FITXES DEL DPD

Ref. 11/2021

Guia violacions de seguretat

Violació de seguretat de les dades personals

El RGPD, obliga al responsable de tractament de l'entitat ha comunicar les violacions de seguretat de les dades personals a l'autoritat de control, quan comportin un risc per als drets i llibertats de les persones i en casos d'alt risc als afectats, tan aviat com sigui possible amb un termini màxim de 72 hores. Per tant, l'obligació de notificar violacions de seguretat es fa extensible a totes aquelles entitats que portin a terme un tractament de dades personals.

Violació de seguretat vs incident de seguretat?

Un **incident de seguretat** és qualsevol esdeveniment inesperat o no desitjat amb conseqüències en detriment de la seguretat del sistema d'informació. Per contra, el RGPD defineix **violació de seguretat** com qualsevol violació de la seguretat que ocasiona la destrucció, la pèrdua o l'alteració accidental o il·lícita de dades personals transmeses, conservades o tractades d'una altra manera, o la comunicació o l'accés no autoritzats a aquestes dades.

CONCEPTES CLAU:

- **Destrucció:** quan les dades no existeixen, o no existeixen en una forma en què el responsable del tractament en pot fer ús.
- **Dany**: quan les dades han estat alterades, malmeses o no són completes.
- **Pèrdua**: quan les dades tot i que pot ser existeixen, el responsable del tractament ha perdut el control o l'accés o ja no les té.
- **No autoritzat o il·legal:** quan pot haver revelació o accés a destinataris no autoritzats.

La principal diferencia entre ambdós conceptes radica en que la violació de seguretat s'aplicarà en el supòsit en que es vegin afectades dades de caràcter personal.

Per tant, **totes les violacions de seguretat** de les dades personals **són incidents de seguretat**, però no tots els incidents de seguretat són necessàriament violacions de seguretat de les dades personals.

Quan l'entitat es troba davant d'un incident de seguretat (accés indegut, sniffing, malware, compromís de credencials, etc) haurà de valorar si aquest a afectat a les dades personals dels interessats i procedir en conseqüència.

Quins tipus de violació de seguretat de les dades personals hi ha?

- **Violació de confidencialitat**: té lloc quan parts no autoritzades, o sense propòsit legítim accedeixen a les dades personals.
  La gravetat de la pèrdua de confidencialitat s'haurà de veure juntament amb l'abast de la seva divulgació, és a dir, número potencial i tipus de parts que poden haver accedit a la informació.

EXEMPLE

Un professional assistencial accedeix a la història clínica d'una veïna per interessar-se pel seu estat de salut. Estaríem davant d'un cas de pèrdua de confidencialitat, en tant que el professional assistencial podria accedir a la història clínica de la pacient sempre i quan hi hagués una vinculació assistencial. Per tant, no pot accedir a històries clíniques de pacients que no estan assignats a ell/a o accedir a dades de familiars, amics o companys, inclòs post-mortem, tot i que sigui de bona fe.

- **Violació d'integritat:** té lloc quan hi ha alteració de la informació original i la substitució de dades pot ser perjudicial per l'individu.
  La situació més greu ocorre quan existeixen possibilitat de que les dades alterades s'hagin utilitzat d'una manera que pugui fer mal a l'individu.
- **Violació de disponibilitat:** té lloc quan no es pot accedir a les dades originals quan és necessari. Pot ser temporal (dades recuperables) o permanent (dades no recuperables).

EXEMPLE

En el context assistencial, pot ser que el sistema no estigui disponible de manera temporal per pèrdua de subministrament elèctric i això pugui suposar un risc per als drets i llibertats de les persones en tant, que es pot veure compromesa l'activitat assistencial i per tant, l'atenció al pacient.

Un altre exemple, seria una infecció de les dades per programari maliciós que xifra les dades a canvi de rescat (ramsorware) que bloqueja el sistema i deixa sense accés als professionals al seus historials clínics.

Quan cal notificar una violació de seguretat de les dades personals?

Per tal de determinar si el responsable de tractament ha de notificar una violació de seguretat de les dades personals a l'autoritat de control competent o als interessats cal determinar en primer terme si implica risc.

Tant si és preceptiu notificar a l'autoritat com als interessats, el responsable del tractament ha de fer constar tota la informació relativa als fets, els efectes i les mesures correctores adoptades al registre de violacions de seguretat.

