Notificacions de violacions de seguretat de dades personals

GUIA INFORMATIVA

AGÈNCIA ANDORRANA DE PROTECCIÓ DE DADES

Versió 2: 11 d'octubre del 2024

Agència Andorrana de Protecció de Dades

Historial de versions

Versió	Data	Detall de la modificació
Versió 2	11 d'octubre del 2024	Actualització del Formulari de notificacions de violacions de seguretat (annex 1)
Versió 1	31 de maig del 2023	Document original

Índex

1) Introducció

Les violacions de seguretat de dades personals són cada cop més freqüents en l'era digital moderna i s'han convertit en una preocupació creixent per a organitzacions de totes les mides i tipus. Les conseqüències d'una violació de dades poden ser greus, ja que s'hi engloben la pèrdua de dades, multes administratives o danys a la reputació, entre d'altres. És essencial que les organitzacions tinguin un pla per protegir les dades i avisar ràpidament els clients i altres parts interessades quan es produeixi una infracció.

Quan es produeix una violació de seguretat de dades personals, els responsables de tractament han d'actuar ràpidament per protegir eficaçment els afectats i mitigar l'impacte de la violació. Les organitzacions han d'adoptar un enfocament proactiu a la notificació de violació de seguretat de dades, i establir, de forma prèvia, una política clara sobre com respondran a aquestes situacions. Aquesta política ha d'incloure els criteris per determinar quan s'ha produït una violació, els passos que s'han de seguir per avaluar-ne l'impacte i el procediment a seguir per tal de notificar-ho a l'autoritat de control competent; i en el cas que així sigui necessari, a les parts interessades.

Aquesta guia descriu les directrius per a la notificació de violacions de seguretat de dades personals, i proporciona a les entitats i les organitzacions un marc per respondre a una violació i minimitzar-ne l'impacte. La guia cobreix tant els passos que s'han de seguir per identificar, avaluar i respondre a una infracció, com els elements essencials per elaborar un protocol intern de resposta davant violacions de seguretat de dades personals. També es preveu el règim sancionador aplicable al no compliment amb el deure de notificació, així com recomanacions sobre les actuacions ex post que ha de seguir un responsable de tractament un cop s'hagi notificat degudament a les autoritats i parts interessades

2) Violacions de seguretat de dades personals

Les violacions de seguretat en protecció de dades es troben regulades tant a la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals (en endavant, LQPD) com al seu reglament d'aplicació (Decret 391/2022, del 28 de setembre, d'aprovació del Reglament d'aplicació de la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals).

En l'article 4, apartat 13 de la LQPD es defineix una "Violació de la seguretat de les dades personals" com:

> *"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."*

Així, entenem que una violació de la seguretat de les dades personals es produeix quan les dades personals que tracta un responsable o encarregat de tractament pateixen un incident de seguretat que dona lloc a la violació de la confidencialitat, disponibilitat o integritat de les dades. Si això passa, i és possible que la violació posi en risc els drets i les llibertats d'una persona, tal com preveu l'article 36 de la LQPD, el responsable de tractament ha de notificar-ho a l'autoritat de control sense demora i a tot estirar 72 hores després de tenir-ne constància. Si la notificació no es produeix en aquest termini, s'han de justificar els motius de la dilació. Si és un encarregat del tractament, haurà de notificar cada violació de la seguretat de les dades al responsable del tractament.

D'altra banda, tal com es preveu a l'article 15 de la LQPD, si la violació de la seguretat de les dades suposa un alt risc per a les persones afectades,

aquestes també hauran de ser informades tan aviat com raonablement sigui possible (llevat que s'hagin aplicat mesures de protecció tècniques i organitzatives efectives, o altres mesures que garanteixin que ja no existeix la probabilitat que es determini el risc).

Tipus de violacions de seguretat (vegeu la Imatge 1)**:**

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

Imatge 1. Tipus de violacions de seguretat

3) Protocols interns

3.1. Organització interna en cas de violació de seguretat de protecció de dades

Abans de realitzar un tractament, cal avaluar el nivell de risc que suposa per als drets i les llibertats dels usuaris de les dades. Per això, s'han d'implementar les mesures establertes a la LQPD com l'article 27 (Deures i obligacions del responsable del tractament), 28 (Mesures de protecció de dades per defecte i des del disseny), 35 (Mesures de seguretat) i 32 (Avaluacions d'impacte per a la protecció de dades), entre d'altres.

Aquestes mesures van des de garantir la confidencialitat, integritat i disponibilitat, pseudonimització i xifratge de dades personals, fins a processos de verificació, avaluació i valoració regulars; i cal aplicar-les tant per prevenir una violació de seguretat de dades com per reaccionar-hi, en cas que calgui.

S'entén doncs la necessitat d'avaluar l'impacte dels incidents sobre les dades de caràcter personal, ja sigui per la possibilitat que es produeixin accidents, tant humans com naturals, o que es realitzin de forma manual o automatitzada. Es requereix, així mateix, gestionar els errors, debilitats, vulnerabilitats o atacs que sorgeixin a partir d'estratègies de protecció de dades, com ara la pseudonimització i el xifratge de les dades personals, els processos d'anonimització, desvinculació, eliminació, tractaments federats, així com els panells de preferències.

La gestió d'incidents ha de ser una part important de la cultura de responsables i encarregats de tractaments per garantir que es compleixin els requisits de la LQPD. Cal una actualització dels procediments de gestió, per complir amb la notificació de la violació de seguretat a l'APDA i la comunicació als afectats (Articles 36 i 37). Els responsables han d'implementar també estratègies i recursos per detectar i gestionar incidents, i assegurar-se que funcionin correctament. Això permetrà una ràpida reacció a la violació de seguretat de

dades personals i avaluar el risc per als drets i les llibertats de les persones físiques. Els encarregats del tractament han de notificar immediatament les violacions de seguretat patides als responsables, perquè avaluïn el risc i compleixin les seves obligacions.

Un cop detectada i avaluada la violació de seguretat de dades personals, cal portar un registre d'incidents per documentar el procés de resolució amb tota la informació recopilada. Aquesta documentació ha d'incloure detalls de les decisions preses sobre la notificació a l'autoritat competent i la comunicació als afectats (incloent-hi una còpia de la comunicació realitzada). No hi ha un model de registre estàndard, cada organització ha d'utilitzar el que consideri més apropiat.

3.2. Actors implicats

S'ha detectat una violació de seguretat de dades personals a l'organització. Per garantir una correcta i eficaç gestió, cal la col·laboració de diversos membres. Abans que cada un pugui actuar de manera eficaç, cal establir els procediments i organitzar-ne els recursos necessaris.

A continuació, s'expliquen breument les funcions i les responsabilitats dels membres involucrats:

3.2. a) Responsable de tractament

Li correspon aplicar les mesures tècniques i organitzatives apropiades per tal de garantir i poder demostrar que el tractament és conforme a la LQPD. Si escau, haurà de garantir que es notifica la violació de seguretat de dades personals a l'autoritat competent sense dilació indeguda, i també que es comunicarà la violació de seguretat de dades personals als afectats quan sigui necessari.

El responsable de tractament haurà de comptar amb l'assessorament del delegat de protecció de dades quan hagi estat designat, o, si no, podrà disposar de l'assessorament d'equips interns o externs experts en protecció de dades.

Igualment, podrà comptar amb l'assessorament d'experts en matèria de seguretat, com el CISO de l'organització, o els serveis informàtics propis o que pugui tenir subcontractats. Així mateix, podrà delegar la gestió de la violació de seguretat de dades personals als encarregats de tractament, com ara serveis informàtics aliens.

