MEMÒRIA ANUAL EXPLICATIVA:

2020

ÍNDEX DE CONTINGUTS

PRESENTACIÓ:

Ens complau un any més presentar la Memòria anual de l'Agència Andorrana de protecció de Dades, que recull les activitats realitzades per aquesta institució durant el 2020 en totes les seves àrees; a més a més d'una anàlisi de les tendències més rellevants, d'una exposició i valoració dels reptes presents i futurs i d'una avaluació de les iniciatives posades en marxa durant l'any.

L'Agència busca ser una institució propera i accessible a la ciutadania i a la resta de les administracions públiques, posant a la seva disposició diferents canals de comunicació a través dels quals es pot sol·licitar informació, criteri jurídic o tecnològic en totes les qüestions en què pugui veure's afectat el dret fonamental a la protecció de dades de caràcter personal; parant especial atenció al fet que el tractament de dades personals continua influenciat pel desenvolupament dinàmic de les tecnologies de la informació i les telecomunicacions en l'economia mundial connectada i, que el mateix, té un impacte major en la vida quotidiana de la població en la feina, en el consum i en el lleure.

La Memòria que em complau presentar exposa les activitats més rellevants dutes a terme per l'Agència de Protecció de Dades en 2020, un any atípic per a tots on aquest organisme no sols ha hagut d'enfrontar-se a nombrosos reptes relacionats amb el dret fonamental del qual és garant sinó que ha hagut de fer-lo a l'entorn de la pandèmia derivada de la COVID-19.

Organitzar l'Agència amb el teletreball, ha permès que l'Agència hagi estat en unes condicions òptimes per a continuar treballant en la situació extrema que hem viscut enguany i que requeria conciliar la salut del personal amb les seves obligacions laborals.

Un dels reptes principals de 2020 ha estat establir criteris i conciliar la garantia de l'assistència sanitària i el control de la pandèmia amb el dret fonamental a la protecció de dades personals. I ha estat un dels reptes perquè, en paral·lel, l'Agència ha hagut de continuar treballant en la resolució de les reclamacions plantejades pels ciutadans, en les consultes plantejades per les empreses i les administracions, atenent els dubtes i consultes tant dels ciutadans com dels subjectes obligats, publicant materials o llançant iniciatives de diversa índole per a fomentar la privacitat. Tot això sense oblidar la necessària pedagogia d'entendre la protecció de dades com un element de competitivitat que redunda en benefici tant de les pròpies organitzacions com de les persones les dades de les quals es tracten. La participació de l'Agència en la Comissió de la Videovigilància, i en la Comissió d'Estadística, han estat necessàries per adaptar els tractaments de les dades personals a les disposicions d'aquest dret fonamental.

La principal fita de 2020 per a l'Agència estat donar resposta des de la perspectiva de protecció de dades a la situació generada per la pandèmia de la COVID-19 en una doble dimensió.

La conciliació de les mesures a adoptar per a garantir l'assistència sanitària i el control de la pandèmia amb el dret fonamental a la protecció de dades personals, en col·laboració amb el Ministeri de Sanitat com a principal autoritat competent per a l'adopció de mesures en relació amb aquesta finalitat. L'adopció de mesures de caràcter organitzatiu que permetessin mantenir el nivell d'activitat de l'Agència en les circumstàncies que ha exigit la COVID-19, de manera que no pogués ressentir-se el sistema de garanties per als ciutadans establert en la Llei.

L'Agència ha desenvolupat una àmplia activitat de difusió d'informacions i documents en relació amb la COVID-19, dirigits tant a ciutadans com als responsables del tractament de les dades. I ha creat una secció específica en la seva web anomenada «Covid 19» que inclou nombrosos documents que es recullen de manera detallada en altres apartats d'aquesta Memòria.

Una qüestió de cabdal importància ha estat la presentació a tràmit parlamentari del text que modernitza la Llei de protecció de dades personals alineant-la amb el Reglament de protecció de dades europeu, així com la resposta als qüestionaris tramesos per la DG de Justícia i Llibertat de la Unió Europea, en el tràmit de revisió de l'adequació del Principat d'Andorra.

Finalment, vull recordar al lector que aquesta Memòria no pretén ser exhaustiva, sinó que busca posar en unes línies les tendències, els fets més destacats, les inquietuds, i les esperances també d'aquesta agència, recordant que l'equip de professionals de la mateixa sempre està disponible per tal d'aportar les precisions que siguin necessàries: equip de persones al que vull expressar el meu reconeixement, doncs el seu talent i esforç ha contribuït al bon funcionament i al repte de mantenir un ritme intens de treball; un repte que han assumit, amb gran professionalitat i que hem gestionat amb fermesa i dedicació.

Joan CRESPO i PIEDRA
Cap de l'Agència andorrana de Protecció de Dades

L'Agència andorrana de protecció de dades

QUÈ ÉS I COM FUNCIONA?
ELS RECURSOS HUMANS DE L'AGÈNCIA.
FUNCIÓ CONSULTIVA.
FUNCIÓ DE CONTROL.
DRETS PERSONALÍSSIMS.
REGISTRE PÚBLIC D'INSCRIPCIÓ DE FITXERS.
PLANA WEB.

L'AGÈNCIA ANDORRANA PROTECCIÓ DE DADES

→ Què és i com funciona?

L'Agència Andorrana de Protecció de Dades és l'**organisme independent** que té per objecte garantir els drets a la protecció de les dades personals i d'accés a la informació que hi està vinculada. Així s'estableix en l'article 38 de la Llei 15/2003, del 18 de desembre, qualificada de protecció de dades personals.

El mateix article qualifica l'Agència Andorrana de Protecció de Dades com una **institució de dret públic, amb personalitat jurídica pròpia i plena capacitat d'obrar** per al compliment dels seus fins, amb plena autonomia orgànica i funcional, que actua amb objectivitat i plena independència de les administracions públiques en l'exercici de les seves funcions i es relaciona amb el Govern per mitjà del departament que es determina per reglament.

Així doncs, l'Agència Andorrana de Protecció de Dades és una institució independent que **vetlla perquè les dades personals dels ciutadans siguin tractades, tant per part de les organitzacions privades com de les administracions públiques, garantint el dret fonamental a la protecció de les dades personals**.

FUNCIONS

1. Tramitar els expedients d'inscripció, modificació i supressió de **fitxers** de dades personals de naturalesa privada

2. Difusió de **bones pràctiques** en el tractament de les dades personals.

3. Informar a les persones físiques sobre els seus **drets** i procedir a la tramitació dels **expedients** administratius quan aquests drets no són atesos

4. Desenvolupar projectes d'**adaptació i canvis d'hàbits** en el tractament de les dades personals tant per a entitats de caràcter privat com per a les administracions públiques.

5. **Assessorar** a les entitats privades i a les administracions públiques en el tractament de les dades personals.

6. **Formar** els responsables del tractament en tots els procediments d'adaptació a la Llei 15/2003, del 18 de desembre, qualificada de protecció de dades personals

7. Instruir els **expedients administratius** d'infracció comesos per entitats de naturalesa privada i pública.

8. Organitzar **conferències** i **xerrades** formatives adreçades als ciutadans i a les escoles

POTESTATS:

Art. 40 de la Llei 15/2003, de 18 de desembre, qualificada de protecció de dades personals.

a) Vetllar pel compliment d'aquesta Llei.

b) Gestionar el Registre Públic d'Inscripció de Fitxers de Dades Personals.

c) Publicar anualment la llista de països amb protecció equivalent, conforme al que estableix l'article 36 d'aquesta Llei.

d) Exercir la potestat inspectora i de sanció per a les infraccions que es tipifiquen en el capítol cinquè d'aquesta Llei.

e) Proposar les millores en la normativa de protecció de dades personals que consideri convenients.

RECURSOS HUMANS DE L'AGÈNCIA:

Cap de l'Agència

Designat pel Consell General (per majoria qualificada en primera votació, o per majoria absoluta en una segona volta) per un període de quatre anys. Aquest nomenament es pot renovar al final de cada període.

2 inspectors

Designats amb el mateix procediment, majories i durada que el Cap de l'Agència.

Administració i suport

Personal de l'Agència

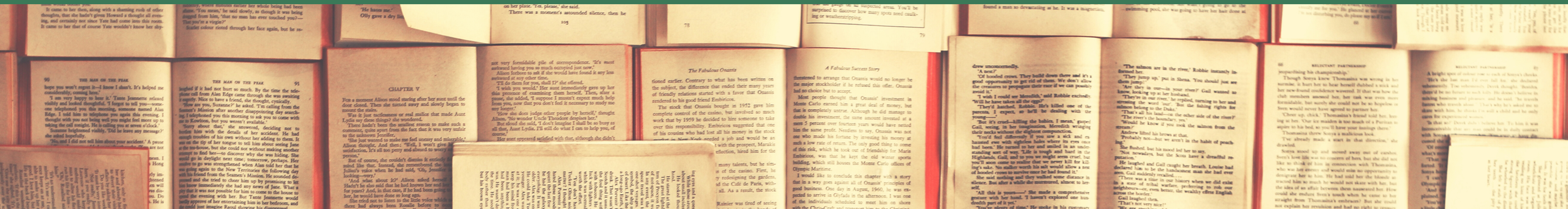
FUNCIÓ CONSULTIVA:

En l'exercici de la seva funció consultiva, l'Agència Andorrana de Protecció de Dades **atén les consultes que li formulen les persones físiques o jurídiques, així com les entitats i administracions públiques, respecte a tractaments de dades incloses en el seu àmbit d'aplicació.**

Al llarg d'aquest 2020, s'han formulat un total de **2.116 consultes** a l'Agència Andorrana de Protecció de Dades, que suposa un gran increment respecte a la xifra registrada l'any anterior (1.763). La principal via de recepció de les consultes ha estat per correu electrònic (57%), tot i que les consultes telefòniques s'han mantingut a un nivell similar (41%) que en l'exercici de 2019. Les visites presencials però, i de forma lògica tenint en comptel context de pandèmia, han sofert una caiguda en picat i només representen un 2,7% de les consultes rebudes. **La majoria de les consultes han estat formulades majoritàriament en l'àmbit privat**, mentre que les provinents de les administracions públiques han estat 508.

