GUIA INFORMATIVA

Guia informativa de l'Avaluació d'Impacte en Protecció de Dades (AI)

AGÈNCIA ANDORRANA DE PROTECCIÓ DE DADES

Versió 1: 27 de gener del 2023

Agència Andorrana de Protecció de Dades

Historial de versions

Versió	Data	Detall de la modificació
Versió 1	27 de gener del 2023	Document original

Índex

1) Introducció

La Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals (LQPD) incorpora una nova obligació per als responsables de tractaments: avaluar l'impacte de les operacions de tractament en la protecció de les dades personals, quan sigui probable que el tractament comporti un risc significatiu per als drets i les llibertats de les persones.

En general, la normativa proposa un model equiparat amb l'estàndard europeu, de compliment orientat a la gestió, és a dir, aposta perquè els responsables demostrin una gestió responsable i proactiva en protecció de dades.

Què entenem quan parlem de riscos significatius? Existeixen dos grans grups de riscos associats a tractaments de dades: els riscos inherents al tractament i els riscos associats a la seguretat i a la confidencialitat de les dades. Ambdós grups hauran de ser avaluats i ponderats per tal de determinar que en cas que el tractament suposi efectivament un risc massa elevat, convindrà ajustar la conducta o la pràctica d'aquell responsable. Per exemple, si de l'anàlisi dels riscos inherents al tractament de dades es considera que hi ha riscos massa elevats per als drets i llibertats dels afectats, caldrà modificar el tractament en si: evitar recollir dades sensibles, restringir l'accés a cert tipus de dades, etc.

Una avaluació d'impacte en protecció de dades (AI) és un procediment que pretén identificar i controlar els riscos associats a un tractament de dades.

2) Avaluacions d'impacte

2.1. Definició

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.

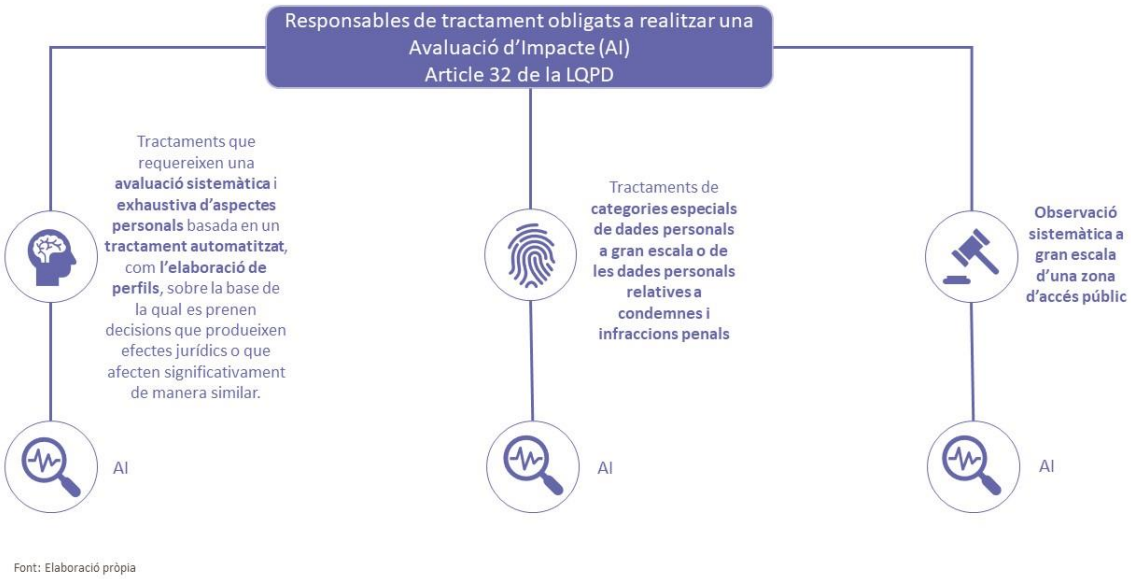
Com hem vist, aquests impactes es poden materialitzar per dues raons principals: la primera és que el tractament, tal com està dissenyat, pugui donar lloc a aquests impactes (pel tipus de dades que es tracten, per qui hi té accés, pel potencial efecte del tractament, etc.); i la segona està relacionada 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, hem 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 haurem d'establir una sèrie de mecanismes per tal de garantir que els interessats puguin exercir-ne els drets.

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

2.2. Quan cal fer una AI?

L'article 32 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 (vegeu la Imatge 1).



Imatge 1. Responsables de tractament obligats a realitzar una AI

a) **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.**

b) **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**

c) **Observació sistemàtica a gran escala d'una zona d'accés públic.**

2.2.1. Concepte "d'alt risc"

Ara bé, l'article 32 de la LQPD no descriu què s'entén per "alt risc" sinó que emplaça l'Agència Andorrana de Protecció de Dades perquè publiqui una llista d'operacions de tractament que requereixin d'una avaluació d'impacte (vegeu annex 1). Alhora, i en la línia d'altres autoritats de protecció de dades com la *Commission Nationale de l'Informatique et des Libertés* (CNIL) o la *Agencia*

Española de Protección de Datos (AEPD), la manca d'especificitat relativa a l'alt risc es pot suplir amb el procediment descrit pel Comitè Europeu de Protecció de Dades (antic Grup de Treball de l'article 29 – GT29) que estableix una llista de 9 característiques de tractaments que poden indicar que ens trobem davant d'un tractament que presenta un alt risc que puguin tenir lloc

1. **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:
    a. Una institució financera que investiga els seus clients en una base de dades de referència de crèdit.
    b. Una empresa biotecnològica que ofereix proves genètiques per avaluar i predir els riscos de patir malalties.
    c. Una empresa que fa perfils de comportament basats en la navegació web.
2. **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.
3. **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.
4. **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.
5. **Tractament de dades a gran escala**. Per determinar si un tractament és a gran escala, cal tenir en compte els factors següents:

   a. El nombre de persones a les quals es refereixen les dades, ja sigui en termes absoluts o com a proporció de la població subjacent.
   b. El volum o la varietat de dades.
   c. La durada o la permanència de l'operació de tractament.
   d. L'extensió geogràfica de l'operació de tractament.
6. **Conjunts de dades que s'han enllaçat o combinat.**
7. **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:
   a. Tractament de dades d'empleats en relació amb la gestió de recursos humans.
   b. Nens i persones grans.
   c. Persones amb malalties mentals o discapacitats.
8. **Ús innovador de tecnologies.**
9. **Tractament que en si mateix impedeix l'exercici d'un dret o l'ús d'un servei o contracte**. Per exemple:
   a. Tractaments fets en un espai públic que els transeünts no poden evitar.
   b. Consulta de l'historial de crèdit d'un client per part d'un banc, per decidir si li concedeix un crèdit.

