tots aquells que tractin dades personals.

L'Agència Andorrana de Protecció de Dades Personals, per tal d'ajudar a esclarir aquestes noves obligacions, participa en aquesta jornada amb la publicació de la Guia informativa «Principals canvis en la nova normativa de protecció de dades: la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals (LQPD)».

A la Imatge 1 es pot observar una llista no exhaustiva de diferències entre la Llei 15/2003, del 18 de desembre, Qualificada de Protecció de Dades Personals i la Llei 29/2021, del 28 d'octubre, Qualificada de Protecció de Dades Personals (LQPD). Aquí es reflecteixen a grans trets, les principals diferències i l'augment d'obligacions per als responsables de tractament que implicarà la nova llei.



Imatge 1. Llista no exhaustiva de diferències entre la Llei 15/2003, del 18 de desembre, Qualificada de Protecció de Dades Personals i la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals (LQPD)

En alguns casos, les recomanacions o interpretacions que s'ofereixen a la Guia podran implantar-se de forma gairebé immediata, perquè tenen a veure amb actuacions que els responsables ja poden iniciar, com pot ser la nova forma de recollida del consentiment. En altres casos, aquestes recomanacions o propostes han de llegir-se entenent que les obligacions encara no són exigibles als responsables i que encara hi ha pendent la publicació d'un Reglament de desplegament de la nova llei que acabarà de concretar aspectes relatius a les obligacions dels responsables. El fet que s'inclogui a la guia obeeix fonamentalment al propòsit d'oferir una primera aproximació a aquestes novetats.

En aquest context, cal remarcar que un dels propòsits de l'Agència andorrana de protecció de dades (APDA) és anar ampliant la informació sobre aquestes obligacions a través de futures publicacions que veuran la llum durant 2022 amb l'objectiu d'acompanyar el màxim possible a tots els organismes perquè garanteixin la protecció de les dades que tracten.

Una de les funcions que ha de desenvolupar l'APDA fa referència a la promoció de la sensibilització o conscienciació dels responsables i encarregats de tractament respecte a les seves obligacions. Sens dubte, un element de millora de la protecció de les dades personals també el constitueix el fet que els principals subjectes obligats per la regulació coneguin amb el màxim de detall possible les seves obligacions

Vegeu a la Imatge 2 altres funcions definides per la normativa d'aquesta Agència.

Imatge 2. Resum de les funcions que la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals (LQPD) estableix per a l'autoritat de control, l'APDA.

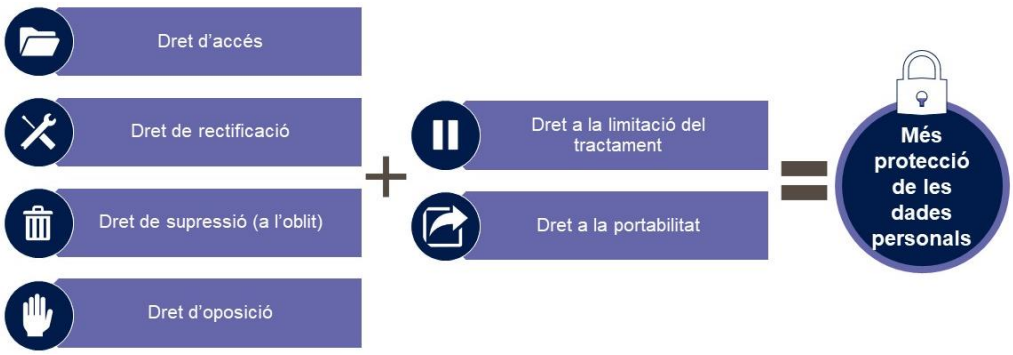
2) Nous drets de l'interessat

La normativa de protecció de dades permet que els interessats puguin exercir davant del responsable del tractament els seus drets d'accés, rectificació, oposició, supressió (dret a l'oblit), limitació del tractament i portabilitat (vegeu la Imatge 3).

Aquests drets es caracteritzen pel punts següents:

- L'exercici és gratuït.
- El responsable està obligat a informar l'interessat sobre els mitjans per exercitar aquests drets.
- Si el responsable no cursa la sol·licitud, informarà en el termini d'un mes de les raons de la seva no actuació i la possibilitat de reclamar davant de l'Autoritat de Control.
- Els drets es poden exercir directament o per mitjà del representant legal.
- La resposta a l'exercici dels drets haurà de fer-se sense dilació i en el termini màxim d'1 mes (en casos de provada dificultat, el termini es podrà prorrogar fins a 2 mesos més, sempre que l'interessat hagi estat informat en el termini establert).

*Alerta! La resposta als exercicis de drets és **OBLIGATÒRIA**: l'interessat ha de veure el seu exercici de dret com a acceptat, rebutjat o prorrogat però sempre haurà de justificar-se la resposta rebuda per part del responsable de tractament.*



Imatge 3. Drets ARSO (Accés, Rectificació, Supressió i Oposició) i nous drets que introdueix la LQPD

2.1. Resum drets ARSO (Accés, Rectificació, Supressió i Oposició)

El **dret d'accés** és el dret que tenen les persones per a adreçar-se al responsable del tractament per conèixer si està tractant o no les seves dades de caràcter personal i, en el cas que s'estigui fent aquest tractament, obtenir-ne la informació següent:

- Les finalitats del tractament.
- Les categories de dades personals de què es tracta.
- Els destinataris o les categories de destinataris als quals es van comunicar o seran comunicades les dades personals, en particular en cas de transferència internacional.
- El termini previst de conservació de les dades personals, o si no és possible, els criteris utilitzats per determinar aquest termini.
- L'existència del dret de l'interessat a sol·licitar al responsable: la rectificació o supressió de les dades personals, la limitació del tractament de les dades personals o oposar-se a aquest tractament, així com el dret a la portabilitat de les dades.
- El dret a presentar una reclamació davant de l'Agència Andorrana de Protecció de dades.
- Quan les dades personals no s'hagin obtingut directament de l'interessat, qualsevol informació disponible sobre el seu origen.
- L'existència de decisions automatitzades, inclosa l'elaboració de perfils; s'ha de facilitar a l'interessat, com a mínim en aquests casos, informació significativa sobre la lògica aplicada, així com la importància i les conseqüències previstes d'aquest tractament per a la pròpia persona.
- En cas de transferència internacional de les dades, el dret a ser informat de les garanties adequades amb què es realitzen.
- Una còpia de les dades personals objecte de tractament.

L'exercici del **dret de rectificació** suposa que l'interessat pot obtenir la rectificació de les seves dades personals que siguin inexactes sense dilació indeguda del responsable del tractament.

Tenint en compte les finalitats del tractament, la persona interessada té dret que es completin les dades personals incompletes, fins i tot mitjançant una declaració addicional.

La persona interessada ha d'indicar en la seva sol·licitud a quines dades es refereix i quina correcció s'hi ha de fer. I ha d'adjuntar a la sol·licitud, quan sigui necessari, la documentació justificativa de la inexactitud o del caràcter incomplet de les dades objecte de tractament.

El responsable del tractament ha de comunicar qualsevol rectificació a cadascun dels destinataris als quals s'han comunicat les dades personals, tret que sigui impossible o requereixi un esforç desproporcionat. Si la persona interessada ho sol·licita, el responsable l'ha d'informar sobre aquests destinataris.

El **dret de supressió** es pot exercir davant la persona responsable, sol·licitant la supressió de les dades de caràcter personal quan concorri alguna de les circumstàncies següents:

- Si les dades personals ja no són necessàries en relació amb les finalitats per a les quals van ser recollides, o són tractades d'una altra manera.
- Si la persona interessada retira el consentiment en què es basa el tractament, i no es basa en cap altre fonament jurídic.
- Si la persona interessada s'oposa al tractament i no hi prevalen altres motius legítims per al tractament, o quan la persona interessada s'oposa al tractament en les circumstàncies següents:

- El tractament de la persona responsable es fonamentava en l'interès legítim o en el compliment d'una missió d'interès públic, i no han prevalgut altres motius per legitimar el tractament de les dades.
- Que les dades personals siguin objecte de màrqueting directe, incloent-hi l'elaboració de perfils relacionats amb l'esmentat màrqueting.

- Si les dades personals s'han tractat il·lícitament.
- Si les dades personals s'han de suprimir per complir una obligació legal.
- Si les dades personals s'han obtingut en relació amb l'oferta directa de serveis de la societat de la informació.

Per motius relacionats amb la seva situació particular i quan el responsable no ha obtingut les dades directament de la persona interessada, es pot exercir el **dret d'oposició** al fet que les dades personals que l'afecten siguin objecte d'un tractament, inclosa l'elaboració de perfils. En cas d'oposició, el responsable deixarà de tractar les dades llevat que acrediti motius imperiosos que prevalguin sobre els interessos, els drets i les llibertats de l'interessat, o per a la formulació, l'exercici o la defensa de reclamacions.

Quan el tractament de dades personals té per objecte el màrqueting directe, la persona interessada té dret a oposar-se en tot moment al tractament de les dades personals que l'afecten, inclosa l'elaboració de perfils relacionada amb el màrqueting esmentat; i, en aquest cas, les dades personals s'han de deixar de tractar per a aquestes finalitats.

Si les dades personals es tracten amb finalitats de recerca científica o històrica o amb finalitats estadístiques, per motius relacionats amb la seva situació particular, la persona interessada té dret a oposar-se al tractament de dades

personals que l'afecten, tret que el tractament sigui necessari per complir una missió realitzada per raons d'interès públic.

2.2. Dret a l'oblit

A més, la LQPD en regular el **dret de supressió** el vincula amb el **dret a l'oblit**, de manera que la persona responsable del tractament en suprimeixin tot enllaç, o les còpies o rèpliques d'aquestes dades.

Això no obstant, aquest dret no és il·limitat, de manera que pot ser factible no procedir a la supressió quan el tractament sigui necessari per a l'exercici de la llibertat d'expressió i informació; per al compliment d'una obligació legal; per al compliment d'una missió realitzada en interès públic o en l'exercici de poders públics conferits a la persona responsable; per raons d'interès públic; en l'àmbit de la salut pública; amb finalitats d'arxiu d'interès públic, finalitats de recerca científica, històrica o finalitats estadístiques; o per a la formulació, exercici o defensa de reclamacions.