A partir de les consultes s'han redactat **177 informes** (65.5% més que el 2019) dels quals **43** han estat dirigits a administracions públiques.

S'entén per informe **la resposta escrita a les consultes sobre una qüestió concreta en relació amb la protecció de dades de caràcter personal.** Aquests han tractat diverses temàtiques: tràmits de declaració de fitxers, l'afectació de la COVID-19 en l'àmbit públic, privat i laboral, ús d'imatges de menors, les transferències internacionals de dades, propostes de modificacions de llei amb afectació a protecció de dades, l'aplicació del RGPD a Andorra o com exercir els drets d'accés, de supressió, de cancel·lació i d'oposició, entre d'altres.



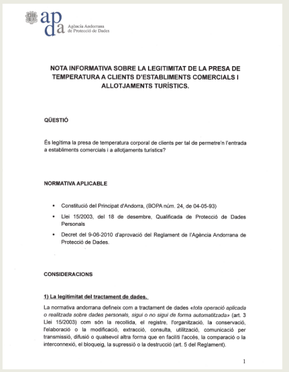
FUNCIÓ CONSULTIVA: COVID-19

Arran de la crisi de la COVID-19 l'agència va haver de donar resposta a diverses qüestions plantejades tant per particulars com per les administracions públiques.

Algunes de les qüestions a les quals es donà resposta foren la **cessió de dades en el marc de la lluita contra la pandèmia a autoritats sanitàries, les mesures de seguretat adients per als treballadors en el context del teletreball, la idoneïtat d'instal·lar sistemes de control d'accés a establiments comercials i d'allotjament turístic basats en la presa de temperatura als clients,... etc.**

En aquests casos, a part de contestar les consultes, l'APDA va publicar **guies formatives o infogràfics** al respecte.

Cal destacar també que aquesta Agència analitzà una **Avaluació d'Impacte** relativa al desenvolupament d'una app de rastreig de contactes de COVID-19, on es ponderava la seva proporcionalitat respecte a la finalitat perseguida.

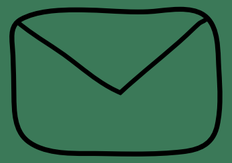


LA FUNCIÓ CONSULTIVA EN XIFRES:

Naturalesa de les consultes rebudes

→ **Orals**
41,3% (867 consultes)

→ **Presencials**
2,7 % (42 consultes)



→ **Correu electrònic**
57% (1207 consultes)

Origen de les consultes rebudes

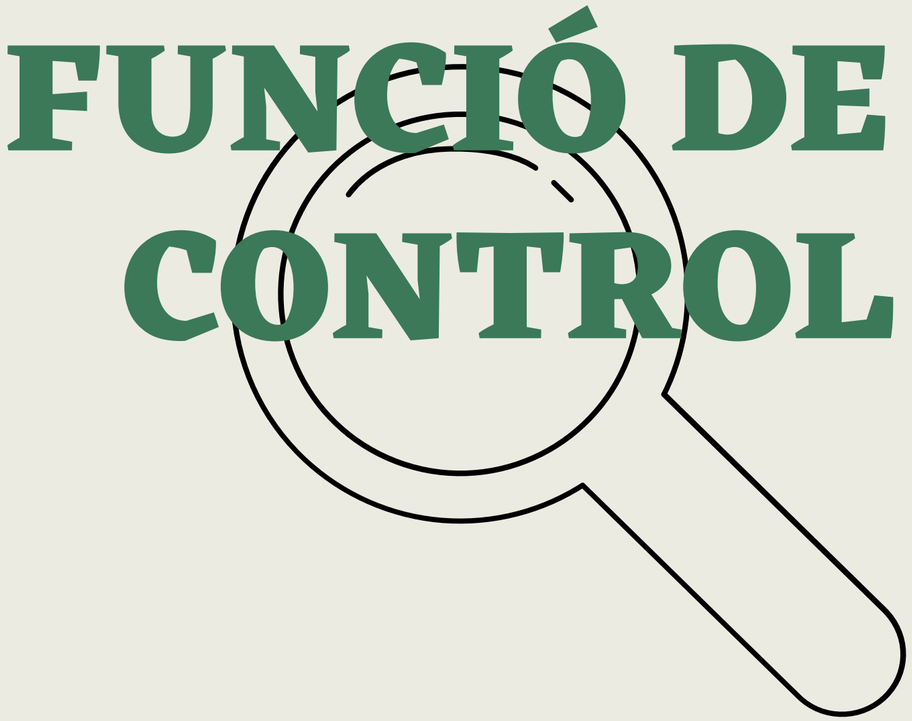
→ **Sector privat**
76% (1608 consultes)

→ **Sector públic**
24% (508 consultes)

⟶ *Art. 41 de la Llei 15/2003, de 18 de desembre, qualificada de protecció de dades personals*

Per complir amb la seva funció de control, l'Agència Andorrana de Protecció de Dades té atribuïda la potestat d'inspecció. Així, es duen a terme una sèrie d'actuacions per verificar el compliment de la normativa per part dels responsables de fitxers de dades personals.

- Es poden examinar els equips físics i lògics utilitzats per al tractament de les dades, i alhora accedir als locals on estiguin instal·lats.
- Les inspeccions poden ser d'ofici o bé com a conseqüència d'una denúncia.
- Es pot requerir la documentació que es consideri necessària o també es poden fer inspeccions de manera presencial, en cas que la documentació aportada es consideri insuficient, al lloc on es tracten les dades, o bé on presumptament s'hagin produït els fets objecte d'investigació.



Funció de control

L'Agència té l'obligació d'iniciar els **procediments d'investigació de totes les denúncies presentades** per qualsevol persona interessada i incoar els expedients administratius en cas que es consideri vulnerat el dret fonamental a la protecció de dades personals.

En els expedients administratius incoats aquest any, l'Agència ha analitzat possibles vulneracions per ús i apropiació de dades personals, la difusió de les mateixes a través de xarxes socials, la tutela de drets personalíssims de protecció de dades, o l'accés i la divulgació de dades sensibles o la recollida excessiva de dades, entre d'altres qüestions.

En l'exercici de la seva funció de control, l'Agència, d'acord amb els procediments previstos al Codi de l'Administració:

- declara l'**existència o no d'infraccions,**
- insta als responsables i als prestadors de serveis a què **adeqüin el tractament de dades a la legislació vigent** i,
- si escau, exerceix la **potestat sancionadora** amb els expedients administratius corresponents.

Així es vetlla pel **correcte compliment de la legislació sobre protecció de dades i es controla l'aplicació dels drets** d'informació, accés, rectificació, supressió i oposició.

Durant l'any 2020, l'Agència ha tramitat

19

expedients administratius.

DRETS PERSONALÍSSIMS

Les causes i els supòsits de denegació d'aquests drets són exclusivament les disposades per llei. Totes les denegacions es poden recórrer davant l'Agència andorrana de Protecció de Dades que avaluarà la possible infracció i en tramitarà l'expedient administratiu de conformitat als procediments d'inspecció i sanció.

DRET D'ACCÉS

Interessats

Dret a ser informat de l'existència de fitxers que continguin dades sobre un mateix i la seva finalitat.

Responsables

5 dies hàbils desde la solicitud escrita per contestar de forma CLARA i INTEL·LIGIBLE.

DRET DE RECTIFICACIÓ

Interessats

Dret a que es corregeixin les dades quan aquestes no es corresponguin amb la realitat.

Responsables

1 mes per a modificar les dades. Si les mateixes s'han comunicat a un tercer, aquest també haurà de corregir-les.

DRET D'OPOSICIÓ

Interessats

Dret a que les dades no es comuniquin a un tercer.

Responsables

15 dies per comunicar la recepció de les dades a l'interessat. Aquest disposa d'un mes per oposar-se a la transferència.

DRET DE SUPRESSIÓ

Interessats

Dret a deixar de constrar en un fitxer de dades.

Responsables

1 mes per respondre. Si s'accepta les dades queden bloquejades i només a disposició de les administracions i els tribunals fins que prescriguin.

PLANA WEB:

La plana web de l'Agència (www.apda.ad) és un excel·lent **mitjà de consulta i d'informació en referència a la protecció de dades personals**, tant per donar resposta a les preguntes que es plantegen els ciutadans com a aquelles que es formulen els responsables del tractament de dades personals.

Dins de la plana web, també tenim el Portal Jove, apartat destinat a facilitar tot tipus d'informació i consells pràctics a joves, pares i educadors. És una prioritat de l'Agència andorrana de protecció de dades **conscienciar als joves sobre la necessitat de protegir les pròpies dades personals al tractar-se d'un dels col·lectius que més risc presenten de veure vulnerats els seus drets**.