El responsable pot delegar a l'encarregat la gestió de la violació de seguretat de dades personals, tant pel que fa a la resposta com pel que fa a la notificació; ara bé, cal documentar aquesta delegació de funcions en el context de la relació contractual establerta. No obstant això, el responsable ha d'assegurar-se que s'estan prenent les accions de resposta, notificació i comunicació oportunes, atès que la delegació de funcions no implica delegació de responsabilitat.

3.2. b) Encarregat de tractament

L'encarregat de tractament ha d'informar, sense dilació indeguda, el responsable de tractament sobre qualsevol violació de seguretat de dades personals que afectin els tractaments encarregats, a més de les obligacions addicionals adquirides en virtut del contracte d'encàrrec. La LQPD exigeix que la informació sigui transmesa sense retard; així mateix, l'encarregat ha de donar suport al responsable per garantir el compliment de les obligacions descrites a la LQPD, incloent-hi la gestió, notificació i comunicació de les violacions de seguretat de dades personals. La informació lliurada al responsable ha de contenir els detalls necessaris perquè compleixi les seves obligacions, concretament avaluar el risc de la violació de seguretat i notificar-ho a l'APDA o comunicar-ho als afectats.

3.2. c) Delegat de Protecció de Dades (DPD)

En els casos en què s'hagi designat un DPD (sigui per exigència de la LQPD o per decisió del responsable/encarregat), exercirà un paper rellevant en la gestió de violacions de seguretat. La LQPD atorga al DPD la tasca d'informar i assessorar el responsable o encarregat de tractament sobre les seves obligacions, incloent-hi la gestió i notificació de violacions de seguretat de dades personals, així com cooperar amb l'Autoritat de Control i actuar com a punt de contacte per a assumptes relacionats amb el tractament.

Per tant, el DPD haurà d'informar i assessorar el responsable/encarregat sobre:

- La implantació d'un procés de gestió de violacions de seguretat de dades personals a l'organització.
- L'avaluació del risc i les conseqüències que pot tenir una violació de seguretat de dades personals per als drets i les llibertats de les persones afectades.
- Les accions adequades per mitigar els efectes de la violació de seguretat de dades personals sobre les persones afectades.
- La necessitat de notificar la violació de seguretat de dades personals a l'APDA i, si escau, als interessats afectats.
- En cas d'encarregats de tractament, la necessitat de notificar la violació de seguretat de dades personals al responsable.

El DPD també actuarà com a punt de contacte amb l'APDA en el procés de notificació per part del responsable de les violacions de seguretat de dades personals, així com en les respostes als requeriments de dita autoritat relacionats amb aquestes, d'acord amb el procés de gestió de violacions de seguretat implantat a l'organització.

El responsable i encarregat de tractament han de proveir el DPD dels mitjans i la informació necessària per al compliment de les seves obligacions.

Cal establir un procediment per notificar-ho a l'APDA i un altre per comunicar-ho als afectats en cas de violacions de seguretat de dades personals. Aquests procediments haurien d'estar definits abans que es produeixi una violació de seguretat, i poden estar integrats dins dels procediments de gestió d'incidents de seguretat de l'organització.

4) Notificació a l'Agència Andorrana de Protecció de Dades

Quan el responsable de tractament notifica una violació de seguretat a l'autoritat de control, l'article 36 de la LQPD, estableix que com a mínim, ha de:

- Descriure la naturalesa de la violació de la seguretat de les dades personals, incloent-hi, si és possible, les categories i el nombre aproximat de persones interessades afectades, i les categories i el nombre aproximat de registres de dades personals afectats.
- Comunicar el nom i les dades de contacte del delegat de protecció de dades o d'un altre punt de contacte on es pot obtenir més informació.
- Descriure les possibles conseqüències de la violació de la seguretat de les dades personals.
- Descriure les mesures adoptades o proposades pel responsable del tractament per fer front a la violació de la seguretat de les dades personals, incloses, si escau, les mesures adoptades per mitigar-ne els possibles efectes negatius.

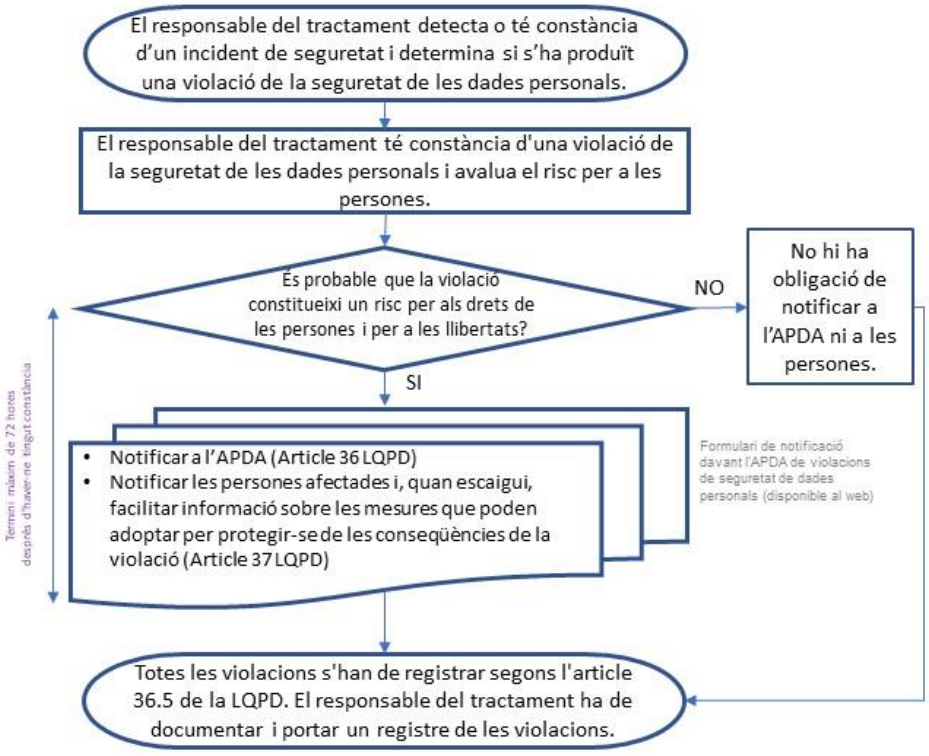
Per facilitar el compliment d'aquests requisits en el contingut de les notificacions de violacions de seguretat, l'APDA posarà a disposició dels responsables de tractament un formulari estandarditzat de notificació. En tot cas, l'APDA podrà requerir al responsable tota la informació addicional necessària.

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

- El caràcter de la notificació.
- Informació general sobre el tractament.
- Intencionalitat i origen.
- Tipologia de la violació de seguretat (si afecta la confidencialitat, la disponibilitat o la integritat).
- Categoria de dades i perfil dels afectats.

- Conseqüències.
- Resum de la violació de seguretat.
- Implicacions transfrontereres.
- Informació temporal de la violació de seguretat i mitjans de detecció.
- Mesures de seguretat abans de l'incident.
- Accions preses.
- Comunicació als afectats.
- Identificació dels intervinents.
- Documentació adjunta a la notificació.

A la Imatge 2, es presenta un diagrama de flux que mostra els requisits de notificació.



Imatge 2. Diagrama de flux- Requisits de la notificació de violació de seguretat de dades personals

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

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

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

L'objectiu de la notificació de violacions de seguretat de dades personals és establir un criteri comú per a totes les activitats de tractament de dades personals realitzades per una organització, i comptar amb els mitjans adequats per avisar en el termini establert. Aquesta notificació no s'adreça a tercers, ni a ciutadans afectats per una violació de seguretat de dades personals.

