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))

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:

_____

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

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

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): _____

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.

S'ha comunicat la violació de seguretat a les persones afectades en els termes anteriorment descrits?

◯ Sí ◯ No, però seran comunicats ◯ No seran informats ◯ Pendent de decidir

Data en què es va comunicar o es té previst comunicar: _____

Nombre de persones comunicades o que es té previst comunicar: _____

Si les persones han estat o estaran informades, amb quin mitjà de comunicació:

☐ Telefònicament

☐ Comunicació dirigida personalment a cada afectat (postal, e-mail, SMS o similar)

☐ Comunicat públic o publicació en web corporatiu

☐ Comunicació dirigida personalment a cada afectat (postal, e-mail, SMS o similar) amb garantia de lliurament i lectura

☐ Difusió en mitjans de comunicació

☐ Altres (especificar): _____

Si les persones no seran informades, indiqueu els motius:

☐ No existeix un risc per als seus drets i llibertats

☐ No hi ha cap acció que puguin portar a terme per mitigar els danys

☐ El dany reputacional per a l'organització seria molt elevat

☐ La comunicació exigeix un esforç excessiu

☐ No interferir en una investigació policial/judicial en curs

☐ Altres (especificar): _____ _____

13. Documentació adjunta

El responsable del tractament ha de documentar qualsevol violació de la seguretat de les dades personals (art. 36.5). En tot cas, l'Agència li podrà requerir la informació addicional necessària.

S'adjunta documentació complementària (per exemple, registre d'incidents, comunicació als afectats, qualsevol altre document relatiu a la violació de seguretat).

Especificar quins documents:

_____

_____

_____

_____

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.