Els documents més descarregats de la nostra plana web han estat:

- *Manual de bon ús del correu electrònic: guia per a les persones treballadores per a la protecció de la privacitat en l'ús del correu electrònic.*
- *Recomanacions sobre tractaments de dades en la crisi de la COVID-19.*
- *Pour un usage raisonné des réseaux sociaux en milieu scolaire.*
- *Dictamen 4/2012 sobre la exención del requisito de consentimiento de cookies.*
- *Dictamen 5/2009 sobre las redes sociales en línea.*
- *Llei 15/2003, del 18 de desembre, qualificada de protecció de dades personals.*
- *Recomanació Teletreball.*
- *Nota informativa sobre la legitimitat de la presa de temperatura a clients d'establiments comercials i allotjaments turístics.*

72.942 visites

46.816 descàrregues

REGISTRE PÚBLIC D'INSCRIPCIÓ DE FITXERS:

El Registre Públic d'Inscripció de Fitxers és un òrgan, que depèn de l'Agència Andorrana de Protecció de Dades, la missió del qual és **vetllar per la publicitat de l'existència dels fitxers de dades de caràcter personal i dels tractaments de dades** per permetre que qualsevol persona pugui conèixer l'existència d'un determinat tractament de les seves dades personals, la finalitat i la identitat del responsable del fitxer, per així fer possible l'exercici dels ciutadans dels drets d'accés, rectificació, oposició i cancel·lació regulats per la Llei 15/2003. És per això que **tots els fitxers de dades personals s'hi han d'inscriure.**

El responsable del fitxer ha de declarar el fitxer mitjançant una notificació i els inspectors de l'Agència revisen que es compleixin els requisits establerts per la Llei, proposant al cap de l'Agència acceptar o rebutjar la inscripció. Malgrat això, la inscripció d'un **fitxer té caràcter declaratiu** i no prejutja que s'hagin satisfet tots els requisits exigits per la Llei 15/2003, del 18 de desembre, qualificada de protecció de dades.

Tots els tràmits de registre són **gratuïts** i el Registre d'Inscripció de Fitxers de dades personals és d'**accés públic, general i gratuït**, i es pot consultar a través de la plana web de l'Agència www.apda.ad.

Els organismes públics i les administracions **no han de declarar els fitxers a l'Agència, sinó que la regulació d'aquests fitxers es preveu mitjançant la publicació al Butlletí Oficial del Principat d'Andorra**.

A 31 de desembre del 2020, constaven inscrits un total de **4.765 fitxers** dels quals **283** suposen noves inscripcions de l'any 2020. Durant aquest s'han produït **413 tràmits** davant aquest òrgan, fet que suposa una disminució del **47,52%** respecte a l'any anterior. **Aquesta davallada es deu a la disminució de tràmits durant el confinament.**

Durant l'any 2020 s'ha pogut apreciar un augment notable en la xifra de fitxers de dades personals de naturalesa privada i pública que contenen **dades sensibles**, com lògicament en allò relatiu a la **salut**, però també dades relatives a les **opinions polítiques o la pertinença a organitzacions sindicals**.

Durant l'any 2020, l'Agència ha tramitat

413 **sol·licituts de les quals:**

- **283 inscripcions**
- **50 modificacions**
- **10 supressions**
- **5 retirades**
- **55 pendents**

Difusió dels principis de protecció de dades

DIA DE LA PROTECCIÓ DE DADES 2020.
L'AGÈNCIA ALS MITJANS.
ACCIÓ FORMATIVA I DIVULGACIÓ.

Un dels principals objectius de l'Agència és difondre i sensibilitzar sobre els drets i els deures relacionats amb les dades de caràcter personal. Amb aquesta finalitat, s'organitzen conferències, es publiquen guies de bones praxis i es realitzen reunions formatives amb els responsables de fitxers de dades, entre altres activitats.

Dia de protecció de dades

Durant el DIA EUROPEU DE LA PROTECCIÓ DE DADES 2020, aquesta agència va publicar "*Biometria: afectació en matèria de protecció de dades*", una guia informativa que busca descriure i determinar l'afectació als drets fonamentals que tenen les tècniques i les tecnologies biomètriques.

Durant els darrers anys hem vist com tant empreses privades com les administracions públiques han optat per la instal·lació de sistemes de recollida i tractament de dades biomètriques i alhora, com aquestes s'han anat fent lloc en l'àmbit privat a través de dispositius mòbils i formes d'interactuar amb el nostre entorn.

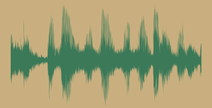
La recollida i el tractament de dades biomètriques suposen un risc molt elevat de produir danys irreparables en la privacitat dels interessats així que aquesta Agència recomanà la seva limitació a aquells supòsits on quedés provada la seva necessitat, proporcionalitat i efectivitat.

L'AGÈNCIA ALS MITJANS:

A l'hora de difondre els principis de protecció de dades, els mitjans de comunicació suposen un excel·lent aliat. Aquesta és la raó per la que l'Agència procura mantenir una bona relació i sempre està disposada a col·laborar amb aquests. Durant l'any 2020 l'Agència ha participat:

→ **Televisió**

4 intervencions



→ **Ràdio**

3 intervencions

abc → **Premsa**

28 intervencions

Temes tractats:

Biometria, Phishing, Història clínica, rastreig i bases de dades de COVID, presa de temperatura als locals comercials, afectació laboral de la COVID, teletreball, etc.

ACCIÓ FORMATIVA

Com s'ha dit, una de les **principals funcions de l'agència és la realització de formacions a entitats públiques i privades**. Ara bé, el context de pandèmia viscut durant l'any 2020 ha impedit dur a terme aquesta funció. Per aquest motiu, l'Agència ha realitzat la seva **funció formativa i divulgativa a través de la creació de guies, recomanacions i infogràfics** explicatius de l'afectació de la COVID-19 a la protecció de dades.

Algunes d'aquestes han estat:

- *Recomanació sobre tractament de dades en el context del COVID-19*
- *Teletreball*
- *Tractament de dades per part d'autoritats sanitàries.*
- *Guia de la Comissió Europea sobre les apps de suport a la lluita contra la pandèmia del COVID-19 en relació amb la protecció de dades.*
- *Nota informativa sobre la legitimitat de la presa de temperatura a clients en establiments comercials i allotjaments turístics.*
- *Recollida de dades COVID-19 en establiments de restauració.*

Consell d'europa i fòrums internacionals

FÒRUMS INTERNACIONALS
PUBLICACIONS
ASSOCIACIONS I XARXES INTERNACIONALS

Fòrums internacionals

Remarcar que arran de la situació pandèmica, aquests fòrums es realitzaren telemàticament.

CONFERÈNCIA INTERNACIONAL. Octubre 2020.

Arran de la crisi sanitària, la Conferència Internacional d'autoritats de protecció de dades que havia de celebrar-se a Mèxic, es celebrà de forma telemàtica l'octubre de 2020.

S'adoptaren les següents resolucions:

- Tecnologies de reconeixement facial.
- El rol de la protecció de dades en el desenvolupament d'ajuda internacional, ajuda humanitària i gestió de crisis.
- Responsabilitat en el desenvolupament i ús d'Intel·ligència artificial.
- Reptes sorgits arran de la Pandèmia de la COVID-19 en matèria de protecció de dades.

CONFERÈNCIA DE PRIMAVERA. Dubrovnik 2020 .

Arran de la crisi sanitària, la Conferència de Primavera d'autoritats de protecció de dades que havia de celebrar-se a Croàcia, es posposà fins al Maig de 2021, mantenint la seu estipulada.

Així mateix, el Grup de Treball sobre el futur de la conferència prorrogà la seva composició i els treballs realitzats fins a la celebració de la conferència.

PUBLICACIONS

Consell d'Europa:

Realització de perfils i el Conveni 108+: Informe sobre els desenvolupaments en tecnologies de realització de perfils arran de la Recomanació de 2010.

Declaracions conjuntes del Conveni 108+ i del Supervisor Europeu de Protecció de dades sobre la protecció de dades en el context de fluxos transfronterers de dades personals, sobre rastreig de contactes i de protecció de dades en el context de pandèmia .

Informe relatiu a la Protecció de dades d'Infants en el sistemes educatius: reptes i possibles remeis.

Guia sobre la Protecció de dades d'infants en el context educatiu.

Informe relatiu a les Solucions Digitals per a la lluita contra la COVID-19.

ASSOCIACIONS I XARXES INTERNACIONALS

Remarcar que la organització i la participació en aquestes xerrades fou telemàtica arran del context de pandèmia.

Associació de la Francofonia de Protecció de Dades (AFAPDP)

En la trobada anual de l'Associació de la Francofonia de Protecció de Dades (AFAPDP) es realitzà una declaració conjunta sobre la necessitat d'harmonitzar la resposta als reptes per a la intimitat i la protecció de dades sorgits arran de la crisi de la COVID-19.

Xarxa Iberoamericana de Protecció de Dades (RIPD) 2020

De forma similar, la reunió online celebrada el passat desembre de 2020 de la xarxa iberoamericana declarà que el dret a la salut i el dret de protecció de dades no són drets incompatibles i que es necessita una actuació conjunta per tal de garantir el respecte a ambdós drets.

Perspectives i prioritats de l'Agència.

PRIORITATS

PRIORITATS:

La principal prioritat de l'Agència són els drets dels ciutadans. Així, la protecció efectiva d'aquests exigeix una doble vessant d'actuació: per una banda cal conscienciar als mateixos en l'ús responsable de les seves dades i dels drets que se li reconeixen; i, alhora, vetllar perquè l'exercici d'aquests drets es faci amb totes les garanties. Una valoració realista de les garanties que dóna qualsevol responsable de tractament de dades fa imprescindible analitzar què coneixen sobre els riscos que planteja el desenvolupament tecnològic i els nous serveis en Internet i com reaccionen davant ells.

A nivell intern, l'Agència busca donar resposta a les necessitats de la ciutadania i en base a això es dóna resposta a les qüestions plantejades per aquests, pels sectors empresarials, i especialment es duen a terme formacions i xerrades adreçades als més joves. No obstant això, i tenint en compte els recursos que es disposen, l'Agència es veu obligada a prioritzar les tasques quotidianes i definir objectius que consideri prioritaris arran de l'aparició de noves realitats que alterin l'estat del dret de protecció de dades i vetllant pel compliment i respecte d'aquest dret fonamental, ja que les autoritats de protecció de dades suposen una de les garanties institucionals d'aquest.