4.1. Qui ha de notificar-ho?

Si la constància d'una violació de seguretat de dades personals comporta un risc per als drets i les llibertats de les persones físiques, el responsable del

tractament ho ha de notificar davant l'APDA d'acord amb l'article 36 de la LQPD.

El responsable pot delegar aquesta notificació a un representant, persona física o entitat autoritzada amb aquesta finalitat.

Si el responsable de tractament fa ús d'encarregats, al contracte ha de quedar reflectit qui ha de realitzar les notificacions, a partir de criteris establerts (dades afectades, interessades, mesures de seguretat, accions preses, etc.). El responsable ha de prendre les precaucions adequades per seleccionar els encarregats de tractament que siguin capaços de brindar el suport necessari per gestionar les violacions de seguretat de dades personals.

En cas que una violació de seguretat d'un encarregat de tractament afecti més d'un responsable, l'encarregat de tractament haurà d'informar en el termini establert cadascun dels responsables afectats per tal que puguin fer la notificació a l'APDA.

4.2. Què cal fer postcomunicació?

Un cop notificada una violació de seguretat de dades personals a l'APDA, el responsable de tractament ha d'estar preparat per rebre i atendre els requeriments, les ordres o les comunicacions relacionades amb la violació de seguretat notificada que l'Agència li pugui enviar. Per això, ha de comptar amb els mitjans tècnics necessaris per tenir accés ràpid i àgil a aquestes comunicacions.

Un cop s'ha realitzat l'enviament de la notificació de la violació de seguretat de dades personals, s'entendrà que ha tingut efectes en la data d'enviament del formulari de notificació.

El responsable de tractament pot rebre per part de l'APDA diverses comunicacions o notificacions, com ara informació relativa al registre d'entrada

de la violació de seguretat de dades personals notificada, un requeriment d'informació addicional, una ordre per comunicar als afectats la violació de seguretat de dades personals, etc.

4.3. Contingut de la notificació

En els apartats següents es detalla la informació rellevant per a la notificació de violacions de seguretat de dades personals al formulari de l'APDA.

4.3. a) Caràcter de la notificació

A través del formulari disponible al web de l'APDA (annex 1) es poden realitzar tres tipus de notificacions de violació de seguretat de dades personals:

- Nova notificació completa de violació de seguretat de dades personals: notificar una violació de seguretat de dades personals de què no s'hagi informat prèviament l'APDA. En aquest cas, es tractarà d'una notificació "completa" ja que en el moment de la notificació es disposarà de tota la informació necessària.
- Nova notificació inicial/parcial de violació de seguretat de dades personals: notificar una violació de seguretat de dades personals de què no s'hagi informat prèviament l'APDA. En aquest cas, es tractarà d'una notificació "inicial/parcial" ja que en el moment de la notificació no es disposarà de tota la informació necessària i es preveurà aportar informació addicional.
- Modificació d'una violació de seguretat de dades personals ja notificada: quan s'hagi notificat prèviament una violació de seguretat de dades personals de manera inicial/parcial, en el termini 30 dies es podrà fer una modificació sobre aquesta informació per completar la notificació de la violació de seguretat de dades personals. De manera general, està prevista una única modificació d'una notificació de violació de seguretat

de dades personals realitzada prèviament, i dins el termini de 30 dies des de la notificació inicial.

4.3. b) Informació general sobre el tractament

Aquesta informació té una naturalesa general i fa referència al tractament de les dades personals que han estat compromeses a causa d'una violació de seguretat. També inclou l'estimació del risc inherent al tractament d'aquestes dades, la qual cosa és una informació fonamental que el responsable de tractament ha de conèixer amb antelació. Es tracta de:

- La durada del tractament, cal distingir entre tractaments puntuals i tractaments de llarga durada.
- Nombre total de persones afectades per la violació de seguretat de dades personals.
- Àmbit geogràfic del tractament, si es fa sobre persones únicament d'Andorra o a escala internacional.

4.3. c) Intencionalitat i origen

Intencionalitat de l'incident que ha causat la violació de seguretat de dades personals:

- Intencionalitat desconeguda, com per exemple, un ciberdelinqüent accedeix de manera no autoritzada en una base de dades d'una entitat per robar i utilitzar indegudament la informació personal dels clients.
- Intencionat per danyar el responsable, l'encarregat o les persones afectades, com per exemple, un treballador molest que decideix vendre les dades personals dels clients de l'empresa a un competidor directe, amb l'objectiu de causar danys a l'empresa i a les persones afectades.

- Accidental o fortuït (sense intencionalitat), com per exemple, quan un treballador envia per error un correu electrònic amb informació confidencial dels clients a una persona no autoritzada.

Origen o àmbit de l'incident:

- Intern: personal o sistemes sota el control del responsable de tractament, com per exemple, l'enviament de dades personals a un encarregat de tractament incorrecte o pèrdua de dispositiu.
- Intern: personal o sistemes sota control de l'encarregat de tractament, com per exemple, l'enviament de documentació a destinataris incorrectes, incidència tècnica en sistemes d'informació.
- Extern: altres, aliens al responsable i a l'encarregat de tractament, com per exemple, un ciberatac o robatori de dispositius.

És necessari identificar els esdeveniments que han originat la violació de seguretat de dades personals, independentment de les seves conseqüències i la tipologia, per tal de determinar-ne les causes, avaluar les repercussions de la violació i prendre mesures per prevenir esdeveniments similars.

En el formulari de notificació de violacions de seguretat de dades personals s'inclouen els incidents següents:

- Revelació verbal no autoritzada.
- Documentació o dispositiu perdut, robat o dipositat en una localització insegura.
- Correu postal perdut o obert.
- Eliminació incorrecta de dades personals en format paper.
- Dades personals enviades per error (postal o electrònicament).
- Dades personals residuals en dispositius obsolets.
- Dades personals eliminades o destruïdes.
- Abús de privilegis d'accés per part d'un treballador per a extreure, reenviar o copiar dades personals.

- Dades personals mostrades a l'individu incorrecte.
- Publicació no intencionada o no autoritzada.
- Enviament d'email a múltiples destinataris sense còpia oculta o en una llista de distribució.
- Ciberincidents.
- Incidència tècnica.
- Modificació no autoritzada de dades.

4.3. d) Tipologia

Un dels paràmetres més importants a l'hora d'avaluar el nivell de risc d'una violació de seguretat de dades personals és determinar-ne amb exactitud la tipologia, és a dir, concretar a quina dimensió de seguretat de les dades personals ha afectat la violació. Aquestes dimensions són la confidencialitat, disponibilitat i integritat. És important considerar que una mateixa violació de seguretat de dades personals pot afectar més d'una dimensió, depenent de les circumstàncies particulars en cada cas.

- Confidencialitat: revelació no autoritzada o accidental de les dades personals, o l' accés.
- Disponibilitat: pèrdua d'accés accidental o no autoritzat a les dades personals, o la destrucció.
- Integritat: una alteració no autoritzada o accidental de les dades personals.

Confidencialitat: una violació de seguretat de dades personals afecta la confidencialitat quan les dades personals d'un tractament han pogut ser accedides per tercers sense permís, incloent-hi quan les dades són exfiltrades[1].