De la mateixa manera, **l'article 17.3 del Reglament d'aplicació de la Llei 29-2021, del 28 d'octubre, qualificada de protecció de dades personals (el Reglament d'aplicació de la LQPD), defineix un tractament que comporta un risc alt en funció del compliment de dos o més dels criteris següents dins de l'operació de tractament**:

a) **L'avaluació o puntuació dels interessats, inclosa l'elaboració de perfils.**

b) **La presa de decisions automatitzades amb efectes jurídics significatius per a les persones físiques o que les afectin significativament de manera similar.**

c) **L'observació sistemàtica d'interessats.**

d) **Dades sensibles (especialment protegides).**

e) **Un tractament de dades a gran escala.**

f) **L'associació o la combinació de conjunts de dades.**

g) **Dades relatives a interessats vulnerables, com ara menors, empleats o grups més vulnerables de la població que necessiten una protecció especial.**

h) **L'ús innovador o l'aplicació de noves solucions tecnològiques o organitzatives.**

i) **El tractament impedeix als interessats exercir un dret, utilitzar un servei o executar un contracte.**

j) **Tractaments de dades economicofinanceres per part d'entitats bancàries o establiments financers.**

D'aquesta manera, el Reglament d'aplicació de la LQPD afegeix una criteri més als 9 ja descrits pel GT29, el de **"Tractaments de dades economicofinanceres per part d'entitats bancàries o establiments financers".**

2.2.2. Concepte de "gran escala"

En aquest punt, convé mencionar que l'article 17.5 del Reglament d'aplicació de la LQPD també aporta els criteris que defineixen el concepte de "gran escala":

a) El nombre de persones afectades, ja sigui en termes absoluts o com a proporció d'una població determinada.

b) El volum i la varietat de dades tractades. En qualsevol cas, el tractament de dades personals de més de cinc mil afectats implica la consideració de tractament a gran escala.

c) La durada o la permanència de l'activitat de tractament.

d) L'extensió geogràfica de l'activitat de tractament.

A l'annex 3 es pot trobar una proposta de càlcul orientatiu per a determinar tractaments a gran escala.

Independentment del risc que pugui tenir un tractament, **no cal fer una AI** en els casos següents:

- Quan la naturalesa, l'abast, el context i les finalitats del tractament són molt semblants a un altre tractament per al qual ja s'ha fet una AI.
- Quan un tractament té una base jurídica d'un estat de la Unió Europea o d'un país considerat adequat per la Comissió Europea.
- Quan el tractament està inclòs en una llista de tractaments (publicada per l'Agència andorrana de protecció de dades) que no requereixen una AI (vegeu annex 2).

Les operacions de tractament poden evolucionar ràpidament, cosa que pot afectar els riscos i la necessitat d'executar una AI, com també els canvis en el context del tractament. Per exemple, canvis en l'estructura organitzativa del responsable del tractament, o canvis socials que incrementen el risc o la percepció que en tenim. Un exemple del darrer cas seria quan la societat pren consciència del fet que hi ha un grup de persones que és vulnerable a patir d'una discriminació.

Si l'AI és obligatòria i no s'executa, els tractaments queden exposats a uns riscos no detectats. No s'hauran analitzat ni valorat i, en conseqüència, no s'hauran adoptat les mesures que haurien de servir per mitigar els efectes negatius que les operacions de tractament poden tenir per als drets i les llibertats de les persones i pot comportar en la incoació d'expedients administratius prevists a la normativa andorrana de protecció de dades.

2.3. Contingut mínim

Les AI també són instruments útils en relació amb el principi de responsabilitat proactiva (en anglès, *accountability*).

Una avaluació d'impacte no deixa de ser un informe o un recull de documentació on s'analitzen les característiques del tractament avaluat i les decisions preses per mitigar-ne els riscos. En base a aquests riscos, també es valora la necessitat i la proporcionalitat de les operacions de tractament.

2.3.1. En quin moment cal fer l'AI?

Tan aviat com sigui possible.

En particular, **per a nous tractaments cal fer l'AI 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. **Convé remarcar que les AI no són una tasca puntual, sinó que impliquen un procés continu de revaluació** → caldrà revisar les nostres AI cada vegada que es produeixin canvis en el tractament o en el seu context.

2.3.2. Quin és el contingut mínim d'una AI?

- Descripció de les operacions de tractament.
- Avaluació de la necessitat i de la proporcionalitat del tractament.
- Avaluació del risc per als drets i les llibertats de les persones.
- Mesures adoptades per mitigar-ne els riscos.

2.3.3. Quines fases té una AI?

La realització d'una AI ha de seguir un procés sistemàtic, objectiu, repetible i comparable dividit en, com a mínim, 7 fases (vegeu la Imatge 2):

1. **Conveniència de fer una AI**. Tot i que aquesta part hauria de ser una anàlisi prèvia, perquè quedi constància que **s'ha avaluat la conveniència de dur a terme una AI**, serà la primera secció del nostre informe d'AI.

2. **Descripció sistemàtica del tractament**. La descripció del tractament i el context en què té lloc és essencial per determinar els riscos que comporta. En aquesta fase s'ha d'analitzar en profunditat el projecte obtenint el **detall de les categories de dades que es tracten, els actors que intervenen en el tractament, els afectats, els processos de tractament, els fluxos d'informació i les tecnologies utilitzades**.

3. **Avaluació de la necessitat i la proporcionalitat del tractament**. Qualsevol tractament de dades té una finalitat. Cal dissenyar el tractament que sigui menys lesiu per assolir aquesta finalitat (necessitat) i cal que el benefici del tractament sigui superior als potencials perjudicis (proporcionalitat). Cal demanar-se si **es pot assolir aquesta finalitat utilitzant altres tecnologies menys invasives o aplicant altres procediments o mitjans de tractament.**

4. **Gestió de riscos en la seguretat de les dades**. S'avalua el risc sobre els drets i les llibertats de les persones que pot tenir la vulneració de la seguretat de les dades. El risc es deriva de l'impacte i de la probabilitat

que la vulneració es produeixi. Com més alt sigui el risc, més exhaustius han de ser els controls per reduir-lo. En aquesta fase s'avalua **la probabilitat i l'impacte de la materialització dels riscos i es determinen els controls i les mesures que s'han d'adoptar per eliminar, mitigar, transferir o acceptar els riscos detectats.**

5. **Anàlisi del compliment normatiu**. Revisió de si el projecte que requereix el tractament de dades **compleix amb els requeriments legals en matèria de protecció de dades.**

6. **Documentació (informe final) i implantació**. **El resultat d'una AI és un document que descriu les anàlisis fetes en els punts anteriors** (un capítol per fase). També recull una relació detallada dels riscos identificats i les recomanacions i propostes per eliminar-los o mitigar-los amb les mesures previstes per afrontar aquests riscos, incloses garanties, mesures de seguretat i mecanismes que assegurin la protecció de dades personals tenint en compte els drets i els interessos legítims de les persones interessades i d'altres persones afectades.

7. **Monitoratge i revisió**. L'AI no s'acaba quan es completa la documentació i la implantació. **Les AI necessiten un procés de monitoratge per detectar canvis en els riscos** (ja sigui a conseqüència de canvis en el tractament, en la percepció de risc de la societat o per altres riscos que podrien haver passat desapercebuts), que poden requerir que es revisi l'AI o, fins i tot, que es refaci.