2.3. Dret a la portabilitat

La finalitat del nou **dret a la portabilitat** és reforçar encara més el control de les dades personals, de manera que quan el tractament s'efectuï per mitjans automatitzats, els interessats rebin les dades personals en un format estructurat, d'ús comú i de lectura mecànica, i es puguin transmetre a un altre responsable del tractament, sempre que el tractament es legitimi sobre la base del consentiment o en el marc de l'execució d'un contracte.

Això no obstant, aquest dret, per la seva naturalesa, no es pot aplicar quan el tractament sigui necessari per al compliment d'una missió d'interès públic o en l'exercici de poders públics conferits al responsable.

2.4. Dret a la limitació del tractament

El nou **dret a la limitació del tractament** consisteix a obtenir la limitació del tractament de les dades que realitza el responsable, si bé l'exercici presenta dues vessants:

Es pot sol·licitar la suspensió del tractament de les dades:

- Quan s'impugni l'exactitud de les dades personals, durant un termini que permeti al responsable verificar-les.
- Quan s'hagi exercit el dret d'oposició al tractament de les dades personals que el responsable realitza en base a l'interès legítim o a la missió d'interès públic, mentre es verifica si aquests motius prevalen sobre els de l'interessat.

Sol·licitar al responsable la conservació de les teves

- Quan el tractament sigui il·lícit i s'hagi exercit el dret a la supressió de les dades i se'n sol·liciti la limitació de l'ús.
- Quan el responsable ja no necessiti les dades personals per a les finalitats del tractament, però l'interessat les necessiti

3) Noves obligacions del responsable de tractament

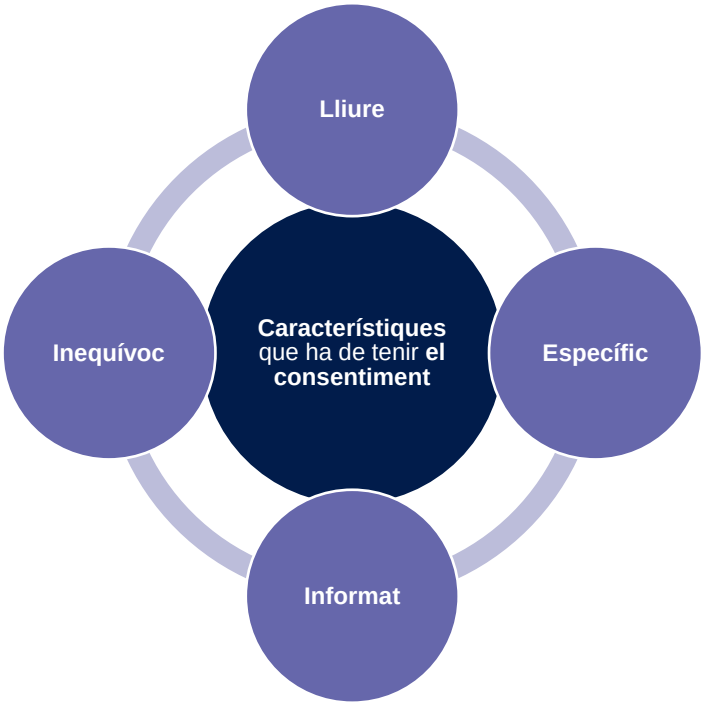
3.1. El consentiment

La Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals (LQPD) defineix el consentiment com "*qualsevol manifestació de voluntat lliure, específica, informada i inequívoca per la qual la persona accepta, mitjançant una declaració o una acció afirmativa clara, el tractament de les dades personals que l'afectin*".

Consentiment de la persona interessada: qualsevol manifestació de voluntat lliure, específica, informada i inequívoca per la qual la persona accepta, mitjançant una declaració o una acció afirmativa clara, el tractament de les dades personals que l'afectin.

3.1.1 Consentiment com a base legitimadora del tractament

Què vol dir un consentiment lliure, específic, informat i inequívoc i recollit mitjançant una declaració o una acció afirmativa clara (vegeu la Imatge 4)?



Imatge 4. Característiques del consentiment

- ***Lliure**:* Per considerar que un consentiment s'ha atorgat lliurement, ha de tenir lloc de manera voluntària. L'element "lliure" implica una **elecció real** per part de l'interessat. Qualsevol element de pressió o influència inadequada que pugui afectar el resultat d'aquesta elecció invalida el consentiment. Així, la llei reconeix l'existència d'un cert desequilibri entre el responsable i l'interessat.

  Per exemple, en una relació empresari-treballador: l'empleat pot preocupar-se que la seva negativa a consentir pugui tenir greus conseqüències en la seva relació laboral, per tant, el consentiment només pot ser una base legal per al tractament en algunes circumstàncies excepcionals.

- ***Específic i informat**:* cal informar l'interessat com a mínim sobre la identitat del responsable del tractament, quin tipus de dades es tractaran, com s'utilitzaran i la finalitat de les operacions de tractament. També s'ha d'informar l'interessat sobre el seu dret a retirar el consentiment en qualsevol moment. La retirada ha de ser tan fàcil com el fet de donar el consentiment. Si escau, el responsable també ha d'informar sobre l'ús de les dades per a la presa de decisions automatitzada, els possibles riscos de les transferències internacionals de dades a causa de l'absència d'una decisió d'adequació o de garanties adequades

  El consentiment es vincularà a una o per a cadascuna de les finalitats especificades (s'hauran d'explicar suficientment). Si el consentiment ha de legitimar el tractament de categories especials de dades personals, la informació de l'interessat hi ha de fer expressa referència.

- ***Inequívoc i mitjançant un acte o una declaració afirmativa**:* El consentiment no pot ser implícit i ha de fer-se sempre mitjançant una clàusula *opt-in,* una declaració o una acció activa, de manera que no hi

hagi malentès del fet que l'interessat ha consentit el tractament en concret. Aquesta declaració o acció no té requisits formals i també serà vàlida la recollida mitjançant formats electrònics.

- Això podria incloure marcar una casella d'un lloc web a internet, escollir paràmetres tècnics per a la utilització de serveis de la societat de la informació, o qualsevol altra declaració o conducta que indiqui clarament en aquest context que l'interessat accepta la proposta de tractament de les seves dades personals. Per tant, el silenci, les caselles ja marcades o la inacció no poden considerar-se com a eines per a consentir.
- Quan el tractament tingui diverses finalitats, cal donar a l'interessat l'opció d'acceptar-les totes, de només una part o de cap.

El consentiment del menor

El consentiment dels infants i adolescents és un cas especial. Per als menors de 16 anys hi ha un requisit addicional de consentiment o autorització del titular de la responsabilitat parental.

3.1.2 Altres bases legitimadores

A part del consentiment, la normativa preveu altres bases legitimadores per al tractament de dades personals:

a) El tractament és necessari per a executar un contracte del qual la persona interessada és part, o bé per a aplicar mesures precontractuals a petició seva.
b) El tractament és necessari per a complir una obligació legal aplicable al responsable del tractament.*****
c) El tractament és necessari per a protegir interessos vitals de la persona interessada o d'una altra persona física.
d) El tractament és necessari per a complir una missió d'interès públic o en l'exercici de poders públics conferits al responsable del tractament.*****

e) El tractament és necessari per a satisfer interessos legítims perseguits pel responsable del tractament o per un tercer, sempre que sobre aquests interessos no prevalguin els interessos o els drets i les llibertats fonamentals de la persona interessada que requereixin la protecció de dades personals, especialment si la persona interessada és menor d'edat.

Alerta! No s'aplica al tractament que en fan les autoritats públiques en l'exercici de les seves funcions.

***** Una normativa establirà aquestes bases del tractament perquè el responsable les pugui aplicar. La finalitat del tractament s'ha de determinar en aquesta base jurídica o bé ha de ser necessària per al compliment d'una missió realitzada en interès públic o en l'exercici de poders públics conferits al responsable del tractament.

La base jurídica o norma haurà de contenir disposicions específiques sobre protecció i tractaments de dades com ara:

> *«les condicions generals que regeixen la licitud del tractament efectuat pel responsable; els tipus de dades objecte de tractament; les persones interessades afectades; les entitats a les quals es poden comunicar dades personals i les finalitats d'aquesta comunicació; la limitació de la finalitat; els terminis de conservació de les dades, així com les operacions i els procediments del tractament, incloses les mesures per garantir un tractament lícit i equitatiu, com les relatives a altres situacions específiques de tractament.»* (article 6, Llei 29/2021, de 28 d'octubre, qualificada de protecció de dades personals).

La base jurídica ha de complir un objectiu d'interès públic i ha de ser proporcional a la finalitat legítima perseguida.

3.2. Deure d'informació

La Llei 29/2021 dona a les persones el dret a ser informades sobre la recollida i l'ús de les seves dades personals, la qual cosa comporta diverses obligacions d'informació per part del responsable del tractament.

3.2.1 Deure d'informació segons la font d'obtenció de les dades:

La llei diferencia dos casuístiques:

Dades obtingudes directament de l'interessat (article 15, Llei 29/2021).	Dades obtingudes no directament de l'interessat (article 16, Llei 29/2021).
Quan?	
• Immediatament, és a dir, en el moment en què s'obtenen les dades.	• En un període de temps raonable, però com a màxim al cap d'un mes. • Si les dades personals s'han d'utilitzar per comunicar-se amb la persona interessada, com a màxim al moment de comunicar-les per primera vegada. • Si està previst comunicar les dades personals a un altre destinatari, com a màxim moment de comunicar-les per primera vegada.

Contingut:

L'obligació d'informar del responsable del tractament inclou:

- la seva **identitat**,
- les dades de contacte del **Delegat de Protecció de Dades** (si estan disponibles),
- les **finalitats** del tractament i la **base legal**,
- els i**nteressos legítims perseguits**,
- els **destinataris** a l'hora de transmetre dades personals i qualsevol intenció de **transferir** dades personals a tercers països,
- informació sobre la **durada** de l'emmagatzematge,
- els **drets** de l'interessat,
- la **capacitat de retirar el consentiment**,
- el **dret a presentar una reclamació** davant les autoritats, i
- sobre l'**obligatorietat o no de facilitar dades** en base a un requisit legal o contractual.