1 "Dades exfiltrades" fa referència a l'acció d'extreure o treure dades d'un sistema o xarxa sense autorització. Aquest terme s'utilitza habitualment en l'àmbit de la ciberseguretat per descriure el procés en què un atacant accedeix i copia dades confidencials d'una organització o individu, i les porta fora de l'entorn de seguretat on es troben. L'exfiltració de dades pot ocórrer de diverses formes, com ara a través de transferències electròniques, correu electrònic, dispositius

Això inclou, per exemple, els casos d'intrusió en sistema d'informació amb accés o exfiltració de dades personals, l'enviament de dades personals per error, la pèrdua de dispositius o documentació amb dades personals, codi maliciós de programari de segrest

És crucial verificar si les dades personals afectades estaven adequadament encriptades, anonimitzades o protegides per garantir que siguin inintel·ligibles per a aquells que van tenir o puguin tenir accés a aquestes dades en el futur. En cas afirmatiu, les conseqüències de la violació de confidencialitat es veurien en gran part mitigades, reduint o fins i tot anul·lant els riscos associats a l'incident.

Per exemple, en una situació en què s'ha produït una fallada de confidencialitat a causa de la pèrdua o el robatori d'ordinadors portàtils que tenen el seu disc dur encriptat amb un algorisme no compromès i l'accés a l'equip està protegit per una contrasenya forta i difícil d'endevinar, es pot considerar que els riscos associats a la pèrdua de confidencialitat de les dades estan adequadament mitigats. Aquestes mesures de seguretat addicionals garanteixen que tercers que tinguin accés als dispositius no puguin llegir la informació confidencial, salvaguardant així la privadesa de les dades implicades.

Disponibilitat: una violació de seguretat de les dades personals impacta en la disponibilitat quan aquestes dades es tornen temporalment o permanentment inaccessibles per a aquells que tenen el legítim dret de tractar-les o accedir-hi. Aquesta situació pot ser el resultat d'incidents que afecten les mateixes dades personals o els sistemes utilitzats per gestionar-les. Per exemple, inclou casos de xifrat de les dades personals o dels sistemes d'informació causat per malware de tipus ransomware (programari de segrest maliciós), pèrdua de documentació en paper que conté dades personals o la incapacitat d'accedir a

d'emmagatzematge extraïbles o altres mitjans. Les dades exfiltrades poden incloure informació personal, secrets comercials, dades financeres, contrasenyes o altres tipus d'informació sensible. Aquesta activitat és realitzada sovint per ciberdelinqüents amb l'objectiu de robar informació valuosa o comprometre la privacitat i seguretat d'una organització o individu. L'exfiltració de dades és una violació greu de la seguretat i pot tenir conseqüències importants per a les parts afectades.

un dispositiu d'emmagatzematge de dades (sigui físic o lògic). Aquests incidents limiten la disponibilitat de les dades personals i poden causar interrupcions significatives en les activitats quotidianes i en els processos de tractament de les dades.

Per al responsable del tractament, és essencial determinar si s'ha aconseguit restaurar o si es troba en procés de restauració la disponibilitat de les dades. Aquesta recuperació és fonamental per mitigar els danys que pot causar aquest tipus de violacions de dades personals. Amb aquest objectiu, els responsables de tractament han d'establir les estratègies i els procediments adequats per afrontar aquestes situacions, que inclouen la realització de còpies de seguretat, plans de resposta a incidents i estratègies de governança de les dades. A través d'aquestes mesures, s'assegura la disponibilitat i la continuïtat de les operacions de tractament de les dades personals, cosa que redueix al màxim els impactes negatius que puguin derivar-se d'aquests esdeveniments.

Integritat: una vulneració afecta la integritat quan les dades personals han estat il·legítimament alterades i el tractament d'aquestes dades pot causar danys als afectats. Per exemple, un tercer ha modificat la informació relacionada amb les dades bancàries dels empleats a la base de dades de l'organització, que s'utilitzen per al pagament de les nòmines, o un alumne ha modificat les qualificacions a la base de dades d'un centre educatiu.

En cas de produir-se vulneracions de dades personals en relació amb la integritat, el responsable ha de determinar si el tractament de les dades alterades il·legítimament pot causar algun dany als afectats i, si s'escau, si aquest dany es pot revertir.

4.3. e) Categories de dades i perfil dels afectats

Davant d'una violació de seguretat de dades personals, el responsable de tractament ha de ser capaç de determinar amb precisió les categories de dades personals afectades, el nombre de persones afectades i el perfil. Aquests tres

paràmetres són fonamentals per poder determinar el nivell de risc per als afectats.

Quant a les categories de dades personals afectades, a la notificació a l'APDA es consideren les següents:

Categoria de dades	Exemples
Dades bàsiques	Nom, cognoms o la data de naixement dels afectats.
Dades de contacte	Número de telèfon, adreça electrònica, o adreça postal de les persones.
Fotografies o vídeos	Imatges individuals o col·lectives de les persones afectades.
Document d'identitat, passaport o qualsevol altre document identificatiu	Carnet de la Caixa Andorrana de Seguretat Social, DNI, carnet de residència, etc.
Dades econòmiques o financeres	Dades referents a nòmines, extractes bancaris, qualsevol informació que pugui revelar informació econòmica dels afectats.
Dades de localització/geolocalització (dades d'ubicació de la persona en un determinat moment o durant un període de temps)	Dades de posicionament, coordenades o direccions habituals (de no residència) dels afectats.
Dades de mitjans de pagament	Número de la targeta bancària o compte bancari, mitjans de pagament en línia, etc.
Credencials d'accés o identificació	Noms d'usuaris, contrasenyes, dades com targetes de coordenades, o segons factors d'autenticació.
Dades de perfils	Perfils d'usuaris en xarxes socials o dades de perfilat psicosocial o que permetin realitzar

	perfilats de persones físiques.
Sobre la vida sexual	Dades relatives a la salut sexual, hàbits, orientació o tendències sexuals, així com informació que permeti inferir-la.
Sobre religió o creences	Religió dels afectats, així com informació sobre postures religioses, agnòstiques o atees.
Sobre origen racial o ètnic	Informació que reflecteixi o permeti establir l'origen racial o la pertinença a una determinada ètnia dels afectats.
Sobre dades de salut	Història clínica, dades de salut de treballadors, de pacients, etc.
Sobre opinió política	Informació que reflecteixi o permeti esbrinar l'opinió o tendències polítiques dels afectats.
Dades genètiques	Característiques genètiques heretades o adquirides d'una persona física que proporcionin una informació única sobre la fisiologia o la salut d'aquella persona, obtingudes en particular de l'anàlisi d'una mostra biològica.
Dades sobre condemnes i infraccions penals	Certificats d'antecedents penals, etc.
Dades biomètriques	Característiques físiques, fisiològiques o conductuals d'una persona física, que en permetin la identificació.
Sobre afiliació sindical	Informen sobre la pertinença o afiliació d'una persona a un sindicat.

En termes d'afectats, i referit exclusivament a persones físiques, no computen com a tal les que són persones jurídiques, siguin clients, proveïdors o qualsevol altra relació que hi pugui mantenir el responsable de tractaments. S'han de tenir en compte els perfils següents:

- Menors o persones amb discapacitat.
- Membres de col·lectius vulnerables o en risc d'exclusió.
- Persones amb perfils concrets: clients/ciutadans, estudiants/alumnes, usuaris, pacients, subscriptors/potencials clients, afiliats/associats, policies, treballadors o altres.

En tots els casos, cal afegir el nombre total de persones que han vist afectades les seves dades per la violació de seguretat o, en cas de desconèixer-se, indicar-ne una xifra aproximada.

4.3. f) Implicacions transfrontereres

Cal indicar si la violació de la seguretat inclou implicacions transfrontereres i, en cas afirmatiu, especificar-ne els països afectats.

4.3. g) Informació temporal de la violació de seguretat

En cas de conèixer la data en què va tenir lloc la violació, s'ha d'indicar exactament. La detecció pot ser mitjançant els mètodes següents:

- Mitjans de detecció implementats proactivament pel responsable o encarregat.
- L'advertència d'algun membre de l'organització del responsable o encarregat.
- Comunicació d'algun afectat.
- Algun mitjà de comunicació.
- Un tercer aliè.
- Altres.