   Per a una correcta identificació dels riscos, és recomanable dur a terme, al llarg del procés i en els moments oportuns, consultes amb totes aquelles parts, tant internes com externes a l'entitat, que puguin ser afectades pels tractaments de dades objecte d'avaluació.

Imatge 2. Fases de l'Avaluació d'Impacte.

Què passa si el tractament és d'alt risc? (consulta prèvia – article 33 de la LQPD)

Segons l'article 33 de la LQPD, si l'AI conclou que el tractament comporta un alt risc, el responsable del tractament ha de lliurar l'informe de l'AI per tal de consultar l'Agència andorrana de protecció de dades la legitimitat del tractament ***ABANS*** *d'iniciar-lo. Tal com indica l'article 17.10 del Reglament d'aplicació de la LQPD, aquesta* ***consulta prèvia*** *es fa de forma telemàtica. L'Agència pot instar el responsable a aportar posteriorment qualsevol informació que consideri rellevant per donar resposta a la consulta feta. Un cop l'autoritat de control té tota la documentació necessària, ha de respondre per escrit en un termini de vuit setmanes. Aquest termini es pot ampliar sis setmanes més, d'acord amb la complexitat del tractament.*

L'Agència Andorrana de Protecció de Dades pot utilitzar qualsevol dels poders recollits als articles 62 i 67 de la LQPD, tant els d'investigació com els correctius, com per exemple

"imposar una limitació temporal o definitiva del tractament, inclosa la prohibició".

2.4. Obligats: Qui farà una AI?

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

L'encarregat de tractament, si n'hi ha, ha de donar suport al responsable a l'hora de fer l'AI.

Tal com disposa l'article 32.2 de la LQPD, **el responsable del tractament ha de demanar l'assessorament del delegat de protecció de dades** (DPD), si l'ha designat, en el moment de realitzar l'AI. Aquest assessorament i les decisions que prengui han de quedar documentades a l'AI.

A més, tal com indica l'article 17.4 del Reglament d'aplicació de la LQPD, **el DPD pot suggerir en qualsevol moment la realització d'una avaluació d'impacte** i, en cas de dubte, s'ha de pronunciar sobre si aquesta avaluació és necessària o no ho és.

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.

Tal com s'ha descrit al final de l'apartat 2.3.3, **és recomanable que el responsable del tractament busqui l'opinió dels interessats sobre l'operació de tractament, quan això es consideri apropiat.** Si no es considera apropiat, cal documentar-ne els motius; com per exemple, que la consulta als afectats tingui un cost desproporcionat, sigui impracticable o pugui posar en risc la confidencialitat del pla de negoci.

L'opinió dels interessats es pot recollir de diferents maneres: enquestes, consulta al representant dels treballadors, etc. En qualsevol cas, cal que el responsable del tractament tingui base legal per tractar qualsevol dada personal que es generi en recollir aquestes opinions.

A banda dels actors anteriors, pot ser necessari que hi concorrin tot un seguit d'agents interns o externs a l'organització, com poden ser unitats o àrees específiques, experts independents, responsables de seguretat, etc.

3) El tractament

Per poder determinar de forma acurada quins riscos poden afectar un tractament, cal conèixer amb detall el tractament i el context on es produeix. Així, el responsable de tractament ha de fer-se una sèrie de preguntes per tal de descriure adequadament el tractament que duu a terme. Aquestes preguntes busquen destacar o ajudar a posar en relleu els aspectes problemàtics o els aspectes que poden ser clau per determinar els riscos del tractament.

Pregunta 1. Quin és el tractament de dades? Delimitar l'operació de tractament que s'està considerant i primera descripció.

- Quines operacions de tractament es poden avaluar en una AI? Una AI pot fer referència a una o a múltiples operacions de tractament, si són similars en termes de tipus de dades, abast, context, finalitat i riscos. També és pot fer una AI per avaluar l'impacte que té una aplicació o plataforma de tractament innovadora.

Exemple 1. Implementació d'un programa de recursos humans per gestionar les dades personals dels treballadors (dades de contacte, bancàries, baixes, vacances, etc).

Exemple 2. Implementació d'una aplicació de seguiment a temps real de l'acompanyament del transport escolar (dades identificatives de menors, dades d'ubicació, etc.)

Pregunta 2. Quina és la finalitat del tractament? La finalitat ha de ser explícita, legítima i determinada. L'obligació d'especificar aquesta finalitat de forma prèvia és, per una banda, una garantia dels interessats per tal que entenguin què es farà amb les seves dades; i de l'altra, evita que un cop recollides, les dades es puguin utilitzar per a altres finalitats.

Exemple. El departament de màrqueting d'una empresa vol fer servir les dades de contacte per a l'enviament de publicitat comercial als seus clients. Si en el

moment de la recollida no van ser informats del fet que les dades es podrien fer servir per això, l'empresa no pot tractar-les amb aquesta finalitat sense el consentiment explícit del client.

Pregunta 3. Quin tipus de dades tractaré i quines característiques tenen?

Pregunta especialment rellevant per tal de determinar-ne els riscos.

Característiques a tenir en compte:

- *Font d'obtenció de les dades* → el risc és diferent si les dades s'obtenen directament d'un interessat de si s'obtenen d'un tercer.
- *Termini de conservació* → establir terminis de conservació més llargs que el necessari per dur a terme la finalitat, suposa més risc.
- *Categoria especial de dades* → hi ha dades que per la seva naturalesa, el tractament és inherentment més arriscat. Aquestes dades són de salut, d'origen ètnic o racial, de creences religioses o filosòfiques, d'opinions polítiques, d'afiliacions sindicals, dades genètiques i biomètriques, de vida o d'orientació sexual, etc. Alhora, també són dades de categoria especial les relatives a interessats vulnerables, com ara menors, empleats o grups més vulnerables de la població que necessiten una protecció especial, així com les dades relatives a condemnes i infraccions penals.

Pregunta 4. Quins actors intervenen en el tractament? Tots els agents que tindran accés a les dades o intervindran en algun moment del procés de tractament suposen un potencial risc per a la seva seguretat. El responsable de tractament ha de determinar qui són aquests agents, quin rol juguen, quines funcions i obligacions desenvolupen i quines responsabilitats els són exigibles.

Exemple. En el tractament de dades relatiu a un sorteig hi haurà el grup d'agents encarregats de la recollida de les dades, el grup d'agents encarregats de la realització del sorteig, els encarregats de tractar les dades relatives al guanyador i els encarregats de tractar les dades relatives als no guanyadors.

L'empresa organitzadora haurà d'identificar els actors pertanyents a cadascun d'aquests grups.

Pregunta 5. Quines operacions de tractament es duran a terme? La recollida, l'organització, la conservació, l'elaboració o la modificació, l'extracció, la consulta, la utilització, la comunicació per transmissió, la difusió, o qualsevol altra forma que en faciliti l'accés, la comparació o la interconnexió, el bloqueig, la supressió o la destrucció, etc. són exemples d'operacions de tractament.