Pel que fa al contingut, el responsable del tractament ha de proporcionar la mateixa informació específica que si les dades personals s'haguessin obtingut directament de l'interessat.

- L'única excepció és la informació sobre qualsevol obligació de facilitar les dades personals, ja que el responsable del tractament no té l'autoritat de decisió en aquest cas.
- A més, el responsable del tractament té l'obligació d'informar de quines fonts s'han originat les dades personals i si estaven disponibles públicament.

L'interessat ha de ser informat de **qualsevol activitat de presa de decisions automatitzada**, inclosa la creació de perfils.

Només si l'interessat ja coneix la informació anterior, no és necessari facilitar-la.	En casos excepcionals no hi ha obligació d'informar: • Si el subministrament de la informació és impossible o té un cost excessiu, • la recopilació i/o la transmissió és obligatòria per llei, o • si les dades han de romandre confidencials per secret professional o altres obligacions de secret legal.

Com?

L'interessat té dret a ser informat d'una forma precisa, transparent, comprensible i de fàcil accés. L'obligació d'informar es pot complir per escrit o de forma electrònica. S'indica explícitament que els anomenats "símbols d'imatge estandarditzats" també es poden utilitzar per transmetre una visió general significativa del processament previst de forma entenedora i clara.

3.2.2 Informació per capes

Se segueix un enfocament per nivells per **presentar la informació bàsica exigida de forma resumida** perquè l'interessat pugui fer-se una idea general sobre el tractament i **oferir la resta d'informació, més detallada, en un segon nivell** (vegeu la Imatge 5).

- **Informació bàsica o resumida (primera capa/nivell):** Redacció senzilla i sense gaire informació (es desenvoluparà en la segona capa). Incloure un epígraf que faci referència a:

- **Responsable** - indicar denominació.
- **Finalitat** - enumerar cadascuna de les finalitats previstes i si es faran o no perfils, o es prendran decisions automatitzades.
- **Destinataris** o tipus de destinataris de les dades.
- **Drets** - fer referència a la possibilitat d'exercir els drets d'accés, oposició, rectificació, supressió (a l'oblit), dret a la limitació del tractament i dret de portabilitat.
- **Categories de dades** (en el cas de no haver obtingut les dades de l'interessat) - ex. dades identificatives, acadèmiques, laborals i economicofinanceres.
- **Procedència** - ex. Com hem obtingut les dades?

- **Informació detallada (segona capa/nivell):** Completar amb tot tipus de detalls la informació continguda als epígrafs de la primera capa o afegir-ne de nous si així es desitja.
  - **Responsable** - identitat i dades de contacte (adreça postal i correu electrònic) + dades de contacte del DPO, si escau.
  - **Finalitat** - determinar totes les finalitats. Cal evitar fórmules massa genèriques que puguin conduir a tractaments posteriors que vagin més enllà de les expectatives raonables dels interessats. En cas que s'elaborin perfils o es prenguin decisions automatitzades, incloure informació sobre la lògica aplicada i les conseqüències previstes d'aquests tractaments.
  - **Destinataris** o tipus de destinataris de les dades- identitat, comunicacions internacionals (país tercer? decisió d'adequació? etc).
  - **Drets** - forma i mecanismes detallats per exercir drets (models, formularis, contacte) + possibilitat de reclamar davant l'autoritat de control.

- **Legitimació** - base legal del tractament de dades (consentiment interessat, execució d'un contracte, obligació legal, etc).

EPÍGRAF	1a CAPA	2a CAPA
RESPONSABLE	Identitat del responsable de tractament	Dades de contacte del responsable Identitat i dades del representant Delegat de protecció de dades
FINALITAT	Descripció de les finalitats del tractament	Descripció àmplia de les finalitats Termini de conservació de les dades
LEGITIMACIÓ DESTINATARIS	Base jurídica del tractament	Detallar la base: Interès públic o legítim Obligació o no de facilitar les dades i conseqüències de no fer-ho
DESTINATARIS DE CESSIONS	Previsió o no de cessions	Destinataris concrets o categories de destinataris (*Alerta! Es pot posar un enllaç en una plana web on s'actualitzin els destinataris i no haver de canviar constantment la clàusula d'informació*).
DRETS	Referència a l'exercici dels drets	Com exercir-los: Dret a retirar el consentiment prestat Dret a reclamar davant de l'APDA
PROCEDÈNCIA DE LES DADES	Font de les dades (quan no procedeixen de l'interessat)	Informació de l'origen de les dades Categories de dades que es tractin

Imatge 5. Informació per capes

Exemple:

Responsable del tractament:
Agència andorrana de protecció de dades.

Primera capa

Responsable del tractament:
Agència andorrana de protecció de dades. C/Doctor Vilanova 15, Ed. Consell General, Planta -5, AD500 Andorra la Vella, ANDORRA. 808 115 apda@apda
DPD: (nom i cognoms + adreça de contacte).

Segona capa

3.3. Responsabilitat proactiva

3.3.1 Registre de les activitats de tractament

Qui?

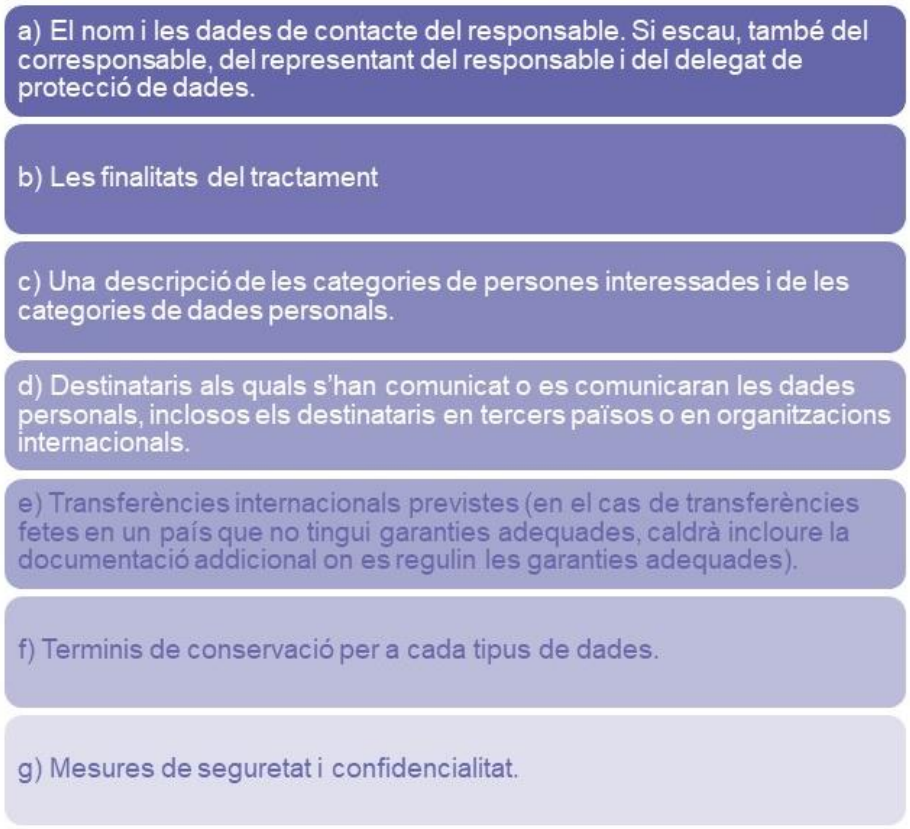
A partir del maig del 2022 ja no serà necessari declarar els fitxers a l'APDA sinó que aquesta obligació serà responsabilitat de l'entitat que tracti les dades personals, en concret (vegeu la Imatge 6):

- Administració pública, parapúbliques, empreses o organitzacions públiques.
- Empreses amb més de 50 treballadors
- Empreses que realitzin tractaments habituals de:
  - Dades sensibles.
  - Dades relatives a condemnes i infraccions penals.
  - Dades amb un risc per als drets i les llibertats.

Imatge 6. Característiques de les entitats obligades a realitzar el registre de les activitats de tractament de dades

Dins d'aquestes organitzacions, qui haurà de portar el registre serà el responsable, el corresponsable, l'encarregat de tractament, el representant o el Delegat de Protecció de Dades (que haurà de ser informat de qualsevol addició, modificació o exclusió en el contingut dels registres).

Contingut mínim que s'ha de registrar (vegeu la Imatge 7)



Imatge 7. Contingut mínim del Registre d'Activitats de Tractament

Com s'ha de registrar?

Per escrit o electrònicament.

Per què s'ha de registrar?

El Registre d'Activitats de Tractament (RAT) és una nova obligació que neix de la necessitat que els responsables de tractament tinguin una responsabilitat activa en matèria de protecció de dades. És un element que ajudarà a acreditar que la seva actuació és conforme a la normativa andorrana de protecció de dades.

El responsable o l'encarregat del tractament i, si escau, el seu representant, han de posar el registre a disposició de l'Agència Andorrana de Protecció de Dades quan aquesta autoritat de control ho sol·liciti.

3.3.2 Mesures tècniques i organitzatives

Protecció de dades *by design* i *by default* (vegeu Imatge 8)

"Protecció de dades *by design* (des del disseny)" i "Protecció de dades *by default* (per defecte)" són dos termes que s'empren des de fa anys en matèries reguladores de protecció de dades i ja apareixien a la derogada Directiva 95/46/CE de la Unió Europea. Segons el considerant 46 d'aquesta Directiva, les mesures tècniques i organitzatives **s'han de prendre en el moment de planificar un tractament de dades per tal protegir-ne la seguretat.** Es busca l'adopció d'un model basat en l'anticipació del responsable i en la presa de mesures proactives per prevenir i anticipar possibles problemes de privacitat.

Quins criteris caldrà tenir en compte quan dissenyem les nostres estratègies *by design* i *by default*?

