

3. Delegat de protecció de dades (DPD) o persona de contacte:

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

En cas de respondre que sí, indiqui les dades del DPD o al contrari, indiqui les dades de la persona de contacte:

Nom: _____

NIA / NRT: _____

Telèfon: _____

Adreça electrònica: _____

Adreça: _____

CP: _____

País: _____

Naturalesa de l'organització: Privada Pública / Parapública

4. Sobre el tractament

Des de quan es porta realitzant 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 aquí declarada: _____

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

Únicament d'Andorra A nivell internacional

5. Sobre la violació de seguretat i les seves conseqüències

L'incident ha sigut:

Accidental o sense intencionalitat

Intencionalitat desconeguda

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

L'origen de l'incident ha sigut:

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 diverses 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 (postal o electrònicament)	Dades personals residuals en dispositius obsolets
Dades personals eliminades / 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/autoritzada	Enviament d'email a múltiples destinataris sense còpia oculta/llista de distribució	Ciberincident: (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

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

Integritat: s'han alterat les dades personals, segueixen sent accessibles, però la substitució de dades pot suposar un dany per a les persones afectades

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?

Si

No

Desconegut

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

Si

No

Encara no, però es preveu que es recuperarà aviat

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

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

Impossibilitat d'exercir algun dret

Impossibilitat per a accedir a un servei

Usurpació d'identitat

Ser víctima de campanyes de phishing/spamming

Pèrdues financeres

Danys reputacionals

Pèrdua de la confidencialitat de les dades afectades pel secret professional

Danys psicològics o físics

Pèrdua de control sobre les dades personals

Altres conseqüències

Encara desconegut

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

Si

No

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

Improbable

Baixa

Alta

Molt alta

Desconeguda

Resum de la violació de seguretat (breu descripció del que ha succeït i les mesures concretes preses per minimitzar el dany sobre les persones):

6. Tipus de dades afectades

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

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

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, ja siguin clients, proveïdors o qualsevol altra relació que pugui mantenir el responsable de tractament amb aquests.

Entre les persones afectades, hi ha menors o persones amb discapacitat?

Si

No

Desconegut

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

Si

No

Desconegut

Les persones afectades tenen els perfils següents:

Clients/ciudadans

Estudiants/alumnes

Usuaris

Pacients

Subscriptors/potencials clients

Afiliats/associats

Policies

Treballadors

Altres (indicar quin):

En total, quantes persones han vist les seves dades afectades per la violació de seguretat?
Si desconeix el valor exacte, indiqui un valor aproximat

8. Implicacions transfrontereres

La violació de seguretat té implicacions transfrontereres?

Si

No

Desconegut

En cas afirmatiu, especifiqueu els països afectats:

9. Informació temporal de la violació de seguretat

Coneix la data en la que es va iniciar la violació de seguretat? En tal cas, indiqui la data:

Data exacta

Aproximada/estimada

Desconeguda

La violació de seguretat s'ha detectat mitjançant:

Mitjans de detecció
implementats proactivament
pel responsable o encarregat

L'advertència d'algun membre
de la organització del
responsable o l'encarregat

Comunicació d'algun afectat

Algun mitjà de comunicació

Un tercer aliè

Altres (indicar quin):

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 requeriment 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

Xifrat de les dades

Còpia de seguretat

Anonimització

Cap de les anteriors

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

Si

No

Desconegut

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

Si

No

Desconegut

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

Si

No

11. Accions preses després de l'incident

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

Si

No

Desconegut

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

Mitjà de comunicació utilitzat o previst:

Telefònicament o verbalment

Comunicació dirigida personalment a cada afectat (postal, email, sms o similar)

Comunicat públic o publicació en web corporatiu

Comunicació dirigida personalment a cada afectat (postal, email, sms o similar) amb garantia de lliurament i lectura

Difusió en mitjans de comunicació

En el seu cas, les persones no seran informades perquè:

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 la organització seria molt elevat

La comunicació exigeix un esforç excessiu

No interferir en una investigació policial/judicial en curs

Altres (indicar quin):

13. Documentació adjunta

No és necessari adjuntar més documentació que les dades sol·licitades en aquest formulari. En tot cas, l'Agència li podrà requerir la informació addicional necessària.

S'adjunta documentació acreditativa de la representació del responsable o la seva autorització per a notificar la violació de seguretat a l'autoritat de control.

14. Notificació completa o per fases

Marqui la opció més adequada a la situació del responsable en el moment de la notificació:

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.

Aquesta notificació és inicial als efectes del compliment amb el termini de notificació establert en la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades

personals, en el termini màxim de 30 dies es notificarà informació addicional. En cas contrari, l'autoritat de control considerarà aquesta notificació com a completa.

Lloc i 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 el 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.

Podeu exercitar 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 complimentat i signat a cada pàgina mitjançant l'enviament del mateix a l'adreça de correu electrònic apda@apda.ad o a través de la intranet de l'Agència Andorrana de Protecció de Dades.