- Caldrà, a més a més, determinar-ne el format (manual, automatitzat o mixt) i amb quins mitjans es durà a terme (i qui és el titular d'aquests mitjans).
- El responsable, a més a més, haurà de portar un registre d'operacions de tractament per tal de saber en tot moment quines operacions s'han realitzat sobre les dades i qui les ha dut a terme.

Pregunta 6. On es fa el tractament de les dades? La localització geogràfica del tractament de dades pot suposar un nivell de risc o un altre. D'acord amb les obligacions específiques de les transferències internacionals de dades, el tractament de dades realitzat en països que no ofereixin els mateixos estàndards de protecció que Andorra suposa un risc més elevat.

Exemple. Si una base de dades està allotjada en un servei de hosting dels EUA, aquest tractament de dades s'haurà d'avaluar com a més perillós que si és a França.

4) Principis rectors

Cal avaluar si el tractament descrit a la secció anterior és idoni per assolir la finalitat, si hi ha una alternativa perquè sigui menys lesiu per als drets i les llibertats de les persones i si el benefici que s'obté del tractament és superior als potencials perjudicis que pot tenir sobre les persones.

4.1. Avaluació de la finalitat del tractament

Com s'ha reiterat, les dades han de tractar-se per la finalitat per la qual s'han recollit i qualsevol finalitat alternativa haurà de ser informada i compatible.

- **Informada i consentida** → La nova finalitat haurà de ser comunicada als interessats conforme a les disposicions de l'article 6.3 de la LQPD que hauran de consentir-la expressament per tal que sigui legítima.
    - Excepcions: finalitats relatives a salvaguardar la seguretat de l'Estat, la defensa, la seguretat pública, la prevenció, la investigació, la detecció o l'enjudiciament d'infraccions penals, altres objectius importants d'interès públic general, la protecció de la independència judicial i dels procediments judicials, la prevenció, la investigació, la detecció i l'enjudiciament d'infraccions de normes deontològiques en les professions regulades, les funcions d'inspecció o de reglamentació de l'exercici d'autoritats públiques, la protecció de l'interessat mateix i dels drets o llibertats d'altres, i l'execució de demandes civils (art. 26.1 de la LQPD).
- **Compatible** → Com a norma general, si la nova finalitat és molt diferent de la inicial i no és una finalitat que els interessats puguin preveure, o pot tenir un impacte injustificat sobre les persones, s'ha de considerar incompatible amb la finalitat inicial. Per avaluar si una nova finalitat és compatible amb la finalitat que va motivar la recollida de dades cal tenir en compte els factors següents:

- Qualsevol relació entre les finalitats per les quals s'han recollit les dades personals i les finalitats del tractament posterior previst.
- El context en què s'han recollit les dades personals, en particular respecte de la relació entre els interessats i el responsable del tractament.
- La naturalesa de les dades personals, en especial quan es tracten categories especials de dades personals, o dades relatives a condemnes i infraccions penals.
- Les possibles conseqüències per als interessats del tractament posterior previst.
- L'existència de garanties adequades, que poden incloure el xifrat o la seudonimització.

Alerta! El tractament de dades personals amb finalitat d'arxiu en l'interès públic, amb finalitat d'investigació científica o històrica o amb finalitat estadística es considera compatible amb la finalitat inicial.

4.2. Principi de licitud

D'acord amb la normativa andorrana, perquè un tractament sigui lícit, cal basar-se en algun dels supòsits següents:

- L'interessat ha donat el seu **consentiment** per al tractament de les dades personals, per a una o diverses finalitats específiques. Aquest consentiment haurà de ser lliure, informat, revocable, explícit i recollit correctament.
- El tractament és necessari per executar un **contracte** en què l'interessat en forma part o per aplicar mesures precontractuals.
- El tractament és necessari per complir una **obligació legal aplicable** al responsable del tractament.

- El tractament és necessari per protegir **interessos vitals** de l'interessat o d'una altra persona física.
- El tractament és necessari per complir una missió feta en **interès públic** o en l'exercici de poders públics conferits al responsable del tractament.
- El tractament és necessari per satisfer els **interessos legítims del responsable del tractament o d'un tercer**, sempre que no hi prevalguin els interessos o els drets i les llibertats fonamentals de l'interessat (en particular, quan l'interessat és un menor).

A banda, cal que l'ús de les dades que facin el responsable i l'encarregat del tractament sigui lícit en un sentit ampli. És a dir, que l'ús que el responsable faci de les dades no pot incórrer en cap

Quina base legal és millor?

Depèn del context i la finalitat perseguida, cal escollir la base que encaixi millor amb les circumstàncies del tractament (a més a més, un tractament pot tenir més d'una base legal).

Exemple. Algunes de les bases legals tenen una finalitat específica: un contracte amb l'interessat, una obligació legal, protegir els interessos vitals d'una persona i l'interès públic. Si el tractament es fa amb alguna d'aquestes finalitats, la base legal apropiada és òbvia.

Pel que fa als riscos cal tenir en compte que la base legal afecta el grau de risc. Per exemple, un interès legítim és una base legal vàlida però si és l'única base legal del nostre tractament caldrà que demostrem activament l'existència i previsibilitat per part dels interessats d'aquest interès, en canvi, dona més control als interessats sobre l'ús de les seves dades i, per tant, és menys arriscat.

Alerta! La base legal adequada s'ha d'escollir i informar des del principi, altrament podria generar incertesa i desconcert en els interessats.

Tractament de dades de menors i categories especials de dades:

Els menors necessiten una protecció especial en el tractament de les seves dades personals, perquè poden no ser conscients dels riscos que comporta. En particular, quan el tractament està relacionat amb l'oferta directa de serveis de la societat de la informació a menors i la base legal és el consentiment, la normativa andorrana estableix una edat mínima de 16 anys perquè el consentiment sigui vàlid. Si el menor té menys de 16 anys, cal que el consentiment el doni o l'autoritzi el titular de la pàtria potestat.

Les categories especials de dades són més sensibles i necessiten més protecció. **Quan es tracten aquestes dades, a banda de determinar una base legal per al tractament, cal determinar i justificar quina de les circumstàncies bases legals de l'article 9.2 de la LQPD és la que permet tractar-les**.

Exemple. Una associació sense ànim de lucre de caràcter social pot tenir accés i tractarà dades personals de molts tipus però també tindrà accés a dades relatives a la salut, creences religioses, etc. El tractament d'aquestes dades serà lícit sempre que aquest només afecti les persones amb qui es mantinguin contactes des de l'associació i per a la finalitats que els són pròpies. Se'n prohibirà la comunicació a tercers sense el consentiment dels interessats.

El tractament de les dades sobre condemnes o infraccions penals només està permès sota la supervisió de les autoritats públiques o quan ho autoritzi la normativa específica. A més, s'estableix que els registres exhaustius de condemnes criminals només es poden mantenir sota control de l'autoritat públiques competents (article 10, LQPD) .

4.3. Principi de minimització

Les dades han de ser adequades (suficients per complir amb la finalitat del tractament de forma adequada), **pertinents** (tenen relació amb la finalitat del tractament) **i limitades a l'estrictament necessari per acomplir la finalitat del tractament**. Aquest és un punt clau a l'hora de justificar la necessitat per complir amb la finalitat d'un tractament. S'ha de recollir aquesta informació mínima i cap altra.