4.3. h) Mesures de seguretat abans de la violació

A l'hora de denunciar una violació de la seguretat, s'han d'indicar les mesures emprades prèviament a l'incident amb la possibilitat de poder-les demostrar, si així ho requereix l'Agència. D'aquesta manera, també s'haurà de reconèixer si la violació es podria haver evitat o no si s'hagués adoptat alguna mesura addicional; si s'ha produït per una fallada, deficiència o incompliment de les mesures implementades i si es disposa d'una anàlisi de riscos documentada que justifiqui les mesures de seguretat adoptades prèviament a l'incident. Aquestes mesures són:

- Política de protecció de dades i seguretat.
- Formació en protecció de dades i seguretat de nivell adequat.
- Sistemes informàtics actualitzats.
- Registre d'incidents.
- Auditories periòdiques.
- Control d'accés físic.
- Control d'accés lògic.
- Nivell d'accés a les dades.
- Xifrat de les dades.
- Còpia de seguretat.
- Anonimització.
- Cap de les anteriors.

4.3. i) Accions preses després de l'incident

Un cop constatada la violació de la seguretat, també caldrà indicar si s'ha actualitzat el registre d'incidents, si s'han adoptat noves mesures per evitar una nova violació i si s'han millorat els procediments i polítiques de seguretat. Així mateix, s'haurà de comunicar si s'ha posat en coneixement de les autoritats policials o judicials, si el responsable creu que, malgrat tot, s'havien pres totes

les mesures escaients possibles i la data en la qual va quedar resolta la violació. Les mesures de protecció són les mateixes que les referides a l'apartat 4.3. h).

4.3. j) Comunicació als afectats

La comunicació de la violació de seguretat als afectats ha de ser en un llenguatge clar i senzill i ha d'incloure els detalls d'allò que ha succeït; així com les dades de contacte on dirigir-se per obtenir més informació, les possibles conseqüències de la violació de la seguretat per a ells, les mesures adoptades per resoldre-la i les mesures adoptades i proposades per minimitzar-ne l'impacte negatiu. El formulari ha d'incloure la data en què s'ha notificat la violació, i quan es té previst comunicar-ho, el nombre de persones a les quals s'informa i la via de comunicació prevista: telefònica o verbal; postal, email, SMS o similar; comunicat públic o a través del web corporatiu; difusió en mitjans de comunicació.

En cas que les persones afectades no siguin informades, s'haurà de justificar segons els motius següents:

- No existeix un risc per als seus drets i llibertats.
- El dany reputacional per a l'organització seria molt elevat.
- No interferir en una investigació policial/judicial en curs.
- No hi ha cap acció que es pugui portar a terme per mitigar els danys.
- La comunicació exigeix un esforç excessiu.
- Altres (s'han d'indicar).

4.3. k) Documentació adjunta

Tot i que no és necessari adjuntar més documentació més enllà de les dades sol·licitades en el formulari, l'Agència podrà requerir la informació addicional

que consideri oportuna. En cas d'adjuntar-se per voluntat pròpia, cal especificar-ho marcant la casella corresponent.

4.3. l) Notificació completa o per fases

Finalment, caldrà que el responsable indiqui si la notificació conté tota la informació que ha pogut aconseguir respecte a la violació de la seguretat i, per tant, es pot considerar completa i no es preveu aportar-ne més; o bé si la notificació és inicial i en un període màxim de 30 dies es notificarà informació addicional. En cas contrari, l'autoritat de control considerarà la notificació completa.

5) Comunicació als afectats

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

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

5.1. Quan cal comunicar-ho?

D'acord amb l'article 37 de la LQPD, el responsable de tractament ha de comunicar sense demora indeguda qualsevol violació de seguretat de dades personals als afectats quan hi hagi un risc alt per als seus drets i llibertats. Per tant, haurà d'avaluar el risc un cop tingui constància de la violació de seguretat per determinar si cal notificar-la. En cas que s'estableixi un risc alt, la comunicació s'ha de fer immediatament.

Alguns factors a tenir en compte per determinar si s'ha de fer la notificació són: les obligacions legals i contractuals; els possibles riscos de què derivin la pèrdua de confidencialitat, integritat o disponibilitat de les dades personals; així com els possibles danys físics, danys reputacionals, fraus, etc. També cal tenir en compte si els danys són irreversibles, es poden prevenir o mitigar, així com la possibilitat de prendre mesures de protecció per atenuar l'impacte.

Si el responsable de tractament ha pres prèviament mesures tècniques i organitzatives que eviten els riscos, minimitzen els danys als drets i a les llibertats o els fan reversibles; o bé ha pres mesures de protecció amb posterioritat a la violació de seguretat per mitigar l'impacte i garantir que ja no hi

ha possibilitat que es materialitzi l'alt risc per als drets i les llibertats, aleshores no serà necessària la comunicació als afectats.

Si el responsable encara no ha notificat una violació de seguretat de dades personals amb alt risc potencial, en el moment de notificar-ho a l'APDA, aquesta pot exigir-li que faci la comunicació als afectats, o bé que demostri que compleix alguna de les condicions perquè la comunicació als afectats no sigui obligatòria.

5.2. Terminis per comunicar-ho

La LQPD no estableix un termini fix per informar els interessats sobre una violació de les seves dades, però requereix que es faci sense dilació indeguda. Qualsevol demora en la comunicació pot tenir el mateix efecte que no fer-la, per tant, qualsevol retard s'haurà de justificar. Si és resultat d'una ordre de l'APDA, s'ha de fer sense dilació indeguda i s'ha de comunicar la confirmació que s'ha complert en dels 30 dies acordats, llevat que s'estableixi un termini diferent a l'ordre.

5.3. Qui ho ha de comunicar?

D'acord amb l'article 37 de la LQPD, la responsabilitat d'informar les persones afectades sobre una violació de seguretat de dades personals recau sobre el responsable del tractament.

El responsable de tractament és l'únic que pren la decisió sobre si cal notificar la violació de seguretat als afectats.

5.4. Com i què cal comunicar?

D'acord amb l'article 37 de la LQPD, la comunicació a les persones afectades per una violació de la seguretat de dades personals ha de contenir informació

clara i senzilla sobre la naturalesa de la violació i els possibles danys que pugui ocasionar.

A més, ha d'incloure el contingut mínim establert a l'article 36.3, lletres (b), (c) i (d) de la LQPD. Això inclou les dades de contacte del Delegat de Protecció de Dades o el punt de contacte, una descripció general de l'incident i del moment en què es va produir, les possibles conseqüències de la violació de seguretat de dades personals, una descripció de les dades i la informació afectades, un resum de les mesures implantades fins ara per controlar possibles danys i qualsevol altra informació útil perquè els afectats puguin protegir les seves dades.

La comunicació es realitzarà de forma directa a l'interessat, per telèfon, correu electrònic, SMS, correu postal o qualsevol altre mitjà adreçat a l'afectat que el responsable consideri adient.

Si l'esforç que suposa contactar amb els afectats és desproporcionat amb relació als riscos per als drets i les llibertats que estan patint els interessats, es podrà procedir a una comunicació indirecta a través d'avisos públics com blocs corporatius o comunicats de premsa. Això últim també pot passar quan no és possible contactar amb les persones afectades, per exemple, perquè hi ha una pèrdua de dades i impossibilitat per recuperar-les o es desconeixen les dades de contacte. En aquests casos, l'avís públic ha d'ocupar un lloc destacat, de manera que sigui visible.