No obstant tots aquests objectius requereixen d'una base jurídica, moderna, actualitzada i emmirallada en la normativa europea, tant del Consell d'Europa com de la Unió europea, raó per la qual s'ha proposat al Consell General, modernitzar la Llei de Protecció de dades, del 2003, per tal que esdevingui una eina jurídica de futur, en la garantia de la protecció del dret fonamental a la protecció de les dades personals. La nova Llei pretén canviar de forma substancial la manera d'afrontar el compliment de la normativa de protecció de dades. D'una banda, a conseqüència del principi de la responsabilitat proactiva o accountability, i d'altra banda, també especialment, a causa de l'enfocament en el risc en relació amb el compliment del conjunt d'obligacions, des de com facilitar el dret d'informació fins a com fer les avaluacions d'impacte sobre la protecció de dades. Aquesta norma obre un camí de reptes i oportunitats en el marc d'un canvi global en termes econòmics, polítics i socials. Incorpora canvis que afecten de manera directa els drets i les llibertats de les persones i, de forma especial, el dret a la protecció de dades i la privacitat, ja que les dades s'han convertit en part essencial del desenvolupament d'aquest nou entorn.

Annexos:

ANNEX 1: DIA DE PROTECCIÓ DE DADES 2020

ANNEX 2: GUIES I PUBLICACIONS DE L'AGÈNCIA

ANNEX 1: DIA DE PROTECCIÓ DE DADES 2020

TAULA DE CONTINGUTS

INTRODUCCIÓ

La biometria forma part de l'avantguarda de les novetats que dia a dia la tecnologia aporta.

Planerament, la biometria **és la mètrica relacionada amb característiques humanes.** Malgrat pugui sonar a matèries pròpies de la ciència ficció, cada cop que desbloquegem la pantalla del nostre smartphone amb l'empremta digital o amb un mètode de reconeixement facial o quan li preguntem a assistents de veu com la Siri o l'Alexa quin temps farà demà estem utilitzant tecnologies biomètriques. Aquests usos poden semblar més innocus però la realitat és que **les possibilitats que ofereix la biometria sobre els àmbits d'aplicació d'aquests mètodes són incalculables.**

Les formes d'identificació biomètrica **actuen tant com una forma d'identificar als interessats com una forma d'autenticar la seva identitat,** donant així l'aparença de ser mètodes que garanteixen la seguretat de matèries sensibles o confidencials. El seu àmbit d'aplicació creix dia a dia i ja podem veure com **el seu ús s'expandeix en múltiples disciplines**: seguretat pública i supòsits penals, militars, l'àmbit transfronterer, l'àmbit civil, medicina i prestacions socials, àmbit laboral, aplicacions comercials, etc.

Alhora, les dades emprades per aquestes tècniques aporten moltes avantatges per als responsables de tractament ja que **es tracta de dades universals a totes les persones úniques, permanents, mesurables, emmagatzemables, i difícilment falsificables**.

Tots aquests valors fan que les tecnologies i les dades biomètriques siguin un **actiu econòmic** cada vegada més rellevant.

2. QUÈ ENTENEM PER BIOMETRIA?

La Biometria és un grup de **tècniques** que permeten que una persona sigui identificada o autenticada en base a una sèrie de **dades reconeixibles i verificables que li son úniques i específiques.**

D'acord amb el RGPD es defineixen les dades biomètriques com les dades que resulten de l'aplicació de tècniques específiques de tractament de **dades, físiques, psicològiques i de comportament** d'una persona física que «*(...) permet la seva identificació* (art. 4) que mereixen de **protecció especial** (art. 9).

Així doncs, podem afirmar que per a que siguin efectives les dades biomètriques han de ser **úniques, permanents i que puguin recollir-se**

Exemple de tractament de dades biomètriques.

Una empresa introdueix un sistema d'escaneig d'empremtes digitals per a regular els horaris dels treballadors i l'accés a les instal·lacions. Aquest sistema tracta dades biomètriques amb l'objectiu d'identificar a una persona física així que l'empresa necessita d'una justificació vàlida per a aquest tractament.

L'ús de tècniques biomètriques respon a **dos objectius:**

- **La identificació biomètrica**: és el procediment de determinar la identitat de la persona. L'objectiu doncs és recollir un element concret de dades biomètriques d'una persona (una fotografia de la seva cara, un enregistrament de veu, una imatge de la seva empremta digital, etc). quest element es compara amb el d'altres persones i s'emmagatzema en una base de dades. Aquest objectiu busca respondre a la pregunta «*Qui és vostè?*».
- **Autenticació biomètrica:** és el procediment de comparar les característiques de la persona amb l'arxiu de dades emmagatzemat per a trobar-hi semblances. Existeix doncs un mode de referència en una base de dades que es compara amb les dades recollides en aquell moment per autentificar que la identitat de la persona es correspon amb aquella emmagatzemada. Podriem dir doncs que aquest objectiu respon a la pregunta «*És vostè el sr./la sra. X?*».

INTRODUCCIÓ

Malgrat el caràcter especial d'aquest tipus de tecnologies, que es basen en aspectes tan íntims com pot ser el propi cos de l'interessat, resulta curiós que **les provisions legals que en regulen l'ús no són molt nombroses i les que existeixen, fan una remissió genèrica a les normes en protecció de dades** sense conferir un estatus específic a aquest tipus de tractaments.

Per tal de reconèixer aquestes particularitats, el Reglament General Europeu en matèria de Protecció de Dades (en endavant RGPD), text legal de la Unió Europea amb voluntat clara d'harmonitzar els estàndards de protecció a nivell internacional, **va descriure les dades biomètriques com a «dades sensibles»** i en prohibeix el tractament a no ser que es provi que l'interessat va consentir expressament al mateix o que es tracta d'una matèria d'interès i seguretat pública (entre d'altres excepcions).

Amb la present guia, l'Agència andorrana de protecció de dades vol aportar una visió genèrica sobre **què entenem per dades biomètriques i els impactes que el tractaments de les mateixes poden tenir sobre els particulars en diferents àmbits del seu dia a dia.**

QUINS TIPUS DE TÈCNIQUES BIOMÈTRIQUES EXISTEIXEN ACTUALMENT?

TÈCNIQUES DE COMPORTAMENT

El processament d'aquest tipus de dades es basa en analitzar la forma amb la que l'interessat interactua amb un sistema informàtic per tal d'analitzar la fluidesa, la velocitat, etc.

Reconeixement de la signatura o de la velocitat d'escriure amb teclats: existeixen dues formes d'anàlisi la estàtica (captura d'una imatge de la signatura) i dinàmica (analitza els moviments de l'interessat per tal de produir la signatura). En el cas de la velocitat de teclejar s'emprarà per considerar si l'interessat està familiaritzat amb el que escriu.

Reconeixement de mirada: anàlisi de la forma i els patrons que segueix l'interessat amb la seva mirada.

Reconeixement de la forma de caminar: la forma de caminar o la velocitat també es poden capturar mitjançant imatges per tal d'identificar als particulars.

TÈCNIQUES BIOLÒGIQUES

El processament d'aquest tipus de dades es basa en analitzar aspectes relatius a la biologia de l'interessat per tal d'identificar-lo.

Identificació d'ADN: identificar al particular a través de l'anàlisi de segments concrets del seu ADN.

Reconeixement de venes: anàlisi dels patrons que creea el sistema circulatori de cada particular en un punt concret del seu cos (mans, dits, etc).

QUINS TIPUS DE TÈCNIQUES BIOMÈTRIQUES EXISTEIXEN ACTUALMENT?

El reconeixement facial o les empremtes digitals són només dos exemples de tècniques biomètriques però no és un llistat exhaustiu. Dins de les tècniques **podem distingir tres tipus: les físiques/sensorials, les de comportament i les biològiques.**

TÈCNIQUES FÍSIQUES / SENSORIALS

El processament d'aquest tipus de dades biomètriques es fa a través de la digitalització d'imatges, enregistraments o mostres per tal de crear una plantilla o un perfil que s'emprarà per trobar coincidències i ajudar a la identificació.

Reconeixement empremtes digitals: captura de la imatge i establiment de patrons. El seu ús és comú en tota mena d'àmbits, policial, de seguretat, tràmits, comerç, etc.

Reconeixement facial: captura de la imatge i establiment de patrons i trets distintius. S'empra habitual en àmbits de seguretat i de law-enforcement, malgrat ja és comú el seu ús per desbloquejar dispositius com smartphones o ordinadors portàtils.

Reconeixement d'iris i retina: captura de la imatge i establiment de patrons. S'empra habitualment a l'àmbit de la seguretat.

Geometria de l'orella, de la mà o dels dits: captura de la imatge i establiment de patrons.

Reconeixement d'olor: captura d'una mostra i establiment de patrons que la facin identificable.

Reconeixement de veu: enregistraments d'audio emprats per analitzar les ondes sonores de la veu del particular. S'empra per verificar la identitat o per donar instruccions assistents de veu.

LA BIOMETRIA I LA PROTECCIÓ DE DADES.

RISCS INHERENTS AL TRACTAMENT DE DADES BIOMÈTRIQUES

Tal i com hem vist, les dades biomètriques tenen la consideració de dades personals ja que permeten identificar a particulars i a més a més, tenen la consideració de dades sensibles. Aquest darrer punt implica doncs que **la llei confereix a aquest tipus de dades una protecció especial i per tant, convindrà analitzar per una banda els riscs que presenten per tal de dissenyar un sistema de seguretat adient per a protegir-les.**

Podem veure com fàcilment existeixen riscs inherents al tractament de dades biomètriques com pot ser la **irreversibilitat** de subsanar filtracions o de ciberatacs.

Com hem dit, en el cas de dades biomètriques cal tenir en compte que **les mateixes són permanents per tant, no es poden modificar**. Per exemple, en el cas de la filtració d'una contrasenya, aquesta pot canviar-se ràpidament. Ara bé, les dades biomètriques d'un particular es mantenen inalterables així que si es veuen compromeses no es pot recuperar el control sobre les mateixes.

Un altre dels riscs inherents al tractament de dades biomètriques és **la impossibilitat de la normativa de mantenir-se al dia de les constants novetats que apareixen i dels nous mètodes** per tal de tractar nou tipus de dades. Per aquest motiu és convenient que les mesures de seguretat adoptades pels responsables de tractament siguin flexibles i permetin la seva constant actualització.