- La naturalesa, àmbit, context i finalitat del tractament
- Els riscos de diversa probabilitat i gravetat (no només respecte al risc alt)
- Estat de la tècnica
- Cost

Protecció de dades *by design*	Protecció de dades mitjançant un disseny tecnològic → el respecte a la privacitat és una part essencial del producte, del servei o del tractament que s'està desenvolupant. Cal que els interessats i la seva intimitat siguin sempre la referència i la prioritat i que durant la vida útil de l'aparell, del software o en el tractament de dades, aquest respecte es mantingui constant. No es pot condicionar l'ús d'aquesta tecnologia a una concessió o una rebaixa de garanties en privacitat. • *Ex. No es pot configurar una plana web per tal de condicionar la navegació a l'acceptació de* cookies.

Protecció de dades *by default*	Moltes entitats intenten que posem en risc la nostra privadesa perquè ens diuen que així aconseguim noves funcionalitats, millors experiències, etc (Ex. «Si es garantís totalment la privadesa de l'usuari no seria tan barat o tan útil el servei»). El *Privacy by Design* demostra que un producte, tractament o servei pot estar plenament operatiu amb totes les funcionalitats actives, sense deixar de banda la privadesa dels usuaris. Protecció de dades en la configuració inicial o en els paràmetres de fàbrica → Qualsevol producte, servei o tractament de dades no requereix cap actuació activa per part de l'usuari o l'interessat per protegir-ne la privacitat. • *Ex. El nostre dispositiu mòbil vindrà amb una configuració de fàbrica garantista amb la nostra privacitat i nosaltres, mitjançant accions afirmatives, anirem reduint aquesta privacitat → Vols permetre que "Mapes" tingui accés a la teva ubicació?*

Imatge 8. Protecció de dades by design i by default

Formació de treballadors i personal amb accés a dades

«Una cadena és tan forta com ho és la seva baula més feble» Thomas Reid.

Forma part essencial de la responsabilitat activa dels responsables de tractament (i ara també, dels delegats de protecció de dades) transmetre els coneixements necessaris en matèria de privacitat als seus treballadors i conscienciar a tot el personal que tingui accés a dades personals de la seva importància. Una plantilla formada i conscienciada redueix immediatament el risc de patir fuites de dades o males praxis i demostra una actitud proactiva del responsable de tractament en el respecte a la privacitat dels interessats.

Alerta! La formació ha d'adaptar-se al tipus de dades tractades, als riscs inherents en el tractament de dades realitzat i a la pròpia naturalesa de les funcions del treballador. No ha de tenir la mateixa formació en protecció de dades un recepcionista que l'informàtic de l'empresa.

3.3.3 Avaluació d'impacte (AI)

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

En identificar els riscos, hem de considerar qualsevol impacte que el tractament pugui tenir sobre els drets fonamentals de les persones: impossibilitat d'accedir a serveis, discriminació, robatori de la identitat i altres fraus, danys a la reputació, impossibilitat d'exercir algun dret, etc.

Aquests impactes es poden materialitzar per dues raons principals:

- la primera és que el tractament, tal com està dissenyat, pugui donar lloc a aquests impactes (pel tipus de dades que es tracten, per qui hi té accés, pel potencial efecte del tractament, etc); i
- la segona està relacionada amb la seguretat de les dades, en particular, la pèrdua de la confidencialitat, la integritat o la disponibilitat de les dades.

Per controlar els riscos inherents al tractament, s'han d'establir els **controls necessaris** per garantir que el tractament es fa d'acord amb els principis de la normativa de protecció de dades: adequació, necessitat, proporcionalitat, etc. Alhora, també s'hauran d'establir una sèrie de mecanismes per tal de garantir que els interessats puguin exercir els seus drets.

Un cop determinats els riscos caldrà valorar-los i, després, establir les salvaguardes apropiades a les valoracions fetes.

Quan caldrà fer una AI?

L'article 32.3 de la LQPD exigeix que el responsable del tractament realitzi una AI, quan el tractament pugui comportar un alt risc per als drets i les llibertats de les persones i estableix 3 casuístiques on serà obligatòria:

- 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 a què es refereix, o de les dades personals relatives a condemnes i infraccions penals
- Observació sistemàtica a gran escala d'una zona d'accés públic.

Exemples no exhaustius d'operacions de tractament on caldrà fer una AI:

- **Avaluació o puntuació**, incloses l'elaboració de perfils i prediccions, especialment en relació amb el rendiment laboral, situació econòmica, salut, preferències o interessos personals, fiabilitat o comportament, ubicació o moviments.

  Exemples:

  - Una institució financera que investiga els seus clients en una base de dades de referència de crèdit.
  - Una empresa biotecnològica que ofereix proves genètiques per avaluar i predir els riscos de patir malalties.
  - Una empresa que fa perfils de comportament basats en la navegació web.

- **Presa de decisions automatitzada amb efectes jurídics o que afecta de manera similar i significativa la persona física.**
  - Per exemple, un tractament automatitzat que pot donar lloc a exclusió o discriminació de les persones.
- **Observació sistemàtica d'una àrea d'accés públic**. En aquest tractament, les dades es poden recollir sense que els interessats siguin conscients que s'estan recollint i de com s'usaran.
- **Tractament de dades sensibles o relatives a condemnes i infraccions penals.** També pot incloure dades que augmenten el risc per als drets i les llibertats de les persones (com ara dades de comunicacions electròniques, dades de localització i dades financeres) o documents personals, correu electrònic, diaris, notes de lectors de llibres electrònics i informació personal inclosa en aplicacions de registre d'activitats vitals.
- **Tractament de dades a gran escala.** Per determinar si un tractament és a gran escala, cal tenir en compte els factors següents:
  - El nombre de persones a les quals es refereixen les dades, ja sigui en termes absoluts o com a proporció de la població subjacent.
  - El volum o la varietat de dades.
  - La durada o permanència de l'operació de tractament.
  - L'extensió geogràfica de l'operació de tractament.
- **Dades relacionades amb persones vulnerables.** Això inclou totes les situacions en què es detecti un desequilibri entre la posició del responsable del tractament i l'interessat.

  Per exemple:
  - Tractament de dades d'empleats en relació amb la gestió de recursos humans.

  - Nens i persones grans.
  - Persones amb malalties mentals o discapacitats.
- **Ús innovador de tecnologies**
- **Tractament que en si mateix impedeix l'exercici d'un dret o l'ús d'un servei o contracte.**

  Per exemple:

  - Tractaments fets en un espai públic que els transeünts no poden evitar.
  - Consulta de l'historial de crèdit d'un client per part d'un banc, per decidir si li concedeix un crèdit.

Independentment del risc que pugui tenir un tractament, **no caldrà fer una AI** quan la naturalesa, l'abast, el context i les finalitats del tractament siguin molt semblants a un altre tractament al qual ja s'ha fet una AI.

Quan?

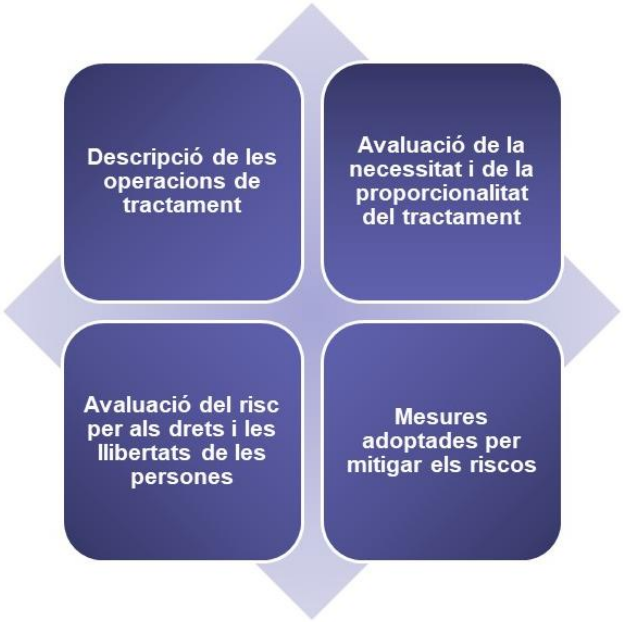
Tan aviat com sigui possible.

En particular, per a nous tractaments cal fer-la abans d'iniciar el tractament (respectant el principi de protecció de dades *by design* i *by default*) i cal emprar l'AI com a guia i base per al disseny del tractament.

En el cas d'una operació de tractament que ja està en marxa, convé fer una AI tan aviat com es detecti un risc greu per als drets i les llibertats de les persones.

Alerta! Una AI no és una tasca puntual, sinó que implica un procés continu de revaluació → caldrà revisar les nostres AI cada vegada que es produeixin canvis en el tractament o en el seu context.

Contingut mínim de l'AI (vegeu la Imatge 9)**:**



Imatge 9. Contingut mínim de l'Avaluació d'Impacte

Qui?

El responsable del tractament és l'actor principal, atès que és qui té la responsabilitat que l'AI s'executi. Això no treu que el responsable del tractament pugui delegar l'AI però, en qualsevol cas, és qui en té la responsabilitat última.

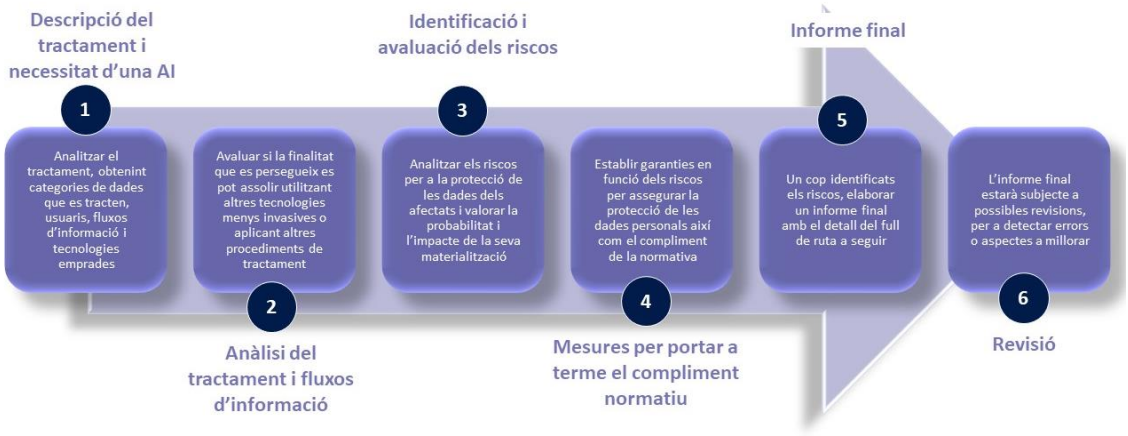
El prestador de serveis, si n'hi ha, ha de donar suport al responsable a l'hora de fer l'AI.