La comunicació ha de ser completa i de fàcil accés, dirigida específicament a aquelles persones per a les quals hi hagi un risc alt que els seus drets i llibertats es puguin veure danyats. Una comunicació incompleta, de difícil accés o realitzada a les persones incorrectes es considerarà no realitzada.

6) Règim sancionador

En el món actual basat en dades, l'absència de protocols adequats per a la protecció de dades pot exposar les organitzacions a riscos importants. Els protocols insuficients no només comprometen la informació sensible, sinó que també deixen les organitzacions vulnerables a les repercussions legals i normatives. Aquest article explora les possibles sancions que es poden imposar a les organitzacions que no tenen protocols sòlids i destaca la importància d'implementar mesures integrals de protecció de dades.

6.1. Sancions econòmiques

La violació de seguretat en dades personals és un fet que pot generar el perfeccionament de tipus sancionadors regulats tant a la normativa de protecció de dades, com a normatives específiques d'aplicació. Determinades indústries, com ara la sanitat i les finances, tenen marcs reguladors addicionals per protegir les dades sensibles.

L'incompliment d'aquesta normativa a causa de l'absència de protocols adequats pot comportar sancions greus, pèrdua de llicències i danys a la reputació.

A la normativa andorrana trobem el següent:

Precepte	Sanció
Article 72.1. Són infraccions considerades molt greus: a) El tractament de dades personals que vulneri l'article 5 de la LQPD. *Article. 5.2. Les dades personals han de ser: (...) f) Tractades de manera que se'n garanteixi una seguretat adequada, inclosa la protecció contra el tractament no*	Entre 30.001 euros i 100.000 euros (article 73.1 LQPD).

autoritzat o il·lícit i contra la seva pèrdua, destrucció o dany accidental, mitjançant l'aplicació de les mesures tècniques i organitzatives adequades ("integritat i confidencialitat").	
Article 72.2. Són infraccions considerades greus: e) L'incompliment dels deures de notificació o de comunicació d'una violació de la seguretat de les dades personals.	Entre 15.001 euros i 30.000 euros (article 73.2 LQPD).
Article 72.3. Són infraccions considerades lleus: i) La notificació incompleta, tardana o defectuosa a l'autoritat de protecció de dades de la informació relacionada amb una violació de seguretat de les dades personals. j) L'incompliment de l'obligació de documentar qualsevol violació de seguretat.	Entre 500 euros i 15.000 euros (article 73.3 LQPD).

En el cas de concórrer dos o més infraccions molt greus tipificades a la LQPD, les sancions econòmiques poden incrementar-se fins al 2% de la facturació global anual de la companyia.

A part de les multes, també cal tenir en compte que el responsable de tractament pot haver de fer front a altres conseqüències econòmiques. Per exemple, les víctimes d'una violació de dades poden iniciar accions legals contra organitzacions per demanar una indemnització pels danys.

6.2. Altres tipus de danys: el dany a la reputació

En el món interconnectat actual, les violacions de seguretat de dades personals s'han convertit en una preocupació important per a les organitzacions. Més enllà de les repercussions econòmiques immediates, les violacions de seguretat de dades poden causar danys reputacionals greus que poden ser especialment pronunciats a països més petits com Andorra.

6.2. a) Pèrdua de confiança

Les violacions de seguretat de dades derivades de l'absència de protocols de seguretat sòlids poden erosionar la confiança dels clients i dels interessats. A Andorra, on la població és relativament petita, l'impacte de les ruptures de confiança és més pronunciat encara. Les notícies es difonen ràpidament dins d'aquestes comunitats i la publicitat negativa que envolta les violacions de seguretat de dades pot soscavar la reputació d'una organització al país. Els interessats poden qüestionar la capacitat dels responsables de tractament o encarregats per protegir la seva informació personal, la qual cosa pot comportar, entre d'altres, la pèrdua d'oportunitats de negoci. Mantenir la confiança és crucial en un mercat més petit com Andorra, on la fidelització dels clients i les recomanacions del boca-orella són primordials.

6.2. b) Impacte en el valor de la marca

La situació única d'Andorra requereix una millor comprensió de l'impacte de les violacions de seguretat de dades en el valor de la marca. A mesura que els clients es tornen cada cop més sensibles a les preocupacions de privadesa i seguretat de les dades, la reputació d'una organització en aquestes àrees esdevé un factor diferencial crucial. En un mercat petit com Andorra, on els consumidors tenen opcions

limitades, una bona reputació de marca és essencial per mantenir una posició competitiva.

6.2. c) Abordar els danys a la reputació

La mitigació dels danys a la reputació després d'una violació de dades és primordial per a les organitzacions que operen a Andorra. La implementació de protocols de seguretat sòlids, la realització d'avaluacions de riscos periòdiques i la inversió en mesures de protecció de dades són passos crucials per prevenir les infraccions. Les estratègies de comunicació proactives, inclosa la divulgació oportuna i transparent de les infraccions, poden ajudar a mantenir la confiança i demostrar la responsabilitat. Les organitzacions també haurien de prioritzar la creació de relacions sòlides amb els interessats, el foment de línies de comunicació obertes i la garantia sobre les mesures de seguretat de les dades vigents.

Les violacions de seguretat de dades personals no només representen doncs amenaces econòmiques, sinó també importants danys a la reputació, especialment en països més petits com Andorra.

En reconèixer les possibles conseqüències de les violacions sobre la confiança, la reputació i el valor de la marca, les organitzacions andorranes poden prendre mesures proactives per prevenir les infraccions i gestionar-les eficaçment, salvaguardant, en definitiva, el seu èxit a llarg termini al mercat.

7) Mesures ex post: seguiment i mesures correctives

7.1. Prevenció proactiva

Les violacions de seguretat de dades personals suposen una amenaça important per a les organitzacions, independentment de la seva naturalesa, mida o sector. Per salvaguardar la informació confidencial i mantenir la confiança dels clients, és essencial que les entitats desenvolupin estratègies internes sòlides per prevenir les violacions de dades.

A més, fomentar una cultura de conscienciació sobre la violació de dades entre els empleats és crucial per mitigar-ne els riscos.

El primer aspecte d'una estratègia interna és la prevenció proactiva. Això implica implementar mesures de seguretat integrals i bones pràctiques per minimitzar el risc de violacions de dades. Els elements clau inclouen:

- **Infraestructura informàtica sòlida** → utilitzant tecnologies de xifratge d'última generació, tallafocs segurs i sistemes de detecció d'intrusions per protegir les xarxes i les dades sensibles de l'accés no autoritzat.
- **Controls d'accés** → implementació de controls d'accés estrictes, mecanismes d'autenticació i permisos basats en rols per limitar l'accés a les dades només al personal autoritzat.
- **Auditories de seguretat periòdiques** → realització d'auditories de seguretat periòdiques per identificar vulnerabilitats, llacunes en els protocols de seguretat i possibles punts d'entrada per als pirates informàtics. La solució ràpida dels problemes identificats és crucial.

7.2. Resposta i correcció d'incidències

Malgrat les mesures preventives, el risc que es produeixin violacions de seguretat sempre existeix. Una estratègia interna eficaç hauria d'incloure protocols de resposta a incidents ben definits. Les consideracions clau inclouen:

- **Resposta ràpida** → establir un equip dedicat de resposta a incidents que pugui identificar i respondre ràpidament a les violacions. Aquest equip hauria de seguir un pla de resposta a incidents predefinit per mitigar els danys causats per l'incompliment.
- **Investigació forense** → realització d'investigacions exhaustives per determinar l'origen, l'abast i l'impacte de la violació. Això inclou identificar dades compromeses, avaluar les vulnerabilitats potencials i preservar les proves amb finalitats legals i reguladores.
- **Correcció i recuperació** → prendre accions immediates per contenir la violació, restaurar els sistemes i evitar més accessos no autoritzats. Implementar mesures com ara aplicar pedaços a vulnerabilitats, actualitzar els sistemes de seguretat i garantir la integritat de les dades afectades.