Per tant, en cas de violació de seguretat de les dades personals:

ACCIONS	SENSE RISC CONEGUT	RISC	ALT RISC
Incloure al Registre de vulneracions de seguretat	✓	✓	✓
Notificar a l'Autoritat de PD		✓	✓
Comunicar als afectats			✓

Qui té l'obligació de notificar violacions de seguretat?

Amb l'aplicació del RGPD, l'obligació de notificar a l'autoritat de control passa a ser un requeriment obligatori dels responsables de tractament que tractin dades de caràcter personal. Així doncs, pel que fa al RGPD:

1. Responsable de tractament

- En cas de violació de seguretat de les dades cal que el **responsable de tractament** notifiqui aquesta violació sense dilació indeguda i, quan sigui possible, com a màxim al cap de 72 hores d'haver-ne tingut constància.
- Ho haurà de comunicar quan té un **grau de certesa raonable** que s'ha produït un incident de seguretat que ha compromès les dades personals.
- El responsable de tractament pot obrir un **període d'investigació** durant el qual no es pot considerar que n'ha tingut constància.
- La **investigació** haurà de començar **el més aviat possible** i haurà de determinar amb un cert grau de certesa si s'ha produït una violació.

- **En cas de tenir encarregats del tractament, el responsable tindrà constància quan l'encarregat l'informi de la violació.**
- **El responsable pot autoritzar a l'encarregat** del tractament a notificar una violació en nom seu, sempre que així es **reflecteixi a l'acord d'encàrrec** de tractament. No obstant, la responsabilitat jurídica de notificar recau en el responsable de tractament.

El responsable del tractament ha de tenir un **Procediment intern per gestionar els incidents de seguretat**, detectar i tractar una violació i determinar qui dins l'organització té la responsabilitat operativa per gestionar una violació, i com escalar una violació a nivells de responsabilitat adequats.

Els treballadors de l'entitat han de conèixer aquest procediment i saber en cas d'incident on s'han de dirigir o comunicar.

2. Encarregat del tractament

- El **contracte o acte jurídic** que s'ha d'establir **entre el responsable i l'encarregat** del tractament ha de marcar que l'encarregat "ha d'ajudar el responsable a garantir el compliment de les obligacions que estableixen els articles 32 a 36, tenint en compte la naturalesa del tractament i la informació a disposició de l'encarregat".
- En cas de **tenir constància d'una violació de seguretat** de les dades personals que està tractant per compte del responsable haurà de notificar "**sense dilació indeguda**" al responsable del tractament. El RGPD no indica temps concret, però atenent que el responsable té un **termini de 72h** per notificar a l'autoritat de control, l'encarregat haurà d'informar el més ràpid possible des de que té constància.
- Per tant, **l'encarregat del tractament** haurà d'establir si s'ha produït o no una notificació i després notificar-ho al responsable.
- **L'encarregat pot notificar** en nom del responsable del tractament si està autoritzat pel responsable i així s'indica a l'acord d'encàrrec de manera expressa.

3. Corresponsables del tractament

- En **l'acord de coresponsabilitat** de tractament s'estableix que els corresponsables han de determinar de manera transparent i de mutu acord les seves responsabilitats respectives, en el compliment de les obligacions imposades pel RGPD.

  Aquest acord ha de reflectir les funcions i les relacions dels corresponsables en relació amb els interessats.

  Per tant, l'acord que reguli la relació entre els corresponsables hauria de determinar el procediment de notificació de les violacions de seguretat i les actuacions i els compromisos que assumeix cadascun en l'aplicació de les mesures correctores que escaiguin.
- Un dels problemes que poden sorgir en aquests casos és la **coordinació de les actuacions** de cadascun dels corresponsables tant en la notificació de les violacions de seguretat com en l'aplicació de les mesures correctores que s'hagin d'aplicar (determinació dels límits de la participació).
- L'RGPD exigeix al responsable que notifiqui a l'autoritat de control les violacions de seguretat, en cas de corresponsables, **la notificació** correspondria al corresponsable en l'activitat de tractament en la que s'ha produït la violació. Si els dos corresponsables resulten afectats per la violació i procedeix efectuar la notificació, cal fer-la conjuntament.
- En els casos en què **l'autoritat de control competent sigui diferent** per a cadascun dels corresponsables (per exemple, AEPD i APDCAT).