El responsable del tractament ha de buscar el consell del delegat de protecció de dades (DPD). Aquest consell i les decisions que prengui han de quedar documentades a l'AI. En particular, el responsable del tractament ha de demanar opinió al DPD en els aspectes següents:

- Determinar si cal fer una AI.
- La metodologia a usar en l'AI.
- Determinar si convé fer l'AI internament o si és millor externalitzar-la.

- Les mesures adoptades per protegir els drets i les llibertats de les persones.
- Determinar si l'AI s'ha fet correctament i si les conclusions satisfan els requeriments de protecció de dades.

Fases d'una avaluació d'impacte (vegeu la Imatge 10)



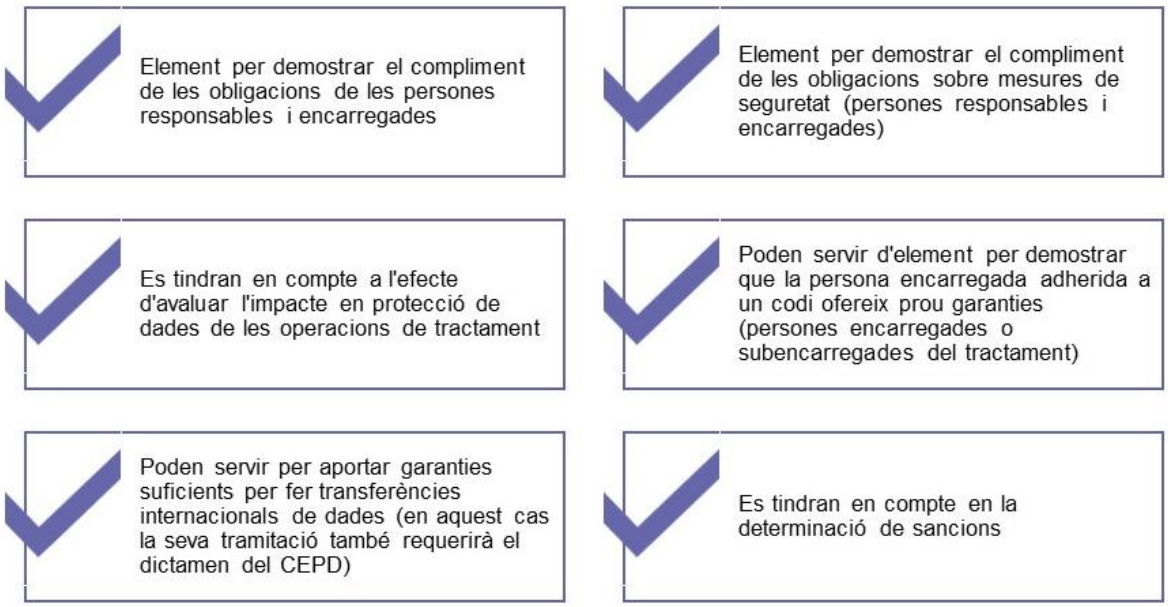
Imatge 10. Fases d'una avaluació d'impacte

3.3.4 Codis de conducta

Què és un codi de conducta?

Els codis de conducta (CC) són un conjunt de pautes i directrius que regulen les obligacions en matèria de protecció de dades de determinats sectors professionals. La principal funció és la d'adequar i facilitar l'aplicació de la normativa de protecció de dades a les característiques dels diferents sectors d'activitat dels seus promotors, que s'hi adheriran de manera voluntària per tal que els resulti d'obligat compliment.

Els principals incentius per tal de desenvolupar CC (vegeu la Imatge 11):



Imatge 11. Principals incentius per tal de desenvolupar un Codi de Conducta

Qui pot elaborar un codi de conducta?

L'ha de constituir una organització representativa d'un sector d'activitat. L'elaboració d'un codi de conducta es basa en un enfocament sectorial que ha de ser iniciat per una associació, una federació o una organització que representi categories de responsables o encarregats de tractament.

Aquesta organització ha de poder demostrar que és ben representativa del sector. Això es pot fer mitjançant índexs com ara el nombre de membres representats, l'experiència de l'organització en el sector rellevant, etc.

Exemples:

- Sector bancari.
- Col·legis professionals.
- Empreses i grups d'empreses (ex. PIMES).
- Universitats.
- Fundacions del sector públic i del sector privat.
- Associacions.

- Organismes que assumeixin funcions de supervisió i resolució extrajudicial de conflictes.
- Etc.

Contingut:

L'objecte és especificar l'aplicació de la normativa andorrana de protecció de dades en aspectes com ara:

- un tractament de dades lleial i transparent;
- els interessos legítims perseguits per responsables del tractament en contextos específics;
- la forma de recollida de dades personals;
- la seudonimització de dades personals;
- la informació proporcionada a les persones interessades;
- l'exercici dels drets de les persones interessades;
- la informació proporcionada als menors d'edat i la seva protecció, així com la manera d'obtenir llur consentiment o el dels titulars de la seva pàtria potestat;
- les mesures i procediments per garantir la seguretat del tractament, així com la protecció de dades des del disseny i per defecte;
- procediments de notificació de violacions de la seguretat tant a l'APDA com a les persones interessades;
- la transferència de dades personals a tercers països i organitzacions internacionals; i
- els procediments extrajudicials i altres procediments de resolució de conflictes que permetin resoldre les controvèrsies relatives al tractament de dades, sense perjudici dels drets de les persones interessades.

Els CC han de presentar-se davant l'APDA perquè n'analitzi la validesa i idoneïtat. Els projectes de CC hauran de presentar-se juntament amb la documentació següent:

Document	Contingut
Memòria justificativa, clara i concisa	Descripció detallada de l'objectiu, àmbit d'aplicació material (operacions de tractament, persones afectades, categories de responsables i encarregats) i territorial (definint també l'autoritat de control competent) i de com facilitarà l'aplicació efectiva de la normativa de protecció de dades.
La justificació de la legitimació del promotor	La representativitat del titular del codi s'ha de demostrar i es pot valorar pel que fa al nombre d'organitzacions que representa respecte al sector, el nombre potencial d'adherents al codi i la seva experiència en el sector i els tipus d'operacions de tractament afectades
Consulta amb les parts interessades	Els obligats per un CC han de ser consultats sobre el propi projecte i han d'emetre la seva opinió. L'absència d'aquesta consulta ha de justificar-se.

Govern del CC	El titular del codi ha d'indicar com s'organitzarà la relació entre els membres, el titular i l'òrgan supervisor al llarg de la vida del CC. Així, la governança es pot reflectir en la indicació de les condicions d'adhesió al codi de conducta, el mecanisme de sortida del codi, el procés d'actualització dels requisits del codi, els criteris de selecció de l'òrgan de control, etc.
Els mecanismes de supervisió i l'organisme de supervisió	La designació d'un òrgan de supervisió dels codis de conducta relatius al tractament realitzat per autoritats i organismes públics no és obligatòria. No obstant això, les directrius recomanen el desplegament d'un mecanisme de control per a la correcta aplicació del codi de conducta.

Criteris d'aprovació dels codis

Per a l'aprovació, l'APDA valorarà si els codis presentats:

- Satisfan una necessitat específica del sector o activitat de tractament de què es tracti → el format del codi ha de facilitar-ne la comprensió. Ús pràctic i aplicació efectiva de la normativa andorrana de protecció de dades per part dels professionals del sector que no són necessàriament experts en protecció de dades.
- Faciliten i especifiquen l'aplicació de la normativa de protecció de dades → el codi defineix mesures operatives, solucions concretes que els

membres poden aplicar per complir amb les obligacions en matèria de protecció de dades.

- Aporten garanties suficients.
- Disposen de mecanismes suficients per supervisar-ne el compliment.

Codis transnacionals

Quan el codi afecti operacions de tractament en diversos estats, s'haurà de presentar davant l'autoritat de control competent. Aquesta autoritat es determinarà segons:

- ✓ La ubicació de la densitat més gran del sector o de l'activitat de tractament.
- ✓ La ubicació de la major densitat d'interessats afectats pel sector o activitat de tractament.
- ✓ La ubicació de la seu del titular del codi.
- ✓ La ubicació de l'organisme de supervisió.
- ✓ Les iniciatives desenvolupades per una autoritat de control en un àmbit específic.

Òrgan supervisor

El CC designarà una entitat que controlarà el compliment i la implementació del CC. Aquest òrgan actuarà paral·lelament a les funcions de control de l'APDA i podrà sancionar també els infractors. Les condicions per esdevenir òrgan supervisor es fixaran en una guia pròpia.

3.3.5 Notificacions de violacions de seguretat

Una violació de la seguretat de les dades es produeix quan les dades personals que tracta un responsable o encarregat de tractament pateixen un incident de seguretat que dona lloc a la violació de la confidencialitat, disponibilitat o integritat de les dades. Si això passa, i és possible que la violació posi en risc els drets i les llibertats d'una persona, tal com preveu l'article 36 de la llei

29/2021, del 28 d'octubre, qualificada de protecció de dades personals, el responsable de tractament ha de notificar-ho a l'autoritat de control sense demora i a tot estirar 72 hores després de tenir-ne constància. Si la notificació no es produeix en aquest termini, s'han de justificar els motius de la dilació. Si és un encarregat del tractament, haurà de notificar cada violació de la seguretat de les dades al responsable del tractament.