Cal revisar de forma periòdica que les dades emmagatzemades continuen essent rellevants i adequades per a la finalitat del tractament, i esborrar qualsevol dada que no ho sigui.

Pel que fa a l'adequació de les dades, cal garantir que siguin útils per assolir la finalitat del tractament. No s'han de tractar dades insuficients o incompletes per a la finalitat pretesa.

4.4. Principi de limitació del termini de conservació

Les dades personals no s'han de conservar més temps de l'estrictament necessari per complir amb la finalitat del tractament. Assegurar-se que s'esborren les dades personals quan deixen de ser necessàries redueix el risc que esdevinguin irrellevants, excessives o inexactes. També convé assegurar-se que l'organització té els procediments necessaris per revisar i fer efectius aquests períodes de retenció.

La normativa no detalla el període concret de temps que s'han de conservar les dades sinó que indica que s'han de conservar de manera que permetin identificar les persones interessades durant un període no superior al necessari per a les finalitats del tractament de dades personals, de manera que cal avaluar periòdicament la necessitat de conservació de les dades. Així, és el responsable del tractament qui ha de fixar-ne el període de retenció, d'acord amb les necessitats del tractament. No s'han de conservar les dades de forma indefinida amb el pretext que podrien ser necessàries en el futur.

- Excepció: Les dades es poden conservar indefinidament amb finalitat d'arxiu en interès públic, amb finalitat d'investigació científica o històrica, o amb finalitat estadística. En aquests casos, cal garantir que s'implanten les mesures tècniques i organitzatives necessàries per garantir el principi de minimització. Tècniques com ara l'anonimització o la seudonimització de les dades tenen una particular rellevància en aquest context.

4.5. Principi d'exactitud

El tractament de dades inexactes pot afectar negativament les persones. **El principi d'exactitud demana que les dades siguin exactes i que es prenguin les mesures adequades per garantir que les que siguin inexactes s'actualitzin o s'esborrin sense dilació**.

4.6. Riscos del tractament

Qualsevol tractament de dades pot tenir efectes negatius sobre els drets i les llibertats de les persones → principi d'enfocament del risc: **les mesures per protegir els drets i les llibertats de les persones han de ser proporcionals al risc associat al tractament.**

La seguretat de la informació és el punt central en les avaluacions de risc. És a dir, normalment s'avaluen els potencials efectes negatius d'una violació de seguretat en el tractament. Ara bé, un tractament pot afectar els drets i les llibertats de les persones, encara que no s'hagi produït cap violació de la seguretat. Per exemple, un tractament pot ser discriminatori en si mateix o pot afavorir l'aparició de pràctiques discriminatòries. Per tant, **l'avaluació del risc se centrarà en els interessats i no tant en el responsable que fa el tractament**.

A l'hora de determinar els efectes que un tractament pot tenir sobre les persones, convé tenir en compte algunes característiques del tractament, com ara:

- El **tipus de dades personals**. El tractament de categories especials de dades, com ara l'origen racial o ètnic, les dades mèdiques o dades sobre les preferències polítiques, són clars indicadors de potencials efectes negatius sobre els drets i les llibertats de les persones. Ara bé, cal remarcar que altres tipus de dades que no formen part de les categories especials també poden tenir un impacte important. Per exemple, localitzacions, informació financera, etc.

- El grau de **sensibilitat** del tractament. Més enllà del tipus de dades tractades, el tipus de tractament també pot indicar potencials impactes. Per exemple, quan el tractament té com a objectiu la monitorització de persones.

- La **quantitat de dades personals** tractades sobre cada individu. Com més gran sigui aquesta quantitat, més gran seran els potencials efectes negatius sobre les persones.

- **L'activitat del responsable del tractament**. Per exemple, si l'activitat del responsable de tractament està relacionada amb la salut o les finances, ja podem entreveure que l'impacte pot ser alt.

- Les **característiques dels interessats**. Si els interessats formen part d'un grup amb necessitats especials (per exemple, menors) cal tenir una cura especial a l'hora de determinar els efectes potencials del tractament.

Impacte i amenaça

Un cop identificats els potencials efectes negatius, cal determinar quin **impacte** tenen. Tal com s'especifica a l'article 17.8 i a l'annex 1 (Taula de valoració del

risc en avaluacions d'impacte) del Reglament d'aplicació, aquest impacte cal avaluar-lo com baix, mitjà, alt o molt alt i serà un càlcul que haurà de fer el responsable de tractament.

Impacte	Descripció
Baix	Els interessats poden patir algunes molèsties menors, que poden reparar-se sense problemes (p. ex. pèrdua de temps).
Mitjà	Risc de patir inconvenients importants reparables (p. ex. augment de costos, impossibilitat d'accedir a algun servei).
Alt	Risc de patir conseqüències importants, reparables però amb moltes dificultats (p. ex. discriminació, robatori de la identitat, pèrdues econòmiques, danys per a la reputació, etc.)
Molt alt	Risc de patir conseqüències greus irreparables (p. ex. danys físics o psicològics greus, mort, etc.)

Una **amenaça és qualsevol circumstància que té el potencial de materialitzar un dels efectes negatius descrits anteriorment**. Un cop determinades les amenaces, cal calcular en quina mesura és probable (n'establirem tres nivells: improbable, possible i probable).

Veurem que per tal de calcular acuradament el nivell de risc associat a un tractament de dades haurem de combinar la gravetat de l'impacte amb la probabilitat de l'amenaça, prenent sempre com a punt de vista i referència els interessats (per exemple, un responsable podria estimar que un impacte alt no és de tanta gravetat com sí que ho podria estimar un interessat). Així, caldrà dur a terme una taula de càlcul en què es ponderarà el risc amb la probabilitat, que en resultarà el següent:

		Impacte			
		Baix	**Mitjà**	**Alt**	**Molt alt**
Probabilitat	**Improbable**	Risc baix	Risc baix	Risc mitjà	Risc alt
	Possible	Risc baix	Risc mitjà	Risc alt	Risc alt
	Probable	Risc mitjà	Risc alt	Risc alt	Risc alt

Llevat que el risc sigui baix, **cal buscar mesures per reduir-lo. Això és especialment necessari en els casos de risc alt o molt alt**. Si no és possible reduir un risc alt, abans de començar el tractament cal consultar l'Agència Andorrana de Protecció de Dades sobre la idoneïtat del tractament. Cal remarcar que en aquest punt no es fa referència a mesures de seguretat o de protecció de les dades, sinó a la protecció *by design*; és a dir, a com està dissenyat el tractament de dades. Per tant, quan es parla de modificacions no es tracta d'implementar més mesures de seguretat, sinó de modificar el disseny del tractament.