7.3. Educació i sensibilització dels treballadors

Els treballadors juguen un paper fonamental en la prevenció de violacions de seguretat de dades personals. Les organitzacions haurien d'invertir en programes d'educació i conscienciació contínua per inculcar una cultura de prevenció de violacions de dades entre la seva plantilla. Els components clau inclouen:

- **Programes de formació** → oferir periòdicament una formació integral sobre les millors pràctiques, polítiques i procediments de seguretat de dades.

- **Exercicis simulats** → Realització d'escenaris simulats de violació, com ara simulacres per provar la resposta dels empleats i millorar-ne la preparació.
- **Comunicació contínua** → establiment de canals per a una comunicació contínua i *feedback* sobre la seguretat de les dades. Això inclou actualitzacions periòdiques sobre amenaces emergents, recordatoris sobre protocols de seguretat i animar els empleats a denunciar qualsevol activitat sospitosa.

Dissenyar estratègies internes per prevenir les violacions de seguretat de dades personals i promoure la consciència dels treballadors és primordial per a les organitzacions de tots els sectors.

Annex 1 – Formulari Notificació de violació de seguretat a l'APDA

Formulari de notificació de violacions de seguretat

Indica de quin tipus de notificació es tracta:

Notificació parcial en un termini de 72 hores després que se n'hagi tingut constància (Aquesta notificació és inicial als efectes del compliment amb el termini de notificació establert en la LQPD, sense dilació indeguda (segons l'article 36.4 de la LQPD) i en el termini màxim de trenta (30) dies, es completarà la notificació aportant informació complementària i documents annexos. En cas contrari, l'autoritat de control considerarà aquesta notificació com a completa).

Modificació d'una notificació parcial (s'aporta informació addicional sense dilació indeguda, a una notificació parcial).

Indicar el núm. registre de carpeta de la notificació: _____ (només omplir els camps on s'aporta informació addicional).

Notificació completa (Aquesta notificació conté tota la informació que com a responsable s'ha pogut recavar respecte a la violació de seguretat. A tots els efectes, l'autoritat de control pot considerar aquesta notificació com a completa i no està previst aportar més informació).

En cas que es derivi d'una notificació parcial, indicar el núm. registre de carpeta de la notificació: _____ (Començar el formulari a partir del camp 4).

1. Responsable de tractament

Raó social: _____

NIA / NRT: _____

Telèfon: _____

Adreça electrònica: _____

Adreça: _____

CP: _____

País: _____

Naturalesa de l'organització: Privada Pública / Parapública

Tipus d'organització:

Treballador per compte propi (menys de 10 treballadors) Petita i mitjana empresa

Gran empresa o multinacional Altres

Sector d'activitat: _____

(Indicar un sector d'activitat segons la classificació d'activitats econòmiques d'Andorra (CAEA-2019)

Agència Andorrana de Protecció de Dades

Formulari de notificació de violacions de seguretat (article 36 de la LQPD)
Per a responsables o encarregats del tractament de dades personals

2. Encarregat de tractament

Hi ha una altra organització implicada en la violació de seguretat? Sí No

En cas de respondre que sí:

Raó social: _____

NRT: _____

Telèfon: _____

Adreça electrònica: _____

Adreça: _____

CP: _____

País: _____

3. Persona de contacte o DPD:

Té el responsable o encarregat designat un Delegat de protecció de dades? Sí No

Nom: _____

NIA /NRT: _____

Telèfon: _____

Adreça electrònica: _____

Adreça: _____

CP: _____

País: _____

4. Sobre el tractament

Quan fa que es realitza el tractament de dades afectat?

Tractament puntual o molt limitat en el temps Menys d'un any

Entre 1 i 5 anys Més de 5 anys

Indicar el nombre aproximat d'afectats per la violació de seguretat: _____

El tractament sobre el qual s'ha produït la violació de seguretat inclou dades de persones:

Únicament d'Andorra A nivell internacional

Si és a nivell internacional, especifiqueu els països afectats:

_____

Pàgina 2 de 10

Agència Andorrana de Protecció de Dades

Formulari de notificació de violacions de seguretat (article 36 de la LQPD)
Per a responsables o encarregats del tractament de dades personals

5. Sobre la violació de seguretat:

Data i hora de la violació de seguretat (si no la coneix exactament, indicar una aproximació):	_____
Data i hora en què el responsable ha tingut el coneixement de la violació de seguretat:	_____

Si s'ha notificat després del termini de 72 hores des que se n'ha tingut constància, justificar el motiu de la dilació :

_____

_____

_____

_____

La violació de seguretat s'ha detectat mitjançant:

Mitjans de detecció implementats pro-activament pel responsable o encarregat	L'advertència d'algun membre de l'organització del responsable o l'encarregat	Comunicació d'algun afectat
Algun mitjà de comunicació	Un tercer aliè	Altres (especificar): _____ _____

6. Naturalesa de la violació de seguretat

L'incident ha estat:

Accidental o sense intencionalitat

Intencionalitat desconeguda

Intencionat, per danyar el responsable, l'encarregat o les persones afectades

L'origen de l'incident ha estat:

Intern: personal o sistemes sota control del **responsable** del tractament

Intern: personal o sistemes sota control de **l'encarregat** de tractament

Extern: altres, aliens al responsable i encarregat de tractament

Pàgina 3 de 10

Formulari de notificació de violacions de seguretat (article 36 de la LQPD)
Per a responsables o encarregats del tractament de dades personals

Com ha ocorregut la violació de seguretat? Es poden indicar vàries opcions:

Revelació verbal no autoritzada	Documentació o dispositiu perdut, robat o dipositat en una localització insegura	Correu postal perdut o obert
Eliminació incorrecta de dades personals en format paper	Dades personals enviades per error (postalment o electrònicament)	Dades personals residuals en dispositius obsolets
Dades personals eliminades / destruïdes	Abús de privilegis d'accés per part d'un treballador per extreure, reenviar o copiar dades personals	Dades personals mostrades a l'individu incorrecte
Publicació no intencionada/autoritzada	Enviament d'e-mail a múltiples destinataris sense còpia oculta/llista de distribució	Ciber-incident: (especificar quin): _____ _____
Incidència tècnica	Modificació no autoritzada de dades	Altres (indicar quin): _____ _____

Com a conseqüència de l'incident, s'ha vist afectada la:

Confidencialitat: persones o organitzacions que no estan autoritzades, o no tenen un propòsit legítim per a accedir a les dades, han pogut accedir i/o extreure-les.

Només en cas de bretxa de confidencialitat, estan les dades xifrades de forma segura, anonimitzades o protegides de forma que són intel·ligibles per a qui hagi pogut tenir accés, o no es pot identificar a les persones?

Sí No Desconegut

Disponibilitat: s'han destruït, perdut o xifrat les dades personals, de forma que no poden ser tractades.

Només en cas de bretxa de disponibilitat, s'ha recuperat la disponibilitat de les dades personals de manera que puguin ser tractades amb normalitat?

Sí No Encara no, però es preveu que es recuperarà aviat

Integritat: s'han alterat les dades personals de manera no autoritzada o accidental.