D'altra banda, tal com es preveu a l'article 15 de la llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals, si la violació de la seguretat de les dades suposa un alt risc per a les persones afectades, aquestes també hauran de ser informades tan aviat com raonablement sigui possible (llevat que s'hagin aplicat mesures de protecció tècniques i organitzatives efectives, o altres mesures que garanteixin que ja no existeix la probabilitat que es determini el risc).

Tipus de violacions de seguretat (vegeu la Imatge 12)**:**

- ✓ "Violació de la confidencialitat": quan es produeix una revelació o s'ha accedit de manera no autoritzada o accidental a les dades personals.
- ✓ "Violació de la integritat": quan es produeix una alteració no autoritzada o accidental de les dades personals.
- ✓ "Violació de la disponibilitat": quan es produeix una pèrdua d'accés accidental o no autoritzat a les dades personals, o bé s'han destruït.

Imatge 12. Tipus de violacions de seguretat

Procediment de notificació a l'APDA:

Quan el responsable de tractament notifica una violació de seguretat a l'autoritat de control, l'article 36 de la llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals, estableix que com a mínim, ha de:

a) Descriure la naturalesa de la violació de la seguretat de les dades personals, incloent-hi, si és possible, les categories i el nombre aproximat de persones interessades afectades, i les categories i el nombre aproximat de registres de dades personals afectats.

b) Comunicar el nom i les dades de contacte del delegat de protecció de dades o d'un altre punt de contacte on es pot obtenir més informació.

c) Descriure les possibles conseqüències de la violació de la seguretat de les dades personals.

d) Descriure les mesures adoptades o proposades pel responsable del tractament per fer front a la violació de la seguretat de les dades personals, incloses, si escau, les mesures adoptades per mitigar-ne els possibles efectes negatius.

Per facilitar el compliment d'aquests requisits en el contingut de les notificacions de violacions de seguretat, l'APDA posarà a disposició dels responsables de tractament un formulari estandarditzat de notificació. En tot cas, l'APDA podrà requerir al responsable tota la informació addicional necessària.

La informació mínima que haurà de contenir aquesta notificació és sobre:

- Caràcter de la notificació.
- Informació general sobre el tractament.
- Intencionalitat i origen.
- Tipologia de la violació de seguretat (si afecta la confidencialitat, la disponibilitat o la integritat).
- Categoria de dades i perfil dels afectats.
- Conseqüències.
- Resum de la violació de seguretat.
- Implicacions transfrontereres.
- Informació temporal de la violació de seguretat i mitjans de detecció.
- Mesures de seguretat abans de l'incident.
- Accions preses.
- Comunicació als afectats.
- Identificació dels intervinents.
- Documentació adjunta a la notificació.

Una vegada notificada una violació de seguretat a l'APDA, el responsable de tractament ha d'estar preparat per rebre i atendre els possibles requeriments, ordres o comunicacions que l'APDA pugui fer electrònicament en relació amb la violació de seguretat notificada.

- Després de notificar una violació de seguretat, el responsable de tractament pot rebre per part de l'APDA diverses comunicacions o notificacions electròniques, per exemple:

- Comunicació amb informació relativa al registre de la violació de seguretat notificada.
- Notificació amb un requeriment d'informació addicional sobre violació de seguretat o el tractament de dades personals en qüestió, en virtut de les funcions i les potestats d'aquesta Agència.
- Notificació amb una ordre per comunicar als afectats la violació de seguretat en virtut de l'article 37, en considerar que el risc per als afectats és alt, en virtut de les funcions i potestats d'aquesta Agència a què fa referència l'article

En cas de rebre un requeriment d'informació addicional, el responsable de tractament haurà d'atendre'l en el termini indicat al requeriment.

Notificació als interessats:

El responsable del tractament ha de prendre les mesures oportunes per facilitar a la persona interessada tota la informació relativa al tractament de les seves dades, entre la qual també hi ha la violació de la seguretat de les dades personals de la persona interessada en el cas escaient.

Aquesta informació s'ha de facilitar d'una manera concisa, transparent, intel·ligible i de fàcil accés, amb un llenguatge clar i senzill, sobretot si la informació s'adreça específicament a un menor d'edat. La informació s'ha de facilitar per escrit o per altres mitjans, inclosos, si escau, els mitjans electrònics.

3.4. Transferències internacionals de dades personals

S'entén per transferència internacional de dades qualsevol comunicació de dades personals o la seva posada a disposició a favor d'un destinatari subjecte a la jurisdicció d'un tercer país, o quan el destinatari sigui una organització internacional.

Exemples:

- *Cessió de dades de treballadors a empresa de prevenció de riscos laborals ubicada fora d'Andorra.*
- *Contractació d'un servei de* cloud *ubicat fora d'Andorra.*
- *Utilització de serveis de* newsletters *gratuïts d'empreses no andorranes.*
- *Etc.*

La norma general diu que es prohibeixen les transferències internacionals de dades fetes a països i organitzacions internacionals que llur normativa vigent no garanteixi un nivell de protecció equivalent al que assegura la normativa andorrana de protecció de dades.

→ Quan podrem transferir dades fora d'Andorra, doncs?

Quan disposem o establim GARANTIES ADEQUADES.

Transferència a països de la UE	Transferència a països que la UE ha considerat adequats amb una Decisió d'Adequació	Transferència a països amb submissió efectiva al Conveni 108+

Transferència amb garanties i amb drets i accions legals exigibles → aquí caldrà que les dues parts, emissor i receptor de les dades, arribin a pactes obligatoris que regulin la transferència de dades i li confereixin garanties equivalents a les de la normativa de protecció de dades.

Aquest pactes poden fer-se a través de:

- Instruments vinculants entre autoritats o organismes públics.
- Normes corporatives vinculants.
- Clàusules tipus de protecció de dades de la Comissió Europea o de l'APDA.
- Adhesió a codis de conducta vàlids a Andorra o la UE.
- Mecanismes de certificació aprovats conforme a les normes de

protecció de dades de la UE.

Alerta! L'APDA és l'encarregada d'avaluar l'existència o no d'aquestes garanties. Per tant, qualsevol responsable que vulgui procedir a la transferència internacional de dades mitjançant un d'aquests instruments, haurà de presentar, ABANS DE LA TRANSFERÈNCIA, tota la documentació explicativa d'aquestes garanties addicionals per tal que l'autoritat de control en decideixi la pertinença. Davant un informe negatiu de l'Agència, la transferència es considerarà il·legítima.

Excepcions[1]

En determinades situacions específiques es podran transferir dades sense garanties específiques si:

- La persona interessada ha donat explícitament el seu consentiment a la transferència proposada, després d'haver-la informat dels riscos d'aquestes transferències a causa de l'absència d'una decisió d'adequació i de garanties adequades.

Alerta! La informació relativa a l'existència de garanties adequades o no ha de donar-se ABANS de procedir a la transferència.

- La transferència és necessària per a executar un contracte:
  - Entre la persona interessada i el responsable del tractament.
  - Entre el responsable del tractament i una altra persona física o jurídica, en interès de la persona interessada.

1 Totes les excepcions han d'interpretar-se de forma estricta i restrictiva i analitzant-ne cas per cas.

  - Per a executar mesures precontractuals adoptades a sol·licitud de la persona interessada.
- Raons importants d'interès públic → interpretació molt restrictiva.
- La transferència és necessària per a formular, exercir o defensar reclamacions.
- La transferència és necessària per a protegir els interessos vitals de la persona interessada o d'altres persones, quan està físicament o jurídicament incapacitada per donar-ne el consentiment.
- La transferència s'efectua des d'un registre públic que té per objecte facilitar informació al públic i està obert a la consulta del públic en general, o de qualsevol persona que hi acrediti un interès legítim.

I les autoritats públiques?

«(...) si no existeix decisió d'adequació, ni tampoc existeixen garanties adequades, i no es pot aplicar a la transferència o a un conjunt de transferències de dades personals cap de les excepcions específiques (...), la transferència només es pot dur a terme si no és repetitiva, afecta un nombre limitat de persones interessades, i és necessària per a les finalitats d'interessos legítims imperiosos perseguits pel responsable del tractament, sobre els quals no prevalen els interessos o els drets i les llibertats de la persona interessada, i 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.» (article 45.2, Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals).

4) La relació entre el responsable de tractament i altres figures: corresponsable, encarregat de tractament, representant i Delegat de Protecció de Dades (DPD)

4.1. Determinació dels responsables

El **responsable del tractament** determina les finalitats i els mitjans relacionats amb el tractament de les dades personals. De manera que, si una persona decideix el «per què» i el «com» cal tractar les dades personals, aquesta persona és responsable del tractament.

Alerta! Els treballadors que realitzen el tractament de les dades personals a l'organització del responsable del tractament ho fan en compliment de les funcions que aquest exerceix.

Un **coresponsable del tractament** existirà quan, de forma conjunta, dos o més responsables del tractament, determinin «per què» i «com» s'hauran de tractar les dades personals. Els coresponsables del tractament han de signar un acord on estableixin les responsabilitats i funcions de cadascun i com compliran amb les obligacions de la normativa andorrana de protecció de dades.

Els principals aspectes de l'acord es comunicaran a les persones interessades mitjançant el seu dret a la informació.

D'altra banda, **l'encarregat del tractament** és qui tracta les dades personals per compte del responsable del tractament. L'encarregat del tractament de dades sol ser un tercer, extern a l'empresa. Ex. Una activitat típica dels encarregats és oferir solucions informàtiques, com ara l'emmagatzematge al núvol.

Alerta! En el cas de grups d'empreses, una pot actuar com a encarregada del tractament per a una altra.

Les tasques i obligacions de l'encarregat del tractament respecte al responsable s'han d'especificar en un contracte o altre acte jurídic. L'encarregat només pot subcontractar una part d'aquesta tasca a un altre encarregat o designar-ne un coencarregat quan hagi rebut l'autorització prèvia per escrit del responsable del tractament.

Hi ha situacions en què una entitat pot ser responsable o encarregada del tractament, o ambdues coses. En qualsevol dels casos, es determinarà si és un responsable, un coresponsable, un encarregat o un subencarregat, **atenent a les funcions i les actuacions que es duguin a terme sobre les dades.**

4.2. Contractes d'encarregats de tractament i cessió de dades

4.2.1 La forma del contracte

El contracte d'encarregat de tractament és un document o acte jurídic que vincula el responsable i l'encarregat del tractament i regula les relacions entre tots dos respecte al tractament de les dades personals.