Exemples de mesures a prendre per tal de reduir-ne el risc:

- *Evitar la recollida de certs tipus de dades.*
- *Reduir l'abast del tractament.*
- *Formar el personal perquè faci un ús apropiat de la informació.*
- *Anonimitzar o seudonimitzar les dades.*
- *Tenir una política clara de compartició de dades.*

4.7. Necessitat i proporcionalitat del tractament

Un cop avaluats els principis de protecció de dades i analitzats quins són els riscos per als drets i les llibertats de les persones, el responsable té **la informació necessària per avaluar la necessitat i la proporcionalitat del tractament**.

Per justificar que un tractament és necessari, cal mostrar que **no hi ha cap altre tractament que sigui, alhora, efectiu i menys lesiu** per als drets i les llibertats de les persones.

Per justificar que un tractament és proporcional, cal mostrar que **el benefici que s'obté del tractament és superior als perjudicis potencials** sobre les persones. En la justificació de la proporcionalitat, convé tenir en compte l'anàlisi de risc fet a la secció anterior.

RECORDA! Un tractament només té sentit si assoleix la seva finalitat. Per tant, justificar l'eficàcia del tractament és un primer pas essencial per justificar-ne la necessitat.

5) Protecció dels drets de les persones

Els principis fonamentals a què fa referència l'apartat 4 d'aquesta guia es materialitzen en una sèrie de **drets que s'estableixen a la normativa andorrana de protecció de dades: informació i accés a les dades personals, rectificació i supressió, limitació, portabilitat i oposició**.

És essencial garantir que les persones poden exercir els drets que tenen reconeguts a la llei. Així, en l'avaluació d'impacte s'haurà de dedicar un capítol a analitzar i avaluar els mecanismes i procediments implementats en l'entitat per tal de garantir-ne un correcte exercici. Aquesta anàlisi haurà de posar el focus en aspectes com:

- La **transparència** en la informació als interessats.
- Les **comunicacions** amb els interessats han de ser concises, intel·ligibles i de fàcil accés, i que utilitzin un llenguatge clar i senzill. Especialment, quan aquesta comunicació estigui adreçada a menors.
- El **procediment** ha de ser àgil i segur en la recepció de sol·licituds → És recomanable establir un procediment estàndard per fer les sol·licituds. Això facilita les coses tant al responsable com a les persones interessades. Ara bé, les sol·licituds són igualment vàlides encara que no utilitzin aquest procediment.
- **Formació** del personal que rebrà i tramitarà aquestes sol·licituds.
- Tramitació en un **termini** raonable i dins dels límits estipulats a la normativa. La resposta a l'interessat ha de donar-se en el termini d'un mes a comptar des de la recepció de la sol·licitud.

ALERTA! La normativa no especifica com s'han de fer les sol·licituds d'exercici de drets. És a dir, es poden adreçar a qualsevol treballador, per qualsevol mitjà i no necessiten cap formalisme concret. Per aquesta raó, cal assegurar-se que el personal que interacciona amb els interessats té els coneixements suficients per identificar les sol·licituds.

6) Riscos en la seguretat

D'acord amb la normativa, les mesures emprades per protegir la informació **han de ser apropiades al risc per als drets i les llibertats de les persones**. A l'apartat 4 s'han avaluat els riscos associats al tractament, tal com està dissenyat. Aquesta secció busca avaluar els riscos des del punt de vista de la seguretat de la informació.

Partint de la descripció del tractament feta amb anterioritat, **s'avalua quin és l'impacte potencial sobre les persones i quina és la probabilitat que aquest impacte es materialitzi**. Això permet calcular el risc inicial. Si el risc és massa gran, cal aplicar controls (mesures de protecció) per reduir-lo. Aquestes mesures poden buscar reduir la gravetat d'un impacte o la probabilitat que es materialitzi.

Exemple:

- *Seudonimització i encriptació de les dades*
- *Mesures per garantir la confidencialitat, integritat, disponibilitat i la resiliència dels sistemes de tractament i els serveis.*
- *En cas d'incident, mesures per recuperar la disponibilitat i l'accés a les dades personals en un temps adequat.*
- *Un procediment continu de prova i avaluació de l'efectivitat de les mesures proposades per garantir la seguretat del tractament.*

Els tres primers punts fan referència a mesures de protecció. Les mesures del primer punt busquen reduir la probabilitat que l'impacte es materialitzi, mentre que les mesures del tercer punt busquen reduir la severitat de l'impacte. El segon punt és més general i engloba tot tipus de mesures. L'últim punt fa referència al fet que el procés de gestió de risc no és un procés puntual, sinó que s'ha de fer un seguiment dels riscos i de l'efectivitat dels controls.

Pel que fa a la metodologia d'anàlisi de riscos, n'hi ha que tenen un ampli reconeixement, com ara *ISO 27005:2013* o *Magerit*. Ara bé, fer una anàlisi de

riscos emprant aquestes metodologies pot ser un procés complex. Per exemple, amb *Magerit* caldrà:

1. Identificar els actius del sistema (que poden ser: informació, serveis, programari, maquinari, comunicacions, instal·lacions, etc.), especificar la relació de dependència que hi ha entre ells i avaluar-los.
2. Identificar les amenaces rellevants per al sistema i caracteritzar-les segons la probabilitat que es materialitzin i la degradació que causen.
3. Identificar els controls que cal desplegar al sistema i qualificar-ne l'eficàcia enfront de les amenaces identificades prèviament.

Amb l'objectiu de fer l'avaluació de riscos més assequible, aquesta guia proposa un mètode simplificat. Si una organització té la capacitat suficient per abordar alguna de les metodologies d'anàlisi de riscos mencionades anteriorment, convé que ho faci però sense perdre de vista que l'objectiu és avaluar el risc sobre les persones (no sobre l'organització).

Glossari

Activitat principal: Les activitats principals són aquelles que es poden considerar necessàries per aconseguir l'objectiu del responsable o de l'encarregat de tractament.

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.

Categories especials de dades personals: dades personals que revelen l'origen ètnic o racial, les opinions polítiques, les conviccions religioses o filosòfiques o l'afiliació sindical; dades genètiques, dades biomètriques destinades a identificar de manera unívoca una persona física, dades relatives a la salut o dades relatives a la vida sexual o l'orientació sexual d'una persona física.

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.

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.

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

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

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 amb les normes en matèria de protecció de dades que són d'aplicació a les finalitats del tractament.

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 o aritmètiques a aquestes dades.