LA BIOMETRIA I LA PROTECCIÓ DE DADES.

PRINCIPIS RECTORS

Conscients d'aquests riscs, els responsables de tractament han d'aplicar una sèrie de principis rectors a la seva actuació amb dades personals de tipus biomètric.

Aquests principis són 5:

- **Objectiu concret i legítim.** Quan es recullen dades biomètriques convé informar extensament i clarament de les finalitats per les quals es fa aquesta recollida. Alhora, qualsevol tractament o ús d'aquestes dades més enllà de les previstes i informades a l'interessat, es considerarà il·legítim de ple dret.
- **Proporcionalitat**. En el moment d'optar per un sistema de tractament de dades biomètrics cal dur a terme una ponderació per tal de veure si aquests sistemes son els adequats i adients per complir amb l'objectiu concret i legítim anteriorment citat. Cal valorar doncs criteris com la necessitat i la proporcionalitat de les mesures en base a la ingerència a la intimitat dels particulars que provoquen.
  Així doncs convindria que els responsables valoressin si existeixen mitjans menys invasius que permetin complir amb el mateix objectiu i, de així existir, optar per aquests últims.
- **Precisió**. Les dades biomètriques hauran de ser pertinents a la finalitat per la qual es recullen i exactes. Aquesta exactitud és de vital importància per tal d'evitar casos d'usurpació d'identitat.
- **Minimització de dades.** Només podran tractar-se, cedir-se i emmagatzemar-se dades personals biomètriques necessàries i no tota la informació que estigui disponible al responsable.
- **Termini de conservació adequat.** Ja en el moment de la recollida convindrà determinar un període de conservació que mai podrà ser superior al necessari per a dur a terme la finalitat concreta i legítima. Alhora convindrà garantir que un cop hagi transcorregut aquest període les dades es suprimiran de qualsevol sistema d'emmagatzematge i no es tractaran en cap cas.

LA BIOMETRIA I LA PROTECCIÓ DE DADES.

EL CONSENTIMENT

Tal i com s'ha mantingut tant en la normativa andorrana com a l'europea es defineix al consentiment com una **manifestació de voluntat, expressa, lliure, específica i informada, mitjançant el qual l'interessat consenteix al tractament de les seves dades personals.** Així doncs, entenent que el fet de condicionar l'acceptació de les condicions generals la oferta o la prestació d'un servei no serà un consentiment lliure.

Concretament en el cas de dades biomètriques fins i tot es considera que el fet de **no proporcionar una alternativa vàlida a l'autenticació per biometria suposarà un vici en el consentiment donat** ja que el mateix no haurà estat donat amb totes les garanties.

Alhora, cal recordar que el consentiment **ha de poder-se revocar en qualsevol moment** i per tant, els responsables de tractament hauran d'adoptar les mesures tècniques necessàries que puguin esborrar les dades biomètriques del seu sistema.

LA BIOMETRIA I LA PROTECCIÓ DE DADES.

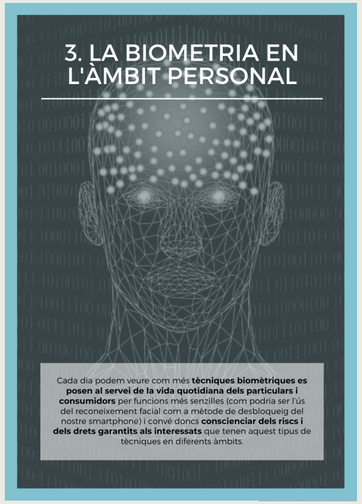
OBLIGACIONS DEL RESPONSABLE I DRETS DELS INTERESSATS

Tal i com hem vist fins ara, **la seguretat** en la recollida de dades biomètriques ha de ser la preocupació principal de responsables de tractament i dels interessat arran de la naturalesa irrevocable d'aquest tipus de dades.

Els drets dels interessats en dades biomètriques són els mateixos que en qualsevol recollida de dades (a consentir lliurement, drets ARSO,etc). És en el **dret a la informació en el que trobem especificitats** ja que la persona interessada haurà de ser informada del tipus de dades biomètriques recollides, la finalitat de la mateixa, la base legal per al tractament de dades, la font d'obtenció, la forma de control sobre les mateixes (*serà el propi usuari qui emmagatzemarà les dades o una base de dades encriptada?*), possibles destinataris d'aquestes dades, etc. De no complir amb aquest deure d'informació, qualsevol cessió de dades de l'interessat es considerarà nul·la ja que no fou consentida plenament.

Obligacions específiques dels responsables de tractament en dades biomètriques:

- Informar degudament a l'interessat i obtenir-ne un consentiment exprés i informat.
- Establir un sistema de recollida i tractament de dades biomètriques basat en la protecció de la intimitat by design i by default; tant en el seu disseny com en la implantació el mecanisme emprat ha de tenir en compte i garantir en tot moment la intimitat i la confidencialitat de les dades recollides i la seva configuració ha de ser d'entrada la més restrictiva a possibles afectacions d'aquests drets.
- Avaluar l'impacte sobre la intimitat que pot tenir aquest mecanisme. Aquestes no només hauran d'identificar els risics inherents al tractament sinó també hauràde proporcionar les mesures adequades de protecció i buscar les solucions més adients per atenuar aquests risics.
- Establir mesures tècniques i organitzatives que asseguirin la confidencialitat i la seguretat de les dades tractades.



3. LA BIOMETRIA EN L'ÀMBIT PERSONAL

Cada dia podem veure com més **tècniques biomètriques es posen al servei de la vida quotidiana dels particulars i consumidors** per funcions més senzilles (com podria ser l'ús del reconeixement facial com a mètode de desbloqueig del nostre smartphone) i convé doncs **conscienciar dels risics i dels drets garantits als interessats** que tenen aquest tipus de tècniques en diferents àmbits.

A. LA BIOMETRIA I ELS SMARTPHONES.

En els darrers anys hem vist com els smartphones han anat **incorporant mètodes de recollida de dades biomètriques per tal d'autenticar la identitat de l'usuari** per a determinades funcions: desbloquejar l'aparell, realitzar pagaments segurs, etc.

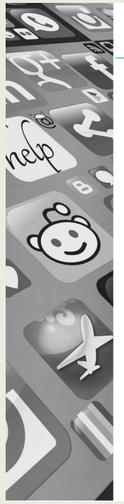
Aquests mètodes s'incorporen de forma automàtica al nostre dispositiu i moltes vegades **l'usuari desconeix que pot optar per altres formes** d'autentificació.

Així doncs podem distingir **dos tipus de dispositius**: aquells que emmagatzemen les dades biomètriques al propi aparell i aquells que ho fan en servidors o núvols.

La primera configuració és habitual en aquest tipus d'aparells i permet que les **dades biomètriques no surtin més enllà del dispositiu** i que estiguin sota el control de l'interessat.

- En aquests casos, serà necessari que el dispositiu garanteixi la seguretat de les dades i la impossibilitat d'accedir-hi de forma extern i ofereixi una alternativa que no impliqui una recollida de dades.

Els dispositius biomètrics que emmagatzemen les dades en servidors externs en canvi presenten més problemes ja que l'interessat en perd el control que passa a ser exclusivament del responsable de tractament. En aquests casos, l'empresa a qui pertanyi aquest dispositiu haurà d'analitzar de forma prèvia els riscs inherents a aquest tipus de tractaments de dades per a les llibertats i els drets dels interessats.



B. LA BIOMETRIA EN APPS.

Des de filtres graciosos a transformacions radicals del nostre aspecte. Cada vegada veiem com més **aplicatius gratuïts demanen que l'usuari cedeixi a la companyia responsable** d'aquestes aplicacions una imatge del nostre rostre. Altres fins i tot ens demanen que portem un dispositiu extern que mesurarà aspectes tan variats com la nostra freqüència cardíaca, les nostres hores de descans o la quantitat de passes que fem en un dia.

Però perquè? Com hem dit la majoria d'aquestes apps son gratuïtes però el que desconeix l'interessat que **el preu que paga per emprar-les és la cessió de les seves dades personals.** Aquestes sovint es cedeixen a tots els col·laboradors de l'empresa responsable de l'aplicatiu i **l'interessat en perd qualsevol tipus de control.** Les dades recollides doncs **es posen a disposició de virtualment qualsevol empresa** per tal que configuri perfils, ens enviï publicitat dirigida en base al nostre estil de vida, es creeín perfils falsos a les xarxes o en altres àmbits.

En la majoria d'aplicatius a més a més es condiciona l'ús del **mateix a l'acceptació d'unes condicions i polítiques de privacitat** que l'interessat no arriba a llegir mai.

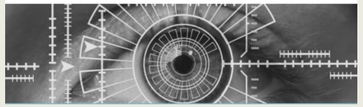
L'ús d'aplicatius que recullen dades personals, i especialment dades biomètriques, ha de condicionar-se sempre a que **l'interessat en conegui les conseqüències.** Aquestes només apareixeràn en aquestes condicions i polítiques d'ús per tant resulta vital que els interessats se les llegeixin abans d'utilitzar-les.

C. BIOMETRIA I COMERÇ

En el comerç online els responsables han de fer front a diferents reptes de seguretat arran de la vulnerabilitat que suposa per al client exposar-se a pràctiques tan habituals com el frau, els hackeigs, spams o el robatori de dades confidencials. Així, veiem que **els responsables de tractament busquen constantment millorar el seu apartat de seguretat online** no només per a que les transaccions siguin més fluides sinó per generar en el client una confiança que garantirà que torni a optar pels seus serveis.