Aquest contracte ha d'establir-se **per escrit o en format electrònic.**

- Els responsables han d'informar els interessats de la ratificació de contractes d'encarregats de tractament?

  La nova llei 29/2021 no estableix l'obligació d'informar sobre la contractació d'un encarregat del tractament. Malgrat això, en determinades circumstàncies (atenent, per exemple, a la sensibilitat de les dades o a l'encàrrec) pot ser aconsellable donar aquesta informació per a més transparència en el tractament de dades personals.

4.2.2 El contingut del contracte

El contracte pot basar-se en clàusules tipus establertes per la Comissió Europea o per l'APDA però no és un requisit obligatori. El que sí que serà

necessari és que el contracte tingui el contingut mínim següent (article 31.4, Llei 29/2021):

- **Servei que l'encarregat prestarà** → són les instruccions del responsable. És necessari identificar de forma clara i concreta quins són els tractaments de dades a realitzar per l'encarregat del tractament, atenent el tipus de servei prestat i la forma de prestar-ho. És especialment necessari determinar de forma clara les comunicacions a tercers que el responsable encomana a l'encarregat o que es deriven del servei prestat.

Alerta! Si l'encarregat del tractament considera que alguna de les instruccions infringeix la normativa andorrana de protecció de dades, l'encarregat ha d'informar immediatament el responsable.

- **Durada del tractament, tipus de dades a les quals s'accedirà i categories de persones afectades.**
  - Què passarà amb les dades un cop s'extingeixi el contracte (retorn o destrucció)?
- **Deure de confidencialitat i mesures de seguretat a aplicar** → Cal establir com l'encarregat del tractament garantirà que les persones autoritzades s'han compromès, de forma expressa, a tractar dades personals i a respectar la confidencialitat de les dades a les quals tinguin accés.
  - L'acord ha d'establir l'obligació de l'encarregat d'adoptar totes les mesures de seguretat necessàries. Correspon al responsable del tractament fer l'avaluació de riscos per determinar les mesures de seguretat apropiades per garantir la seguretat de la informació tractada i els drets de les persones afectades. Així mateix, l'encarregat també ha d'avaluar els possibles riscos derivats del

tractament, tenint en compte els mitjans utilitzats (tecnologies, recursos etc.) i altres circumstàncies que puguin incidir en la seguretat, com per exemple que l'encarregat faci altres tractaments.

A partir d'aquí, la determinació de les mesures de seguretat concretes es pot fer mitjançant una llista exhaustiva, o amb la remissió a un estàndard o a un marc nacional o internacional reconegut.

- **Drets dels interessats** → Cal establir la forma en què l'encarregat del tractament assistirà el responsable per al compliment de l'obligació de respondre a les sol·licituds que tinguin per objecte l'exercici dels drets dels interessats
- **Règim de subcontractació** → quan podrem subcontractar una part de l'encàrrec? Com ens haurà d'autoritzar el responsable per a fer-ho? Qui respondrà pels actes del subencarregat?
- **La col·laboració amb el responsable per demostrar el compliment** → Cal establir l'obligació de l'encarregat de posar a disposició del responsable tota la informació necessària per demostrar el compliment de les obligacions de l'encarregat, així com per permetre i contribuir a la realització d'auditories o inspeccions.

4.3. El Delegat de Protecció de Dades (DPD)

La Llei 29/2021, de 28 d'octubre, qualificada de protecció de dades personals ha establert el concepte de Delegat de Protecció de Dades (DPD) a Andorra.

El criteri per determinar l'obligació de nomenar un DPD dependrà de la mida de l'organització o de les activitats bàsiques de tractament que són essencials per assolir els objectius de l'empresa.

- Si aquestes activitats bàsiques consisteixen en el tractament de dades personals sensibles a gran escala o en una forma de tractament de

dades que tingui un abast particular per als drets de les persones interessades, l'empresa ha de designar un DPD.

Els organismes públics o parapúblics, en canvi, sempre han de designar un DPD, a excepció dels tribunals que actuen en la seva capacitat judicial.

Alerta! Si no hi ha cap obligació legal, les empreses també poden designar un DPD de manera voluntària per ajudar en el compliment de la protecció de dades .

4.3.1 Qui pot ser designat DPD?

- Un treballador de l'organització a càrrec del responsable de tractament.
- Un DPD extern com a encarregat de tractament.

En seleccionar aquesta persona, el responsable ha d'assegurar-se que el DPD no pugui tenir conflicte d'interessos i que aporti coneixements professionals experts en dret de protecció de dades (l'abast d'aquests coneixements depèn de la complexitat del tractament de dades i de la mida de l'empresa).

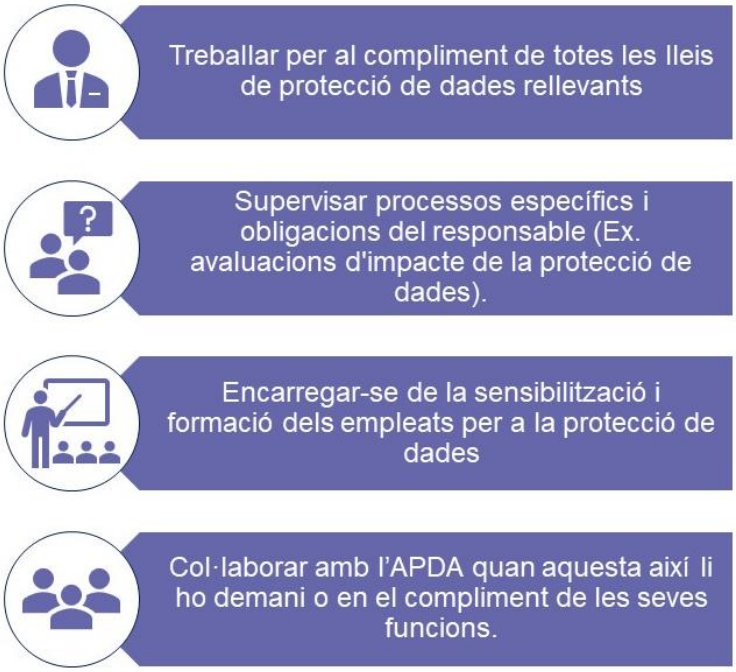
Quan es nomena un DPD, el responsable ha de fer públiques les seves dades de contacte i comunicar el nomenament i dades de contacte a l'APDA.

- Si una empresa ha designat voluntàriament un DPD, també ha de complir els criteris i les disposicions anteriors.

La falta deliberada o negligent de nomenar un DPD quan hi hagi una obligació legal és una **infracció subjecta a multes**.

4.3.2 Funcions generals del DPD

Les funcions generals d'un Delegat de Protecció de Dades es poden veure a la Imatge 13:



Imatge 13. Funcions generals del DPD

Alerta! Malgrat la seva funció de seguiment, la pròpia empresa continua sent responsable del compliment de les lleis de protecció de dades.

5) Sancions

La nova Llei 29/2021, de 28 d'octubre, qualificada de protecció de dades personals recull també **un nou règim sancionador** on llista i quantifica les possibles infraccions que puguin dur a terme responsables o encarregats de tractament en l'exercici de les seves funcions.

Ara bé, per tal de valorar les infraccions, l'APDA tindrà en compte una sèrie de criteris que analitzarà cas per cas per tal de determinar l'import de la multa administrativa com són:

- La naturalesa, la gravetat i la durada de la infracció, segons l'operació de tractament, així com el nombre de persones interessades afectades i el nivell dels danys i perjudicis que hagin sofert.
    - Qualsevol mesura presa pel responsable o l'encarregat del tractament per pal·liar els danys i perjudicis que han sofert les persones interessades.
- La intencionalitat o la negligència en la infracció.
- El grau de responsabilitat del responsable o de l'encarregat del tractament, tenint en compte les mesures tècniques o organitzatives que s'hagin aplicat en la protecció de les dades i la seguretat del tractament.
- Qualsevol infracció anterior que hagin comès el responsable o l'encarregat del tractament o el compliment de mesures correctives prèvies.
- El grau de cooperació amb l'APDA, amb la finalitat de posar remei a la infracció i de mitigar-ne els possibles efectes adversos.
- Les categories de dades de caràcter personal afectades per la infracció.
- La forma en què l'APDA s'ha assabentat de la infracció, en particular si el responsable o l'encarregat del tractament han notificat la infracció i, si és així, en quina mesura i en quin termini ho han fet.
- L'adhesió a codis de conducta.
- Etc.

Així, les conductes infractores es podran classificar en (vegeu Imatge 14, Imatge 15 i Imatge 16):

Grau	Infraccions	Quantia
Molt greus	Dur a terme tractaments de dades que no compleixin amb els principis de la Llei 29/2021 (article 5).	30.001 euros a 100.000 euros
	Dur a terme tractaments de dades il·lícits.	
	Tractaments fets sense consentiment vàlid de l'interessat.	
	Tractament il·lícit de dades sensibles, dades relatives a condemnes o infraccions penals o dades amb finalitat d'arxiu d'interès públic, científic, històric o estadístic.	
	Omissió del deure d'informar.	
	Impediment, obstaculització, no atenció o exigència de cànon econòmic en la resposta als exercicis dels drets dels interessats (excepte en supòsits permesos per la llei).	
	Transferències internacionals de dades sense garanties adequades.	
	Reversió deliberada d'un procediment d'anonimització.	
	Incompliment de resolucions de l'APDA o manca de cooperació en les seves potestats d'inspecció.	