  En aquests casos es considera oportú que cada corresponsable notifiqui la violació especificant en cadascuna de les notificacions que es tracta d'una coresponsabilitat i que s'ha declarat per part de l'altre corresponsable a la seva autoritat de control indicant quina és.

Què ha de contenir la notificació a l'Autoritat de control i als interessats?

1. La notificació a l'Autoritat de control contindrà com a mínim:

- Descripció de la naturalesa de la violació de la seguretat de les dades. Si és possible, també cal incloure-hi les categories i el nombre aproximat d'afectats, així com les categories i el nombre aproximat de registres de dades personals afectats.
- Nom i dades de contacte del delegat de protecció de dades.
- Descripció de les possibles conseqüències.
- Descripció de les mesures adoptades o proposades per mitigar-ne els possibles efectes negatius.

Si no és possible facilitar tota la informació en la primera comunicació es pot fer de manera gradual, sense dilació indeguda.

Més informació:

Podeu consultar el formulari que **l'Autoritat Catalana de Protecció de Dades** disposa a la seva web aquí.

Un cop emplenat i signat electrònicament, el formulari s'ha de trametre (juntament amb la documentació que correspongui, si és el cas).

Per presentar-lo:

- Les entitats que estan donades d'alta a la plataforma EACAT han de presentar el formulari mitjançant el tràmit Notificacions de violacions de seguretat d'aquesta plataforma.
- La resta d'entitats l'han de presentar a través d'aquest tràmit de la seu electrònica de l'Autoritat.

2. La comunicació als interessats:

Haurà de descriure en llenguatge clar i senzill, la naturalesa de la violació i contindrà com a mínim, la següent informació:

- Dades del Delegat de Protecció de Dades.
- Descripció general de l'incident i moment en que s'ha produït.
- Possibles conseqüències de la violació de seguretat de les dades personals.
- Descripció de les dades i informació personal afectada.
- Resum de les mesures implantades.
- Altre informació útil.

La comunicació s'haurà de realitzar preferentment de **forma directa** a l'interessat a través de qualsevol medi dirigit a l'afectat si el responsable ho considera adient.

Per tant, la comunicació es pot realitzar per:

- Telèfon.
- Correu electrònic.
- SMS.
- Correu postal.

La comunicació de forma indirecta es farà servir quan els costos de notificació directa siguin excessius o quan no sigui possible contactar amb les persones afectades.

En aquests casos, la comunicació es pot realitzar per:

- Llocs web.
- Blogs corporatius.
- Comunicats de premsa.

EXEMPLE

Una comunicació indirecta es pot realitzar si s'ha produït un robatori d'un portàtil amb un alt volum d'informació de pacients i desconeixem les dades de contacte dels mateixos.

Com he de notificar una violació de seguretat de les dades personals per tractaments transfronterers?

En el cas de tractaments transfronterers les violacions de seguretat poden afectar les dades personals en més d'un estat membre.

En aquests casos:

- Cada autoritat de control és competent per desenvolupar les funcions que se li assignen i per exercir els poders que té conferits d'acord al reglament, al territori del seu estat membre.
- Quan el tractament el duen a terme autoritats públiques que actuen de conformitat amb l'article 6, apartat 1, lletres c) o e), l'autoritat de control competent és la de l'estat membre de què es tracta.
- Per la resta de supòsits, l'autoritat de control de l'establiment principal o de l'únic establiment del responsable o de l'encarregat del tractament és competent per actuar com a autoritat de control principal per al tractament transfronterer efectuat per aquest responsable o encarregat, de conformitat amb el procediment de cooperació entre autoritats de control establert al reglament.

Quan no cal notificar?

1. **No serà necessari notificar a l'autoritat de control:**
   - Quan sigui improbable que la violació de seguretat constitueixi un risc per als drets i llibertats de les persones. *(Veure apartat avaluació de risc).*
2. **No serà necessari notificar als interessats:**
   - Si **s'han adoptat les mesures tècniques i organitzatives apropiades**, que aplicades a les dades compromeses fes inintel·ligible i no permetés l'accés, per part d'un tercer.

EXEMPLE

Un professional decideix copiar informació dels pacients en un usb i fer-la pública a internet. El centre es dona conta uns dies més tard. En quan el responsable del tractament té constància disposarà de 72h per comunicar-ho a l'autoritat de control i als pacients afectats. En aquest sentit, si el centre hagués aplicat mesures de protecció tècniques i organitzatives apropiades (com el xifrat de les dades), no existiria la probabilitat de que es produís el risc i no caldria notificar.