Només en cas de bretxa d'integritat, seleccioni l'opció més apropiada:

Dades alterades, però sense constància d'ús il·legal o incorrecte	Dades alterades i utilitzades de forma il·legal o incorrecta, **però amb** la possibilitat de revertir/recuperar els danys	Dades alterades i utilitzades de forma il·legal o incorrecta, **sense** possibilitat de revertir/recuperar els danys

Pàgina 4 de 10

Agència Andorrana de Protecció de dades

Formulari de notificació de violacions de seguretat (article 36 de la LQPD)

Per a responsables o encarregats del tractament de dades personals

Resum de la violació de seguretat, descripció de què ha succeït (indicant la possible causa, la ubicació, el tipus d'emmagatzematge i un detall de la cronologia dels esdeveniments):

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Quina probabilitat de constituir un risc per als drets i les llibertats de les persones físiques es considera que la violació de la seguretat de les dades personals pot comportar?

Cap probabilitat	Poques probabilitats	Algunes probabilitats	Moltes probabilitats

7. Perfil de les persones afectades

Referit exclusivament a persones físiques. En termes d'afectats no computen com a tal els que són persones jurídiques, siguin clients, proveïdors o qualsevol altra relació que pugui mantenir el responsable de tractament amb aquests.

Entre les persones afectades, hi ha menors de setze anys?

Sí No Desconegut

Entre les persones afectades, hi ha membres de col·lectius vulnerables o en risc d'exclusió social o persones amb diversitat funcional?

Sí No Desconegut

Quins són els perfils de les persones afectades?

Personal propi	Estudiants/alumnes
Pacients	Subscriptors/clients
Ciutadania	Altres (indicar quin): _____

Pàgina 5 de 10

8. Tipus de dades afectades

Seleccioni els tipus de dades que s'hagin vist afectades, exclusivament de persones físiques, marqui totes les opcions aplicables:

Dades bàsiques (ex: nom, cognoms, data de naixement)	Document d'identitat, passaport o qualsevol altre document identificatiu	Dades de contacte
Imatge (Foto/vídeo)	Dades relatives a infraccions administratives	Sobre condemnes i infraccions penals
Dades de perfils (ex: xarxes socials, solvència, psicològic, etc.)	Credencials d'accés o identificació (usuari i/o contrasenya)	Dades acadèmiques
Sobre la vida sexual	Dades de salut	Sobre afiliació sindical
Sobre origen racial o ètnic	Dades de localització/geolocalització	Dades genètiques
Sobre religió o creença	Sobre opinió política	Biomètriques
Dades econòmiques o financeres (sense mitjans de pagament)	Dades de mitjans de pagament (ex: targeta bancària, etc.)	Altres (especificar) _____ _____

La incidència ha afectat dades:

Actuals Històriques

9. Conseqüències sobre les persones físiques

Quines podrien ser les conseqüències sobre les persones físiques? Es poden indicar diverses opcions.

Usurpació d'identitat	Pèrdua de control sobre les dades personals	Danys psicològics o físics
Ser víctima de campanyes de phishing/spamming	Pèrdues financeres	Danys reputacionals
Pèrdua de la confidencialitat de les dades afectades pel secret professional	Impossibilitat per a accedir a un servei	Impossibilitat d'exercir algun dret
Discriminació	Encara desconegut	Altres (especificar) _____ _____

En data d'aquesta notificació, té constància que s'hagi materialitzat alguna de les conseqüències identificades?

Sí No

Si encara no s'ha materialitzat, com valora la probabilitat que es materialitzi sobre les persones afectades?

Improbable Baixa Alta Molt alta Desconeguda

10. Mesures de seguretat abans de la violació de seguretat

Marqui les mesures de seguretat implementades en l'organització abans de l'incident (haurà de poder acreditar les mesures marcades davant d'un eventual requisit per part de l'Agència):

Polítiques de protecció de dades i seguretat	Formació en protecció de dades i seguretat al nivell adequat	Sistemes informàtics actualitzats
Registre d'incidents	Auditories periòdiques	Control d'accés físic
Control d'accés lògic	Nivells d'accés a les dades	Xifratge de les dades
Còpia de seguretat	Anonimització	Altres (especificar) _____ _____

Es podria haver evitat la violació de seguretat adoptant alguna mesura de seguretat addicional?

Sí No Desconegut

L'incident s'ha produït per una fallada, deficiència o incompliment de les mesures implementades?

Sí No Desconegut

Disposa d'una anàlisi de riscos documentada que justifiqui les mesures de seguretat adoptades prèviament a l'incident?

Sí No

11. Accions preses després de l'incident

Ha actualitzat el registre d'incidents amb la informació d'aquesta violació de seguretat?

Sí No

Ha adoptat després de l'incident noves mesures de seguretat que podrien haver evitat la violació de seguretat?

Sí No

Marqui exclusivament les noves mesures de seguretat o les que s'hagin actualitzat o que s'actualitzaran:

	Indicar si es tracta d'una nova mesura o explicar el detall de l'actualització	Data d'implementació
Polítiques de protecció de dades i seguretat		
Formació en protecció de dades i seguretat al nivell adequat		
Sistemes informàtics actualitzats		
Registre d'incidents		
Auditories periòdiques		
Control d'accés físic		
Control d'accés lògic		
Nivells d'accés a les dades		
Xifratge de les dades		
Còpia de seguretat		
Anonimització		
Altres (especificar)		

Ha posat en coneixement l'incident a les autoritats policials/judicials per considerar que és constitutiu de delicte?

Sí No

Considera que ha pres totes les accions possibles i dona per resolta la violació de seguretat?

Sí No

Indiqui la data en què es va donar per resolta la violació de seguretat:_____

12. Comunicació als afectats

La comunicació de la violació de seguretat als afectats ha de ser en un llenguatge clar i senzill, incloure els detalls de què ha succeït, així com les dades de contacte a on dirigir-se per obtenir més informació, les possibles conseqüències de la violació de seguretat per a ells, les mesures adoptades per resoldre la violació i les mesures adoptades i proposades per minimitzar l'impacte negatiu de la violació.

14. Declaració Jurada i Signatura

El formulari té la consideració de DECLARACIÓ JURADA. Per tant, la persona signant declara que les dades aquí donades són verídiques i que disposa de l'autorització i/o la facultat per a realitzar el següent tràmit.

També declara tenir autorització de representació del responsable per a notificar la violació de seguretat a l'autoritat de control.

Lloc: _____

Data: _____

Signatura:

Clàusula informativa sobre protecció de dades

Les dades de caràcter personal seran tractades per l'Agència Andorrana de Protecció de Dades i incorporades a l'activitat de tractament sobre violacions de seguretat, la finalitat de les quals és la gestió i avaluació de la notificació de violació de seguretat. Aquesta finalitat està basada en el compliment d'obligacions legals que la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals imposa a l'Agència Andorrana de Protecció de Dades. Les dades seran conservades durant el temps necessari per complir amb la finalitat per a la qual s'han demanat i per determinar les possibles responsabilitats que es puguin derivar de la finalitat esmentada i del tractament de les dades. No seran cedides a tercers, tret d'obligació legal. Podeu exercir els vostres drets d'accés, rectificació, supressió i portabilitat de les vostres dades, de limitació i oposició al vostre tractament, així com a no ser objecte de decisions basades únicament en el tractament automatitzat de les seves dades, quan siguin procedents, davant de l'Agència Andorrana de Protecció de Dades, C/ Dr. Vilanova, 15-17 Nova seu del Consell General, planta -5 AD500 Andorra la Vella o a l'adreça de correu electrònic dpd@apda.ad

El present formulari haurà de presentar-se omplert i signat electrònicament mitjançant l'enviament del mateix a l'adreça de correu electrònic apda@apda.ad.

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