

L'APDA recorda què és una violació de seguretat de dades personals i quines obligacions tenen els responsables del tractament

L'Agència Andorrana de Protecció de Dades (APDA) publica una comunicació informativa de caràcter general per recordar què s'entén per violació de seguretat de dades personals i quines actuacions cal dur a terme quan es produeix una incidència que pugui comprometre la seguretat de la informació.

Què és una violació de seguretat de les dades personals

Una violació de seguretat de dades personals és qualsevol incident que provoqui, de manera accidental o il·lícita, la destrucció, la pèrdua, l'alteració, la divulgació no autoritzada o l'accés indegut a dades personals, comprometent la confidencialitat, la disponibilitat o la integritat de les dades.

Aquest tipus d'incident no es limita als atacs informàtics. També pot derivar d'errors humans, de la pèrdua de documentació o de qualsevol altra situació que afecti la seguretat de la informació personal.

Exemples habituals de violacions de seguretat

Entre les situacions que poden constituir una violació de seguretat es troben, entre d'altres:

- L'enviament d'un correu electrònic amb dades personals al destinatari equivocat.
- L'enviament d'un missatge a diversos destinataris sense relació entre ells sense utilitzar la còpia oculta.
- La pèrdua o robatori d'un ordinador, telèfon mòbil, dispositiu USB o expedient en paper.
- L'accés no autoritzat a una base de dades o a una carpeta compartida.
- La publicació indeguda d'informació personal.
- L'alteració o eliminació accidental de dades.
- Un atac de programari maliciós, ransomware o una intrusió als sistemes.
- La indisponibilitat temporal o definitiva de dades essencials.

Quan s'ha de notificar a l'APDA

D'acord amb l'article 36 de la Llei qualificada de protecció de dades personals (LQPD), el responsable del tractament ha de notificar la violació de seguretat a l'APDA sense dilació indeguda i, si és possible, dins de les 72 hores següents al moment en què n'ha tingut constància.

Aquesta notificació no és exigible quan sigui improbable que la violació comporti un risc per als drets i les llibertats de les persones físiques.

Quan la notificació es realitza fora del termini de 72 hores, s'han d'indicar els motius que justifiquen la dilació.

Què ha de fer l'encarregat del tractament

Quan la incidència és detectada per l'encarregat del tractament, aquest ha de comunicar-la sense dilació al responsable del tractament.

Amb caràcter general, l'encarregat no és qui notifica directament la incidència a l'autoritat de control, sinó que ha d'informar immediatament el responsable perquè aquest pugui valorar la situació i complir amb les obligacions legals que li corresponen.

Informació que ha d'incloure la notificació

La notificació dirigida a l'APDA ha d'incloure, com a mínim:

- La naturalesa de la violació de seguretat, indicant, si és possible, les categories de dades afectades, el nombre aproximat de persones afectades i el nombre aproximat de registres afectats.
- Les dades de contacte del delegat de protecció de dades o del punt de contacte designat.
- Les possibles conseqüències de la violació.
- Les mesures adoptades o proposades per fer front a la incidència i per mitigar-ne els possibles efectes negatius.

A la pàgina web de l'APDA es pot trobar el formulari per notificar una violació de seguretat, que s'ha d'enviar juntament amb la documentació necessària perquè l'Agència pugui avaluar els fets.

Si en el moment de la notificació no es disposa de tota la informació, aquesta es pot facilitar posteriorment de manera progressiva, però sempre sense dilació indeguda.

Comunicació a les persones afectades

Quan la violació de seguretat pot comportar un alt risc per als drets i les llibertats de les persones físiques, el responsable del tractament també ha de comunicar-ho a les persones afectades sense dilació indeguda, d'acord amb l'article 37 de la LQPD.

Aquesta comunicació ha d'utilitzar un llenguatge clar i senzill i ha d'incloure, com a mínim:

- La naturalesa de la violació de seguretat.
- Les dades de contacte del punt de contacte o del delegat de protecció de dades.
- Les possibles conseqüències de la incidència.
- Les mesures adoptades o proposades per fer-hi front.

Quan no cal comunicar-ho a les persones afectades

La comunicació individual a les persones interessades no és necessària si es dona alguna de les circumstàncies següents:

- Les dades estaven protegides amb mesures tècniques adequades, especialment si eren intel·ligibles per a tercers no autoritzats, com en el cas del xifrat.
- S'han adoptat mesures posteriors que garanteixen que ja no existeix l'alt risc.
- La comunicació individual suposa un esforç desproporcionat. En aquest cas, s'ha de fer una comunicació pública o adoptar una mesura equivalent igualment efectiva.

En qualsevol cas, si el responsable del tractament no comunica la violació a les persones afectades i l'APDA considera que hi pot haver un alt risc per als seus drets i llibertats, l'Agència pot exigir que es faci aquesta comunicació.

Actuació immediata davant una incidència

Quan es detecta una possible violació de seguretat és important actuar amb rapidesa i de manera ordenada.

En primer lloc, cal contenir la incidència per evitar que s'agreugi. Això pot implicar bloquejar accessos, desconnectar equips, canviar contrasenyes, recuperar documentació o limitar la difusió de la informació.

En segon lloc, cal analitzar què ha passat i quines dades poden haver resultat afectades, així com el nombre aproximat de persones implicades, la possible existència de dades sensibles i les conseqüències potencials de la incidència.

En tercer lloc, s'ha de valorar el nivell de risc per als drets i les llibertats de les persones afectades, ja que aquesta anàlisi és clau per determinar si cal notificar la violació a l'APDA i si també s'ha de comunicar als interessats.

En quart lloc, si escau, s'ha de procedir a la notificació a l'APDA dins del termini de 72 hores i preparar, si correspon, la comunicació a les persones afectades.

Finalment, és essencial documentar tota la gestió de la incidència.

Obligació de documentació interna

Encara que una incidència no s'hagi de notificar a l'APDA, el responsable del tractament ha de documentar qualsevol violació de seguretat.

Aquesta documentació ha d'incloure els fets relacionats amb la incidència, els seus efectes, la valoració del risc, les mesures correctores adoptades i la decisió sobre si es notifica o no a l'autoritat de control, així com els motius d'aquesta decisió.

Aquest registre permet demostrar el compliment de la normativa i facilita la verificació per part de l'autoritat de control.

Conseqüències de no notificar quan és exigible

La manca de notificació d'una violació de seguretat a l'APDA quan aquesta és exigible pot constituir una infracció greu de la normativa de protecció de dades, d'acord amb l'article 72.2 e) de la LQPD.

La notificació d'una violació de seguretat forma part de les obligacions de diligència del responsable del tractament i permet demostrar una actuació transparent i proactiva davant d'un incident.

Per aquest motiu, davant la detecció d'una possible violació de seguretat, és recomanable informar l'APDA dins dels terminis establerts, ja que la manca de comunicació d'un incident que hauria d'haver estat notificat pot ser susceptible de sanció.

Atentament.

A Andorra la Vella, el dia 10 de març del 2026

Agència Andorrana de Protecció de Dades