Amb aquesta idea en ment podem veure com la biometria com a mètode per tal d'aprovar o dur a terme pagaments o transaccions proporciona un sistema fluït, ràpid i segur que dona per una banda **aparença de seguretat** i de l'altra, permet en molts casos que l'interessat mantingui el **control sobre les seves dades biomètriques.** Cal remarcar però que en el cas d'optar per mètodes biomètrics per a la autenticació d'usuaris serà responsabilitat del venedor o del proveïdor dels serveis de que, en cas de detectar algun tipus d'accés indegut o divulgació de dades, canviar els mecanismes d'autenticació; ja que, com hem vist, la informació basada en qualitat físiques o sensorials de l'interessat és immutable en el temps.

A part de l'exemple comentat de transaccions comercials online podem veure com aquest tipus de tècniques són adoptades cada vegada més sovint per altres àmbits com ara les entitats bancàries. En el cas de transaccions bancàries **on sigui obligatòria la autenticació de l'usuari, mètodes com el reconeixement facial o de veu poden ajudar a agilitzar aquestes verificacions.** Ara bé, per tal d'assegurar que l'interessat no perdi el control sobre aquestes dades, la informació biomètrica recollida ha d'emmagatzemar-se o bé en un dispositiu en possessió de l'interessat o en una base de dades centralitzada i encriptada a la que només podrà accedir a les dades biomètriques la persona afectada.



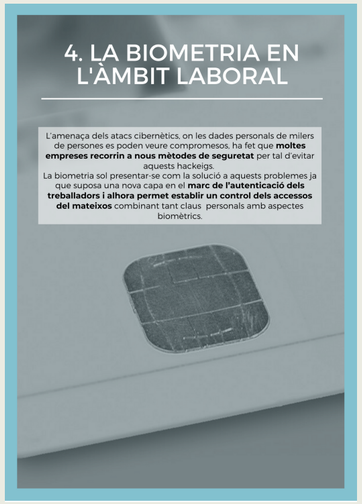
4. LA BIOMETRIA EN L'ÀMBIT LABORAL

L'amenaça dels atacs cibernètics, on les dades personals de milers de persones es poden veure compromeses, ha fet que moltes empreses recorrin a nous mètodes de seguretat, per tal d'evitar aquests hackeigs.
La biometria sol presentar-se com la solució a aquests problemes ja que suposa una nova capa en el marc de l'autenticació dels treballadors i alhora permet establir un control dels accessos del mateixos combinant tant claus personals amb aspectes biomètrics.

La biometria en l'àmbit laboral permet implementar un sistema mitjançant el qual el treballador registra alguna dada biomètrica tant com a mecanisme de fitxar com per tal d'accedir a dades confidencials de l'empresa. Així podem veure com aquests mètodes resulten especialment atractius per a empreses que vulguin dur a terme aquest tipus de controls o vulguin optar per aquests mètodes de seguretat.

Ara bé, les empreses que vulguin implantar aquests sistemes hauran de tenir en compte que els mecanismes emprats hauran de respectar una sèrie d'exigències legals i concretament de la normativa de protecció de dades, donant èmfasi a la necessitat de complir amb els principis rectors de tractament de dades, els drets dels interessats o qualsevol altre precepte d'aplicació.

Així doncs hem de distingir, entre d'altres diferents aspectes com ara les finalitats permeses per a aquestes tècniques i la seva justificació, el tipus de dades que podem recollir les tècniques més adients a emprar en cada cas, la conservació de les dades, la recollida del consentiment del treballador i les avaluacions d'impacte a dur a terme abans de la instal·lació.



4. LA BIOMETRIA EN L'ÀMBIT LABORAL

L'amenaça dels atacs cibernètics, on les dades personals de milers de persones es poden veure compromeses, ha fet que **moltes empreses recorrin a nous mètodes de seguretat** per tal d'evitar aquests hackeigs.
La biometria sol presentar-se com la solució a aquests problemes ja que suposa una nova capa en el **marc de l'autenticació dels treballadors i alhora permet establir un control dels accessos del mateixos** combinant tant claus personals amb aspectes biomètrics.

TIPUS D'EMMAGATZEMATGE DE DADES BIOMÈTRIQUES

TIPUS A

Les dades biomètriques recollides i emmagatzemades en **dispositius en possessió i control exclusiu de la persona interessada** (els treballadors). Ex: una targeta identificativa.

TIPUS B

Les dades biomètriques **són emmagatzemades en un sistema controlat pel responsable** (l'empresari) però són conservades en una forma que les fa inservible a no ser que **s'introdueixi una clau o un suport controlat per l'interessat**. Ex: Base de dades protegides amb múltiples contrasenyes.

TIPUS C

Les dades són **emmagatzemades i controlades pel responsable de tractament de forma exclusiva**. Ex. Sistema biomètric per a fitxar amb dades biomètriques.

En el supòsit que els responsables vulguin optar per mesures d'emmagatzematge de tipus B o C hauran de **justificar de forma profusa i per escrit la necessarietat** d'aquestes mesures.

Cal tenir en compte també que les mesures de seguretat a adoptar per part dels responsables de tractament **s'establiran en base al risc previsible** inherent al tractament de dades biomètriques.

FINALITAT I JUSTIFICACIÓ

Recórrer a dispositius biomètrics en l'àmbit laboral ha de respondre a una finalitat legítima i concreta. Al tractar-se d'un mecanisme molt intrusiu en la intimitat dels treballadors, l'ús de dades biomètriques només es podrà restringir a:

- controlar l'accés a les instal·lacions o a locals o zones identificades pel propi empresari com a zones de circulació restringida.
- controlar l'accés a aplicatius o dispositius informàtics professionals especificats pel responsable de tractament.

Alhora convindrà justificar l'ús d'aquestes tècniques per sobre de mecanismes tradicionals d'organització o de control. Així doncs, el responsable haurà d'especificar en un document:

- el context específic que fa necessària l'adopció d'un sistema de protecció més elevat;
- les raons que justifiquen l'ús d'una tècnica biomètrica per sobre d'una tradicional.

DADES PERSONALS TRACTABLES:

DADES IDENTIFICATIVES

Són dades recollides pel responsables basades en **identificar als treballadors.** Poden referir-se a:

- Identitat: *nom, cognom, fotografies, enregistraments en brut de dades biomètriques, número d'autenticació o de suport individual, contrasenyes, etc.*
- Vida professional: *número de registre intern, lloc de treball.*
- Accessos: *zones permeses, zones restringides, dispositius permesos i horaris autoritzats.*

DADES DERIVADES

Són dades **generades pels dispositius de tractament de dades biomètriques** com és el registre d'accessos a zones o dispositius i el seu control.

CONSENTIMENT DELS TREBALLADORS

Tal i com s'ha especificat en el primer apartat d'aquesta guia, **la obligació d'informar és un dels pilars que legitimen el tractament** de dades biomètriques.

Així doncs, el responsable de tractament haurà d'informar als seus treballadors, per escrit, del **tipus** de dades biomètriques recollides, la **finalitat** de la mateixa, la **base legal** per al tractament de dades, la font d'obtenció, la **forma de control** sobre les mateixes, possibles **destinataris** d'aquestes dades, etc. Davant aquesta informació, l'interessat (treballador) haurà de **consentir**.

Ara bé, en l'àmbit laboral convé qüestionar **fins a quin punt el treballador és lliure** de consentir arran de la dinàmica de poder entre les dues figures. Per aquest motiu, en supòsits que el responsable condicioni l'acceptació de les mesures a la continuïtat al lloc de treball o no ofereixi mesures no biomètriques alternatives, **s'entendrà que el consentiment prestat pel treballador no serà vàlid.**

4. LA BIOMETRIA EN L'ÀMBIT LABORAL

CONSERVACIÓ DE DADES BIOMÈTRIQUES

En el cas de la conservació de dades biomètriques en l'àmbit laboral cal distingir segons el tipus de dades de que és tractin.

Dades en brut.

Es tracta de les imatges, els àudios, que capturen la dada biomètrica a tractar. Aquestes dades només es podran conservar durant el temps necessari per a la seva digitalització o transformació en càlculs o plantilles. Un cop feta aquesta transformació, han de destruir-se.

- Les dades biomètriques que es generin hauran d'encriptar-se de forma que no es pugui recalcular les característiques biomètriques d'origen i hauran de conservar-se durant el temps d'habilitació del treballador.

Dades derivades.

Les dades generades pels dispositius de tractaments de dades biomètriques hauran de conservar-se en el propi dispositiu durant un termini màxim de 6 mesos des del seu enregistrament. Si aquestes dades es traslladen a un dispositiu diferent, es podran conservar durant més temps sempre que aquesta pròrroga es justifiqui en un imperatiu legal o una necessitat del responsable per a complir amb les seves funcions.

Dades identificatives.

Les dades diferents a les dades biomètriques que es vinculin a les mateixes (nom del treballador, càrrec professional, etc) hauran de suprimir-se en un termini màxim de 6 mesos a comptar des de la inhabilitació del treballador en qüestió. Aquesta supressió no afecta a dades similars o idèntiques que el responsable de tractament tracti per a finalitats diferents a les finalitats que justifiquen la recollida de dades biomètriques.

5. LA BIOMETRIA EN L'ÀMBIT PÚBLIC I LAW ENFORCEMENT (L.A)

Entenem per *law enforcement* com la **prevenció, la investigació, la detecció i la persecució de delictes o l'execució de sentències penals**, incloent les accions dutes a terme per a la prevenció d'amenaces a la **seguretat pública.**

5. LA BIOMETRIA EN L'ÀMBIT PÚBLIC I LA

El reconeixement facial o les empremtes digitals són només dos exemples de tècniques biomètriques però no és un llistat exhaustiu. Dins de les tècniques **podem distingir tres tipus: les fisiques/sensorials, les de comportament i les biològiques.**

COM FUNCIONA EL SISTEMA DE RECONEIXEMENT FACIAL?

Durant els darrers mesos hem vist com molts estats i administracions públiques han optat per la instal·lació de sistemes de reconeixement facial en punts estratègics i públics com son duanes, estacions de transport públic o aeroports. Aquests sistemes es basen en un **tractament de dades en temps real mitjançant el qual es capta la imatge de tota persona mitjançant càmeres de videovigilància.** Les imatges llavors es processen per un software de reconeixement facial que produeix una plantilla biomètrica de cada rostre.