Imatge 14. Infraccions molt greus

Grau	Infraccions	Quantia
Greus	Encarregar el tractament a un tercer sense un contracte o acte jurídic equivalent, o la contractació d'un subencarregat sense l'autorització del responsable.	15.001 a 30.000 euros
	Dur a terme tractaments de dades sense avaluació d'impacte quan així ho obligui la llei.	
	No disposar d'un Registre d'Activitats de Tractament.	
	Incomplir amb els deures de notificar violacions de seguretat.	
	Incomplir amb els deures de designar un DPO o un representant establert a Andorra.	
	Incomplir amb els deures de bloqueig de dades.	
	Tractaments de dades de menors sense el seu consentiment o de llurs tutors legals o no acreditar la realització d'esforços raonables per comprovar-ne la validesa.	
	L'impediment, l'obstaculització o la no atenció reiterada dels drets en tractaments en què no es requereix la identificació de la persona interessada, quan aquesta, per a l'exercici d'aquests drets, hagi facilitat informació addicional que en permeti la identificació.	
	La falta d'adopció de les mesures tècniques i organitzatives apropiades per garantir que les dades es tracten només per les finalitats determinades o l'incompliment de les mesures implantades.	
	La falta d'atenció per part del representant del responsable o de l'encarregat del tractament de les sol·licituds que efectuïn l'autoritat de protecció de dades o les persones interessades.	
	No possibilitar la participació efectiva del delegat de protecció de dades en totes les qüestions relatives a la protecció de dades personals, no donar-li suport o interferir en l'exercici de les seves funcions.	

Imatge 15. Infraccions greus

Grau	Infraccions	Quantia
Lleus	L'incompliment del principi de transparència de la informació o el dret d'informació de la persona interessada per no facilitar-ne tota la informació.	500 a 15.000 euros
	L'incompliment de l'obligació d'informar la persona interessada, quan així ho hagi sol·licitat, dels destinataris als quals s'hagin comunicat les dades personals rectificades, suprimides o respecte de les quals s'ha limitat el tractament.	
	L'incompliment de l'obligació de suprimir les dades referides a una persona difunta.	
	Falta de formalització entre corresponsables de les funcions, obligacions i responsabilitats de cadascun o no posar a disposició dels interessats aquest acord.	
	L'incompliment de l'obligació de l'encarregat del tractament d'informar el responsable del tractament sobre la possible infracció, per una instrucció rebuda d'aquest, de les disposicions de la normativa de protecció de dades.	
	L'incompliment per part de l'encarregat de les estipulacions imposades en el contracte que regula el tractament o les instruccions del responsable del tractament, tret que hi estigui obligat de conformitat amb aquesta Llei.	
	Disposar d'un registre d'activitats de tractament que no incorpori tota la informació requerida.	
	La notificació incompleta, tardana o defectuosa a l'autoritat de protecció de dades, de la informació relacionada amb una violació de seguretat de les dades personals.	
	L'incompliment de l'obligació de documentar qualsevol violació de seguretat.	
	No publicar les dades de contacte del delegat de protecció de dades, o no comunicar-les a l'autoritat de protecció de dades, quan el nomenament sigui exigible.	
	Els altres actes i les conductes que siguin contraris a aquesta Llei i no siguin considerats infraccions molt greus o greus.	

Imatge 16. Infraccions lleus

I l'administració?

L'administració no està subjecta al règim de sancions aquí especificat sinó que es basarà en les seves pròpies normes disciplinàries. L'APDA pot amonestar l'actuació de l'Administració però no imposar sancions econòmiques a les mateixes. Si una resolució de l'APDA determina que un organisme públic ha violat la normativa de protecció de dades:

- Farà pública la resolució per tal de donar publicitat a la infracció.
- Traslladarà la resolució al superior jeràrquic de l'òrgan infractor per tal que se li apliquin les mesures coercitives escaients.

Glossari

Anonimització: procés que consisteix a eliminar tots els elements identificatius d'un conjunt de dades personals perquè ja no sigui possible identificar la persona interessada.

Autoritat de control: organisme públic establert per l'Estat amb personalitat jurídica pròpia, independent de les administracions públiques, amb competències de registre, control, inspecció, resolució i sanció, així com de proposició d'adopció de normes, en matèria de protecció de dades personals.

Consentiment de la persona interessada: qualsevol manifestació de voluntat lliure, específica, informada i inequívoca per la qual la persona accepta, mitjançant una declaració o una acció afirmativa clara, el tractament de les dades personals que l'afectin.

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, com imatges facials, dades dactiloscòpiques o patrons d'iris.

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

Dades personals o de caràcter personal: tota informació numèrica, alfabètica, gràfica, fotogràfica, acústica o de qualsevol altre tipus relativa a una persona física identificada o identificable ("persona interessada"); s'entén per persona física identificable qualsevol persona amb una identitat que es pugui determinar, directament o indirectament, en particular mitjançant un identificador, o un o diversos elements específics, característics de la seva identitat física, fisiològica, genètica, psíquica, econòmica, cultural o social.

Dades relatives a la salut: dades personals relatives a la salut física o mental d'una persona física que revelen informació sobre el seu estat de salut, inclosa la prestació de serveis d'atenció sanitària.

Destinatari: persona física o jurídica, autoritat pública, servei o qualsevol altre organisme al qual es comuniquen dades personals, sigui o no una tercera persona. Això no obstant, les autoritats públiques que poden rebre dades personals en el marc d'una investigació concreta, no s'han de considerar destinataris, de conformitat amb la normativa aplicable. El tractament d'aquestes dades efectuat per les autoritats públiques referides ha de ser conforme a les normes en matèria de protecció de dades aplicables a les finalitats del tractament.

Elaboració de perfils: qualsevol forma de tractament automatitzat de dades personals consistent a utilitzar aquestes dades per avaluar determinats aspectes personals 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.

Empresa: persona física o jurídica dedicada a una activitat econòmica, independentment de la seva forma jurídica, incloses les societats o les associacions que exerceixen regularment una activitat econòmica.

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

Fitxer de dades personals ("fitxer"): qualsevol conjunt estructurat de dades personals accessibles d'acord amb criteris determinats, ja sigui centralitzat, descentralitzat o repartit de forma funcional o geogràfica, qualsevol que sigui la seva forma o modalitat de creació, emmagatzematge, organització i accés.

Grup empresarial: grup constituït per una empresa que exerceix el control i les seves empreses que controla.

Interès públic: concepte definit i determinat entès com a avantatge general, important i primordial, que justifica la finalitat de la intervenció de l'Estat i en fonamenta la legitimitat, sempre dins del marc de l'objectivitat i dels principis constitucionals de legalitat, de jerarquia, de publicitat de les normes jurídiques, de no retroactivitat de les disposicions restrictives de drets individuals o que comportarien un efecte o establirien una sanció desfavorables, de seguretat jurídica, de responsabilitat dels poders públics i d'interdicció de tota arbitrarietat.

Interès vital: interès essencial per a la vida de la persona interessada.

Limitació del tractament: el marcatge de les dades de caràcter personal conservades, amb la finalitat de limitar-ne el tractament en el futur.

Normes corporatives vinculants: les polítiques de protecció de dades personals assumides per un responsable o un encarregat del tractament, adoptades de conformitat amb la normativa de protecció de dades personals de la Unió Europea, per a transferències o per a un conjunt de transferències de dades personals a un responsable o a un encarregat en un o més tercers països, dins d'un grup empresarial o d'una unió d'empreses dedicades a una activitat econòmica conjunta.

Organització internacional: una organització internacional i els seus ens subordinats de dret internacional públic, o qualsevol altre organisme creat mitjançant un acord entre dos o més països o en virtut d'aquest acord.

Persona interessada: la persona física identificada o identificable a la qual corresponen les dades de caràcter personal objecte de tractament.

Representant: persona física o jurídica que, havent estat designada per escrit pel responsable o per l'encarregat del tractament, representa el responsable o l'encarregat del tractament pel que fa a les seves respectives obligacions en el tractament de dades personals.

Responsable del tractament o responsable: la persona física o jurídica, autoritat competent, pública si escau, servei o qualsevol altre organisme que, sol o juntament amb d'altres, determina les finalitats i els mitjans del tractament de dades personals, i vetlla per al correcte compliment de conformitat a les normes en matèria de protecció de dades que són d'aplicació a les finalitats del tractament.

Servei de la societat d'informació: tot servei prestat normalment a canvi d'una remuneració, a distància, per via electrònica i a petició individual d'un destinatari de serveis. Als efectes d'aquesta definició, s'entén per: (i) a distància: un servei prestat sense que les parts hi siguin presents simultàniament; (ii) per via electrònica: un servei enviat des de la font i rebut mitjançant equipaments electrònics de tractament (inclosa la compressió digital) i d'emmagatzematge de dades i que es transmet, canalitza i rep enterament per fils, radi, mitjans òptics o qualsevol altre mitjà electromagnètic; i (iii) a petició individual d'un destinatari de serveis: un servei prestat mitjançant transmissió de dades a petició individual.

Seudonimització: el tractament de dades personals de manera que no es puguin atribuir a una persona interessada 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.

Tercer: persona física o jurídica, autoritat pública, servei o organisme, diferent de la persona interessada, 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 del tractament de dades personals.

Tractament de dades personals ("tractament"): qualsevol operació o conjunt d'operacions efectuades mitjançant procediments, automatitzats o no, sobre dades de caràcter personal, 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, la difusió, la posada a disposició, o qualsevol altra forma d'habilitació d'accés, acarament o interconnexió, limitació, bloqueig, supressió o destrucció de dades, o l'aplicació d'operacions lògiques i/o aritmètiques a aquestes dades.

Transferència internacional de dades: comunicació de dades personals o la seva posada a disposició a favor d'un destinatari subjecte a la jurisdicció d'un tercer país o quan el destinatari sigui una organització internacional.

Violació de la seguretat de les dades personals: qualsevol violació de la seguretat que ocasiona, de manera accidental o il·lícita, en tot cas no autoritzada, la pèrdua, l'alteració, o la divulgació de dades personals transmeses, conservades o tractades d'una altra manera, o la comunicació o l'accés no autoritzats a aquestes dades.

Índex d'imatges

C/ Dr. Vilanova, 15-17
Nova seu del Consell General, planta -5
AD500 Andorra la Vella
Principat d'Andorra
+(376) 808115
apda@apda.ad
@AndorraDPA
www.apda.ad

AGÈNCIA ANDORRANA DE PROTECCIÓ DE DADES

Agència Andorrana
de Protecció de dades