Transferència internacional de dades: comunicació de dades personals o posar-les 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

Annex 1. Llista de tipus d'operacions de tractament per a les quals es requereix una anàlisi d'impacte en la protecció de dades[1]

Tipus d'operacions de tractament	Criteris de risc	Exemples
Tractaments de dades de salut implementats per establiments sanitaris o establiments medico-socials per a la cura de les persones.	Recollida de dades sensibles. Persones considerades vulnerables.	• *Tractaments implementats per establiments sanitaris:* ◦ *història clínica;* ◦ *ús d'algoritmes per a la presa de decisions mèdiques;* ◦ *vigilància de la salut i sistemes de gestió de riscos;* ◦ *dispositius de telemedicina;* • *Tractaments fets per laboratoris o farmàcies relatius a la salut dels pacients/clients.* • *Tractaments fets per centres d'assistència dels seus residents o beneficiaris (p. ex. dependències, gent gran, etc).*
Tractament de dades genètiques de persones considerades "vulnerables" (pacients, empleats, nens, etc.).	Recollida de dades sensibles. Persones considerades vulnerables.	• *Investigacions mèdiques sobre pacients amb el tractament de les seves dades genètiques.* • *Tractament utilitzat per a la gestió d'una consulta genètica en un establiment sanitari.*
Tractaments de dades destinats a la creació de perfils de persones físiques a efectes de gestió de recursos humans.	Avaluació o qualificació de persones a través de perfils. Persones considerades vulnerables.	• *Tractament dirigit a facilitar la contractació, sobretot gràcies a un algoritme de selecció.* • *Tractament dirigit a oferir accions de formació personalitzades mitjançant un algoritme.* • *Tractament dirigit a detectar i prevenir les sortides dels empleats a partir de correlacions establertes entre diversos factors.*
Tractament dirigit a controlar constantment l'activitat dels empleats afectats	Persones considerades vulnerables. Vigilància	• *Sistema de ciberseguretat com els que realitzen una anàlisi dels fluxos de correu electrònic sortints per tal de detectar possibles fuites d'informació (els*

1 Aquesta llista no és exhaustiva. En cas de dubtar si una operació de tractament pot comportar l'obligació de realitzar una AI podeu fer ús de l'eina de consulta prèvia prevista a l'article 33 de la LQPD o posar-vos en contacte amb l'APDA.

	sistemàtica.	*anomenats sistemes de prevenció de pèrdues de dades).* • *Videovigilància dels empleats que manipulen diners en efectiu.* • *Videovigilància d'un magatzem on s'emmagatzemen mercaderies valuoses amb què treballen els manipuladors.* • *Geolocalització per a vehicles de transport per carretera.*
Tractament amb la finalitat de gestionar alertes i informes en matèria social i sanitària	Recollida de dades sensibles. Avaluació o qualificació de persones a través de perfils. Persones considerades vulnerables.	• *Sistema d'alerta de menors en perill.* • *Tractament utilitzat per una agència sanitària per gestionar una crisi sanitària o una alerta sanitària.* • *Sistema per denunciar situacions de maltractament de persones vulnerables (gent gran, persones amb discapacitat, etc.).*
Tractament amb la finalitat de gestionar alertes i informes en matèria professional	Recollida de dades sensibles. Avaluació o qualificació de persones a través de perfils. Persones considerades vulnerables.	• *Sistema de recollida d'alertes professionals per a les entitats privades o públiques interessades.* • *Sistema de recollida d'informes sobre actes de tràfic d'influències o corrupció comesos a l'organització.* • *Sistema d'alerta implementat com a part del deure de vigilància.*
Tractament de dades sanitàries necessàries per a la creació d'un registre de dades	Recollida de dades sensibles. Persones considerades vulnerables.	• *Bases de dades creades per establiments sanitaris amb finalitats de recerca.*
Tractaments que impliquen la creació de perfils de persones els quals poden resultar en conseqüències negatives per als interessats (exclusió de beneficis, suspensió o resolució de contractes, etc).	Avaluació o qualificació de persones a través de perfils. Encreuament de dades	• *Procediments que atorguen una puntuació per a la concessió de crèdit.* • *Tractament basat en anàlisis de comportament dirigits a detectar comportaments "prohibits" a una xarxa social.* • *Procediments destinats a la lluita contra el frau i blanqueig de capitals.*

Tramitació agrupada d'incompliments contractuals observats, que poden conduir a la decisió d'excloure o suspendre el benefici d'un contracte.	Encreuament de dades Presa de decisions automatitzades amb efectes jurídics o similars significatius.	• *Tractament d'identificacions de deutes impagats i subscripcions irregulars compartides per un sector d'activitat.* • *Tractament de dades de propietaris d'automòbils que permet a les companyies asseguradores comprovar els antecedents d'un futur assegurat en sol·licitar un contracte d'assegurança d'automòbil.*
Tractament de perfils mitjançant dades de fonts externes.	Avaluació o qualificació de persones a través de perfils. Encreuament de dades Ús de tecnologies de nova creació Recollida de dades sensibles.	• *Compartició de dades entre data brokers.* • *Tractaments destinats a publicitat dirigida.*
Tractament de dades biomètriques amb la finalitat d'identificar de manera única una persona física, incloses les persones anomenades "vulnerables" (alumnes, gent gran, pacients,etc.)	Recollida de dades sensibles. Persones considerades vulnerables.	• *Tractaments de dades basats en el reconeixement dactilar amb la finalitat de controlar la identitat de l'afectat.* • *Control d'accés a recintes escolars, centres d'assistència, etc.*
Examen de sol·licituds i gestió d'habitatge social.	Recollida de dades sensibles Avaluació o qualificació de persones a través de perfils.	• *Tractament destinat a la gestió i el tràmit de demandes d'habitatge social.*
Tractaments destinats a proporcionar suport social o medicosocial a les persones.	Recollida de dades sensibles Avaluació o qualificació de persones a través de perfils. Persones	• *Tractament implementat per un establiment o una associació en el marc de l'atenció a les persones en la seva integració o reinserció social i professional.* • *Tractament implementat per residències per a persones amb discapacitat com a part de l'acollida, l'allotjament, el suport*

	considerades vulnerables.	*i el seguiment d'aquestes persones.* • *Tractament implementat per un centre d'acció social com a part del seguiment de persones amb patologies cròniques en situació de fragilitat social.*

Annex 2. Llista de tipus d'operacions de processament per a les quals no es requereix una anàlisi d'impacte en la protecció de dades [2]

Tipus d'operacions de tractament	Exemples
Tractament, implementat únicament amb finalitats de recursos humans i en les condicions previstes pels textos aplicables, per a la gestió exclusiva del personal de les organitzacions que donen feina a menys de 250 persones, amb l'excepció de l'ús de perfils.	Tractaments que permeten: • Gestió de nòmines, emissió de fulls de pagament. • Gestió de la formació. • Gestió del restaurant de l'empresa, emissió de vals de dietes. • Reemborsament de despeses professionals. • Seguiment de les entrevistes d'avaluació anuals. • Manteniment de registres obligatoris. • L'ús d'eines de comunicació (missatgeria electrònica, telefonia, videoconferències, eines de col·laboració en línia). • Control del temps de treball (sense dispositiu biomètric, sense dades sensibles o altament personals).
Tractaments de gestió de relacions amb proveïdors.	Tractaments que permeten: • realitzar operacions administratives relacionades amb contractes, controls, recepcions, factures, normatives, comptabilitat de la gestió de comptes a pagar; • establir documents de pagament (esborranys, xecs, pagarés, etc.); • establir estadístiques financeres i de facturació per proveïdor; • proporcionar seleccions de proveïdors per a les necessitats de l'empresa o de l'organització; • mantenir documentació sobre proveïdors.
Tractaments de dades implementats en les condicions regulades a les normes relatives a la gestió del cens electoral dels comuns.	Tractaments que permeten: • gestionar les sol·licituds d'inscripció a les llistes electorals que es presenten o s'envien als municipis i continuar amb la instrucció; • instruir i retirar de la llista electoral els votants que ja no compleixin les condicions per a la inclusió; • gestionar les sol·licituds de comunicació i còpies de la llista electoral.
Tractaments destinats a la	Tractaments que permeten:

2 La implementació d'un tractament que aparegui en aquesta llista no eximeix el responsable del compliment de la resta d'obligacions de la normativa andorrana de protecció de dades. Alhora, tampoc l'eximeix de l'anàlisi més preliminar sobre la pertinença o no de fer una AI analitzant les particularitats del seu cas (en cas de dubte, podeu contactar amb l'APDA). El tractament, fins i tot exempt d'anàlisis d'impacte, ha d'estar subjecte a una avaluació del seu compliment amb la normativa de protecció de dades, tant legalment com en termes de seguretat.

gestió de les activitats dels comitès d'empresa i d'establiments.	• gestionar els programes socioculturals de l'empresa, la comunicació interna; • formació dels càrrecs electes; • gestió d'agendes i reunions; • gestió dels membres.
Tractament implementat per una associació, una fundació o qualsevol altra institució sense ànim de lucre per a la gestió dels membres i donants com a part de les activitats habituals sempre que les dades no siguin sensibles.	Tractaments que permeten: • la gestió administrativa dels socis i donants, en particular la gestió de les quotes dels socis; • establir, per satisfer les necessitats de gestió, informes estadístics o llistes de membres o contactes; en particular amb l'objectiu d'enviar butlletins, invitacions, diaris. (els criteris seleccionats han de ser objectius i basats només en característiques que corresponguin a la finalitat legal de l'organització); • establir directoris de membres, fins i tot quan aquests directoris es posen a disposició del públic o a Internet; • realitzar per qualsevol mitjà d'operacions de comunicació relacionades amb accions de prospecció amb membres, donants i prospectes.
Tractament de les dades sanitàries necessàries per a l'atenció d'un pacient per part d'un professional de la salut que treballa de forma individualitzada en una consulta mèdica, un dispensari de farmàcia o un laboratori de biologia mèdica.	Tractaments que permeten: • gestió de cites; • gestionar i guardar els registres necessaris per al seguiment del pacient; • comunicacions entre professionals identificats implicats en l'atenció de la persona interessada; • comptabilitat.
Tractaments implementats per advocats en l'exercici de la seva professió de manera individual.	Tractament de la gestió de clients, inclosos els que contenen dades sensibles que poden afectar persones vulnerables (p. ex. menors).
Tractaments implementats pels secretaris judicials mercantils amb la finalitat de desenvolupar la seva activitat.	Tractament dirigit a controlar la legalitat dels actes, mantenint els diversos registres i directoris legals.
Tractament implementat pels notaris amb la finalitat de desenvolupar la seva activitat notarial i redacció de documents per a oficines notarials.	Tractament amb la finalitat de: • l'enviament desmaterialitzat de còpies i extractes de documents d'estat civil, com a part de la tramitació de la gestió de l'estat civil dels serveis competents dels municipis i la del Ministeri d'Afers Exteriors; • mantenir en nom dels clients documents justificatius de les seves sol·licituds de deduccions dels ingressos globals, reduccions o crèdits fiscals, com a part de la seva missió com

	a tercers de confiança, tal com preveu el codi tributari general.
Tractament implementat per les ens locals i les persones jurídiques regides pel dret públic i privat amb la finalitat de gestionar serveis en matèria d'assumptes escolars, extraescolars i de primera infància.	Aquesta exempció s'aplica al tractament relacionat amb: • preinscripció, registre, seguiment i facturació de serveis en matèria d'assumptes escolars, extraescolars i d'educació infantil (escolarització a escoles bressol i primària); • el cens de nens subjectes a educació obligatòria; • restauració escolar i extraescolar; transport escolar; • activitats de benvinguda i extraescolars; acollida col·lectiva de menors; • participació en l'organització material i financera de sortides escolars, estades escolars curtes i classes de descoberta a l'educació primària; • atenció a la primera infància en establiments i serveis per a menors de sis anys.
Processament implementat amb l'únic propòsit de gestionar els controls d'accés físic i els horaris per calcular el temps de treball, fora de qualsevol dispositiu biomètric; excloent el processament de dades que reveli dades sensibles o altament personals.	Tractaments amb la finalitat de : • la implementació d'un dispositiu d'insígnia sense dades biomètriques per entrar a les instal·lacions d'una organització per motius de seguretat; • l'establiment d'un sistema de control del temps de treball realitzat pels empleats, amb exclusió de qualsevol altra finalitat.
Tractaments relatius a les proves d'alcoholèmia, emmarcats estrictament per un text i implementats en el context de les activitats de transport amb l'únic propòsit d'evitar que els conductors condueixin un vehicle sota la influència de l'alcohol o les drogues.	Els tractaments amb la finalitat d'instal·lar l'alcoholèmia "immobilitzador" en camions de transport.

Annex 3. Proposta de càlcul orientatiu per a determinar tractaments a gran escala.

Alerta! ***El resultat del càlcul és una eina d'anàlisi orientativa per al responsable i no determina l'obligació de tenir un DPD o no.***

Criteri	Requisit	Puntuació
El nombre d'interessats afectats com a xifra concreta.	De 0 a 500	(1)
	De 501 a 1.000	(2)
	De 1.001 a 5.000	(3)
	+ de 5.000	(4)
Les categories de dades tractades: 1. Categories especials de dades. 2. Dades de caràcter identificatiu. 3. Característiques personals. 4. Circumstàncies socials. 5. Dades acadèmiques i professionals. 6. Detalls de l'ocupació 7. Dades econòmiques, financeres i d'assegurança. 8. Transaccions de béns i serveis.	Només s'aplica a 1 categoria de dades	(1)
	S'aplica d'entre 1 a 4 categories de dades	(2)
	S'aplica d'entre 5 a 8 categories de dades	(3)
La durada o conservació de l'activitat de tractament de dades.	Instantani	(1)
	Dies	(2)
	Mesos	(3)
	Anys / indefinit	(4)
L'abast geogràfic de l'activitat de tractament.	Tractament en àmbit parroquial	(1)
	Nacional	(2)
	Internacional	(3)

Un cop hem posat xifres als aspectes a analitzar per determinar si un tractament és a gran escala, hem d'establir fórmules de càlcul.

Per això, assignem números creixents a cada barem i, sabent que la sumatòria màxima dels quatre aspectes és 14, podem establir, orientativament, que un tractament és de gran escala quan la sumatòria sigui igual o superior a 9.

Vegem-ne un exemple per entendre aquest sistema de càlcul.

- El nombre d'interessats afectats és de 700 persones (2)

- Les categories de dades tractades són dades de caràcter identificatiu, dades acadèmiques i professionals, detalls de l'ocupació i dades econòmiques (2)
- El tractament serà d'anys
- El tractament tindrà una extensió geogràfica internacional (3)

La suma és d'11, per tant, es considera que el tractament és a gran escala.

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