Aquestes plantilles llavors **es comparen amb una base de dades** de persones d'interès creada per autoritats legitimades com el cos policial de l'Estat en qüestió i organismes policials supranacionals.

Si el software estipula que entre la imatge captada en temps real i alguna de les cares de la base de dades **hi ha semblances suficients, es procedeix a la comprovació de la identitat de la persona interessada** per part del personal de seguretat d'aquests espais públics per veure si, efectivament, es tracta d'alguna de les persones llistades per les autoritats de law enforcement.

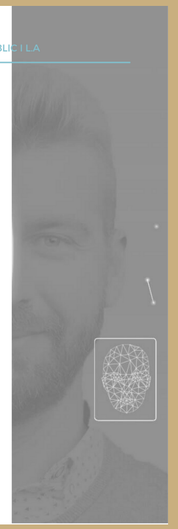
5. LA BIOMETRIA EN L'ÀMBIT PÚBLIC I LA

LA NECESSARIETAT

Al tractar-se d'un tractament de dades considerades sensibles, la justificació per l'ús d'aquestes mesures ha de ser més elevat; així que cal fixar-se en el criteri de la necessarietat. La necessarietat es basa en els principis de proporcionalitat i efectivitat.

Així, el responsable haurà de considerar si el tractament d'aquestes dades sensibles és proporcional a la finalitat perseguida i si no es pot optar per mesures alternatives al reconeixement facial o la recollida de dades biomètriques. Fàcilment podem deduir que l'ús de tecnologies com el reconeixement facial hauria de limitar-se a la persecució de crims greus i no optar per un auge d'aquest tipus de mètodes per a delictes menors o, fins i tot, infraccionsa dministratives.

Per tant, l'ús de tècniques com el reconeixement facial serà més respectuosa amb la normativa de protecció de dades com més concreta sigui la finalitat per la qual s'empra i com menor sigui l'escala d'afectats a la que es pensa aplicar.



5. LA BIOMETRIA EN L'ÀMBIT PÚBLIC I LA

QUINA HA DE SER LA BASE PER A AQUESTS TRACTAMENTS?

En la recollida d'aquestes dades biomètriques s'afectaran els interessos tant de persones presents a les llistes de persones d'interès com de particulars que no hi constin. Així convindrà que el tractament de dades descrit haurà d'ajustar-se sempre a les limitacions de la normativa de protecció de dades.

Així les dades podran recollir-se si el tractament de dades:

- és **legítim** (d'acord amb els principis prevists a l'art. 11 de la Llei 15/2003, de 18 de desembre, qualificada de protecció de dades i a l'art. 6 del Decret del 9-6-2010, d'aprovació del Reglament de l'Agència andorrana de protecció de dades).
- Es fonamenta en una **disposició legal** que estableixi de forma prèvia uns usos clars, precisos i previsibles. Alhora, aquesta norma haurà de revisar-se de forma periòdica per tal d'adaptar-la als avenços científics i tecnològics.
  - *Pot un particular preveure de forma raonable que la seva imatge es recolli i tracti amb aquesta pràctica?*
- Es basa en el **consentiment** de l'interessat o en **la seguretat pública** (aquest últim, caldrà justificar la necessarietat de la mesura arran del seu caràcter excepcional).
  - *Consentiment?* Ha de ser una manifestació de voluntat, expressa, lliure, específica i informada, mitjançant el qual l'interessat consenteix al tractament de les seves dades personals.

Al mateix temps convindrà que el responsable de tractament conscienciï, formi i posi a l'abast dels treballadors que duran a terme la recollida d'aquestes dades biomètriques de la normativa de protecció de dades, dels riscs iles bones pràctiques d'aquestes tècniques.

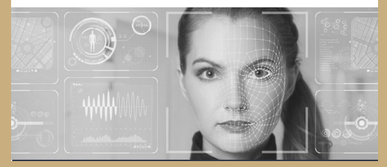
5. LA BIOMETRIA EN L'ÀMBIT PÚBLIC I LA

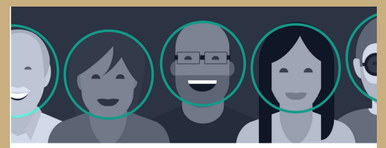
LA NECESSARIETAT

Cal considerar també que un ús indiscriminat d'aquestes tècniques provocaria que la confiança de la opinió pública en aquest tipus de mesures fes que els potencials interessats deixessin de poder preveure clarament les conseqüències esdevenint llavors el tractament il·lícit.

En aquest sentit, un exemple clar de principi afectat podria ser el de la minimització de dades. Així, les llistes de persones d'interès haurien d'incloure només aquells casos que siguin més greus.

Ens referim a efectivitat com la valoració que ha de fer el responsable de valorar si les mesures preses són les que, en relació a la intromissió a la intimitat que suposen, garanteixen al màxim els beneficis que es volen obtenir d'emprar tècniques com el reconeixent facial. En aquest cas, l'efectivitat no ha de valorar-se amb criteris com el número de coincidències i de falsos positiu sinó que l'ús d'aquestes mesures es demostri útil i beneficiós per al ciutadà en la prevenció de delictes penals greus. La informació suficient i complerta que cal proporcionar als potencials interessats abans de procedir al tractament de les seves dades biomètriques serveis per a que els mateixos puguin entendre de la necessarietat d'aquestes mesures i així crear una conscienciació de prevenció de delictes i de respecte a la intimitat.





5. LA BIOMETRIA EN L'ÀMBIT PÚBLIC I LA

EL FUTUR DEL RECONEIXEMENT FACIAL

Com hem vist la recollida i tractament de dades biomètriques, i més concretament, dades derivades d'un mecanisme de reconeixement facial comporta una série de riscs per a la intimitat dels interessats amb conseqüències tant lesives que es comencen a sentir veus des de la Comissió Europea que parlen d'una possible prohibició d'aquest tipus de tècniques durant un futur pròxim. Malgrat això, el negoci del reconeixement facial s'estima com un negoci a l'auge que en menys de 5 anys doblarà el seu volum de negoci. Les principals crítiques versen doncs sobre l'eficàcia d'aquests mètodes ja que bàsicament presenten un risc de mal ús que es tradueixi en una vigilància generalitzada.

D'acord amb l'executiu de la Unió Europea el principal repte passa per regular aquestes tècniques per tal de garantir els drets dels ciutadans. Amb aquest objectiu en ment, s'ha preparat per part de la Unió un llibret blanc sobre consells i bones pràctiques en matèria de reconeixement facial (que es publicarà al Febrer de 2020) i ha proposat la prohibició d'aquest tipus de tècniques als espais públics durant un termini de 2 a 3 anys.

6. CONCLUSIONS

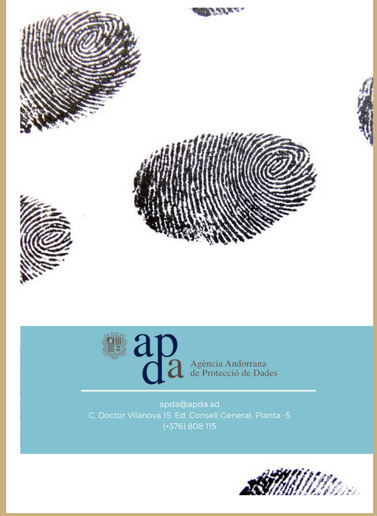
Durant els darrers anys hem vist com t**ant empreses privades com les administracions públiques** han optat per la instal·lació de sistemes de recollida i tractament de dades biomètriques i, alhora, com aquestes **s'han anat fent lloc en l'àmbit privat** a través de dispositius mòvils i formes d'interactuar amb el nostre entorn.

La pròpia naturalesa permanent de les dades biomètriques les converteix en un mètode aparentment segur d'identificació o autenticació però, alhora, aquesta immutabilitat pot comportar greus riscs per a la intimitat dels interessats en supòsits d'accessos indeguts o il·legítims a les dades o la seva filtració o comunicació indegudes o no autoritzades.

Així doncs podem veure com la seguretat en la recollida de dades biomètriques ha de ser la preocupació principal de responsables de tractament i dels interessat arran de la naturalesa irrevocable d'aquest tipus de dades.

Així doncs hem cregut necessària la redacció d'aquesta guia per tal de conscienciar als responsables de les seves obligacions (informar degudament a l'interessat i obtenir-ne un consentiment vàlid, establir un sistema de recollida i tractament de dades biomètriques basat en la protecció de la intimitat by design i by default, tant en el seu disseny com en la implantació, avaluar l'impacte sobre la intimitat que pot tenir aquest mecanisme, etc) i alhora informar sobre els drets dels que disposen els particulars davant d'aquest tipus de tractament de dades i les eines necessàries per tal d'impedir-ne un mal ús o possibles atacs fraudulents.

La recollida i el tractament de dades biomètriques **suposen un risc molt elevat de produir danys irreparables en la privacitat dels interessats** així que cal limitar-ne l'ús a supòsits on quedi provada la seva **necessarietat, proporcionalitat i efectivitat.**



apda Agència Andorrana de Protecció de Dades

apda@apda.ad
C. Doctor Vilanova 15, Ed. Consell General, Planta -5
(+376) 806 115

ANNEX 2: GUIES I PUBLICACIONS DE L'AGÈNCIA

RECOMANACIONS TELETREBALL

Agència Andorrana de Protecció de Dades

És recomanable prendre certes mesures per a assegurar-nos de **mantenir la seguretat i protecció dels equips informàtics fora del centre** de treball i, conseqüentment, de les dades que puguin tractar.

Aquestes **recomanacions** són tant perquè les tinguin en compte els **treballadors** a distància, com perquè els **empresaris** controlin que es compleixen, de manera que es respecti el que s'estableix en lleis i normatives vigents sobre protecció de dades i dades digitals.

1 AVALUAR ELS RISCS

Abans d'instaurar una mesura com el teletreball, el responsable de les dades haurà d'**avaluar el risc i adoptar els procediments i les mesures de control necessàries per a permetre el tractament de les dades dels dels domicilis** particulars i per protegir la intimitat dels treballadors.

2 DEURE DE SECRET I CONFIDENCIALITAT

En els contractes laborals s'acostuma a incloure una clàusula mitjançant la qual el **treballador es compromet a no divulgar dades a que tingui accés arran de la seva feina**. Si aquesta no està inclosa al contracte, és recomanable que **el treballador signi un annex al seu contracte de treball o un acord específic sobre teletreball** abans de procedir al teletreball.
Aquest acord haurà de contenir, entre d'altres, les **instruccions dictades pel responsable de les dades en matèria de protecció de dades** personals, especialment aplicables al teletreball.
Els responsables de **recursos humans o representants dels treballadors hauran de ser informats** dels signants i del contingut d'aquests acords i annexos, sempre preservant la **intimitat** i el dret a la protecció de dades del treballador.
Els treballadors, en el desenvolupament del teletreball hauran de complir amb les **instruccions del responsable** tant a nivell de protecció de dades personals com a especificitats tècniques de seguretat de la informació.

3 DISPOSITIUS DE TREBALL

Obligacions treballadors:

- No deixar **desatesos** els equips portàtils en **llocs públics**.
- **Restringir l'accés no autoritzat** a la informació o recursos per part d'altres persones que utilitzin el dispositiu personal (familiars o amics) i restringir l'ús de tercers a dispositius de l'empresa.
- Evitar la **instal·lació d'aplicacions o la navegació** per pàgines no segures.
- **Bloquejar la pantalla** de l'ordinador quan no estiguem treballant.
- Si s'usa un **equip personal** per al teletreball, a part de seguir totes aquestes recomanacions, és bona idea:
  - Crear un *perfil professional* per a mantenir separats comptes i navegació.
  - *No descarregar* fitxers amb dades de caràcter personal si es poden utilitzar en línia.
  - *Evitar distraccions amb tasques domèstiques* o amb altres membres de la família

Obligacions responsable:

- El responsable **no pot obligar a la instal·lació de programari en dispositius personals del treballador ni l'ús d'aquests** dispositius en el teletreball. Es recomana sempre que el responsable proporcioni els dispositius de treball per tal de minimitzar riscs de filtracions de dades.
- L'acord de teletreball haurà d'especificar quins **termes d'ús podrà fer el treballador de dispositius de l'empresa** durant el teletreball.

4 XARXES I NAVEGACIÓ

- Crear una **xarxa privada o VPN** (Virtual Private Network) per a connectar entre si als treballadors i amb l'oficina, on l'accés a la xarxa estigui protegit per un xifrat que doni una capa extra de protecció. Així evitarem l'accés de tercers no autoritzats a la informació que es comparteix a través d'aquesta xarxa.
- **No** emprar ***Wifi* públiques**.
- **Tancar totes les connexions amb servidors i webs** recorrent a "tancar sessió" o "desconnectar".
- **Esborrar l'historial** de navegació, les cookies i altres dades, així com les contrasenyes recordades.

5 CESSIÓ, DESCÀRREGA I EMMAGATZEMATGE

- Utilitzar tècniques de xifrat de dades **per a la transmissió** de la informació, ús de contrasenyes, *firewall* i antivirus.
- Cura amb l'ús de **memòries USB**, ja que són una possible porta a les infeccions de *malware*.
- **Eliminar la informació temporal** en carpetes de descàrrega, paperera de reciclatge, etc.

6 TAULETES I SMARTPHONES

- **Limitar l'accés al dispositiu** mitjançant un bloqueig amb contrasenya, patró o similar.
- Disposar de mesures per a **localització** del dispositiu o poder realitzar un esborrat remot en cas de pèrdua o robatori.
- Realitzar **còpies de seguretat periòdiques** (preferiblement diàries) de la informació continguda en el dispositiu. Aquestes còpies hauran de fer-se en un dispositiu diferent i a poder ser alocat en servidors de l'empresa o a la pròpia oficina.
- **Actualitzar el sistema operatiu i el programari** a les versions més recents abans de tractar dades personals.

Reforça la ciberseguretat: En una situació d'emergència social, la urgència i manca de temps poden fer-nos descurats, sobretot en el que a seguretat digital es refereix. Per això cal **prestar especial atenció i seguir les recomanacions en ciberseguretat** establertes per organismes oficials o per la mateixa empresa per tal d'assegurar-nos que no es filtrin dades personals o que siguem víctimes de ciberatacs. Alhora, recorda que **qualsevol escletxa de seguretat ha de notificar-se immediatament a l'empresa i a l'Agència andorrana de protecció de dades.**

RECOLLIDA DE DADES PER ESTABLIMENTS DE RESTAURACIÓ

En virtut del *Decret del 8-10-2020 d'adopció de noves mesures excepcionals en el marc de la situació d'emergència sanitària causada pel coronavirus SARS-CoV-2 atès l'augment de la taxa de reproducció de la pandèmia* els establiments de restauració tenen l'obligació de recollir, i per tant, tractar dades personals dels seus clients.
Com podem protegir aquestes dades?

QUINES DADES?

Només es podrà recollir **nom, cognom i número de telèfon.** Es prohibeix la recollida addicional de dades personals.

La recollida del dia i l'hora d'entrada s'emprarà per determinar el termini de **conservació**.

L'establiment **NO** podrà demanar la presentació de **documentació acreditativa** de les dades recollides (còpia de documents d'identitat).

QUINA FINALITAT?

Les dades recollides només es tractaran per recollida per **facilitar la recerca de contactes per part de membres del Cos de Policia i dels funcionaris o treballadors de l'Administració general amb funcions relacionades amb el control de la pandèmia i autoritzats pel Ministeri de Salut i**

Es prohibeix qualsevol altre ús.

DRET A SER INFORMAT

Els clients han de ser informats al moment de la recollida de la **normativa** que empara el tractament de les dades, del **responsable**, de la **finalitat**, la durada de **conservació**, destinataris i de l'existència i l'exercici dels seus **drets** ARSO.

QUANT DE TEMPS?

Tal com marca el Decret, les dades hauran de conservar-se durant **un mes després de la recollida.**
Un cop esgotat aquest termini, les dades es **destruiran**.

COM PROTEGIR LES DADES?

El Decret obliga a la presa de mesures de seguretat necessàries per **garantir la confidencialitat de les dades**, és a dir, per evitar l'accés indegut de tercers a les mateixes.

- Dades en format paper: *dades guardades en un lloc tancat amb clau, evitar que altres clients puguin veure les dades, etc*
- Dades en format digital: *accés protegit per contrasenyes, prohibició d'emmagatzemar les dades en suports mòbils (com ara USBs), etc.*

En qualsevol cas, caldrà **determinar quins treballadors podran accedir a les dades i quins no en base a les seves funcions.**

MODEL

El nostre establiment té la obligació en virtut del Decret del 8-10-2020 d'adopció de noves mesures excepcionals en el marc de la situació d'emergència sanitària causada pel coronavirus SARS-CoV-2 atès l'augment de la taxa de reproducció de la pandèmia, de recollir una sèrie de dades sobre els nostres clients en el marc de la lluita contra la COVID-19.

DATA I HORA D'ARRIBADA: [*a emplenar per l'establiment*]
DADES CLIENTS:
Nom i cognoms: .....
Número de telèfon: .....

***

La informació recollida en aquest formulari només serà recollida per facilitar la recerca de contactes per part de membres del Cos de Policia i dels funcionaris o treballadors de l'Administració general amb funcions relacionades amb el control de la pandèmia i autoritzats pel Ministeri de Salut i no podran ser emprades per cap altra finalitat. Les dades es conservaran durant un (1) mes a comptar des de la data de la recollida i, esgotat aquest termini, es destruiran. Els interessats disposen dels seus drets d'accés, rectificació, supressió i oposició que hauran d'exercir-se davant [*nom de l'establiment, adreça postal i correu electrònic*]; així com el dret a sol·licitar la tutela de l'Agència andorrana de protecció de dades.

EN VIGOR DES DEL 23 DE JULIOL DE 2020

AFECTACIÓ DE LA SENTÈNCIA SCHREMS II A LES TRANSFERÈNCIES INTERNACIONALS DE DADES ENTRE ANDORRA I ELS EUA

Sentència del Tribunal de Justicia de la Unió Europea en l'assumpte C-311/18 - Comissaria de Protecció de Dades vs. Facebook Irlanda i Maximillian Schrems

Agència Andorrana de Protecció de Dades

apda Agència Andorrana de Protecció de Dades

NOTA INFORMATIVA SOBRE LA LEGITIMITAT DE LA PRESA DE TEMPERATURA A CLIENTS D'ESTABLIMENTS COMERCIALS I ALLOTJAMENTS TURÍSTICS.

QÜESTIÓ

És legítima la presa de temperatura corporal de clients per tal de permetre'n l'entrada a establiments comercials i a allotjaments turístics?

NORMATIVA APLICABLE

- Constitució del Principat d'Andorra, (BOPA núm. 24, de 04-05-93)
- Llei 15/2003, del 18 de desembre, Qualificada de Protecció de Dades Personals
- Decret del 9-06-2010 d'aprovació del Reglament de l'Agència Andorrana de Protecció de Dades.

CONSIDERACIONS

1) La legitimitat del tractament de dades.

La normativa andorrana defineix com a tractament de dades «*tota operació aplicada o realitzada sobre dades personals, sigui o no sigui de forma automatitzada*» (art. 3 Llei 15/2003) com són la recollida, el registre, l'organització, la conservació, l'elaboració o la modificació, extracció, consulta, utilització, comunicació per transmissió, difusió o qualsevol altra forma que en faciliti l'accés, la comparació o la interconnexió, el bloqueig, la supressió o la destrucció (art. 5 del Reglament).