- Quan **es reaccioni de manera eficaç** adoptant mesures ulteriors, que assegurin que no es produirà cap risc per als drets i llibertats dels interessats.
- Si la **comunicació suposa un esforç desproporcionat**. En aquest cas, s'hauria de realitzar una comunicació pública o similar que fes efectiva la notificació.

El **responsable** de tractament té **l'obligació sempre de documentar les violacions de seguretat** de les dades, incloent, el fets relacionats amb la violació, el seus efectes, així com les mesures correctores adoptades.

La documentació ha d'estar disponible per l'autoritat de control, que si ho considera oportú en atenció a la probabilitat de que la violació impliqui alt risc per als interessats, podrà demanar al responsable que es comuniqui als afectats ("accountability").

Què passa si no notifico o comunico una violació de seguretat de dades personals?

La **no notificació** d'una violació de seguretat de les dades a l'autoritat de control o als afectats, o a cap dels dos, pot revelar l'absència de mesures de seguretat o una insuficiència de les mesures de seguretat existents.

Així mateix, les autoritats de protecció de dades disposen de mecanismes per als casos en que una administració pública realitza un incompliment:

- **Possible infracció**: comporta un **avís**.
- **Infracció: advertència** o **prohibició temporal o definitiva** del tractament.

Què hem de tenir en compte en les violacions de seguretat en l'àmbit de recerca?

En l'àmbit de recerca amb dades de salut, existeixen dos elements que afegeixen complexitat a la gestió de les notificacions de les violacions de seguretat.

a) Complexitat normativa en l'àmbit de la recerca.

En funció del tipus de projecte hem d'estar a la normativa especifica que la regula el projecte concret (per exemple els projectes amb mostres es regulen per la Llei 14/2007 d'Investigació Biomèdica o els estudis observacionals es regulen per l'Ordre SAS/3470/2009).

Cada norma, estableix una sèrie d'obligacions específiques i diferents en relació al tractament de les dades utilitzades en el projecte de recerca, com per exemple el termini de conservació de les dades (p.ex 25 anys assaig clínic), o les comunicacions a tercers (p.ex comunicació d'efectes adversos a autoritats competents), i que hem de tenir en compte per determinar si s'ha produït o no una violació de seguretat.

b) Complexitat per determinar la responsabilitat del tractament.

En l'àmbit de la recerca existeixen diversos actors que tracten dades (centre hospitalari, promotor, fundació que gestiona la recerca, monitor, ...), i cal determinar quines són les relacions que s'estableixen entre ells (responsable del tractament, corresponsables, encarregat de tractament), per determinar qui avaluarà i comunicarà la violació de seguretat.

Per l'assaig clínic...

En aquest cas, **el centre hospitalari i el promotor seran corresponsables** del tractament de les dades dels participants, o bé responsables independents en els assaigs. El monitor serà encarregat de tractament de les dades en quan realitza tasques de monitoratge, i la Fundació que gestiona la recerca, sols podrà accedir a aquestes dades en la seva condició d'encarregat de tractament, quan les seves funcions de suport a la recerca així ho exigeixin. En aquest cas la violació de seguretat s'hauria de dur a terme pel centre Hospitalari o pel Promotor en funció de la natura de la violació de seguretat.

Per tant quan gestionem una violació de seguretat en l'àmbit de la recerca, **cal definir de forma prèvia qui és el responsable del tractament de les dades, així com aquells tercers autoritzats** per tractar informació, evitant així possibles errors en quan a forma i el contingut de la notificació.

Davant una violació de seguretat de les dades personals, quan m'he de comunicar amb el DPD?

Des del moment en que es té constància de que la violació afecta als drets i llibertats de les persones, la persona designada es posarà en contacte amb el Delegat de Protecció de dades. Aquest, un cop informat de l'incident:

- Assessorarà al CPD o persona designada per l'entitat i al Comitè de seguretat i protecció de dades.
- Supervisarà el compliment de la normativa de protecció de dades.
- Actuarà com a punt de contacte amb l'Autoritat, tal i com s'haurà d'indicar al formulari de notificació.

Que ha de contenir el registre d'incidents?

El Reial Decret 1720/2007, de 21 de desembre, pel qual es va aprovar el reglament de desenvolupament de Llei Orgànica 15/1999, recollia l'obligació de portar a terme un registre d'incidències intern.

L'RGPD estableix que el responsable del tractament ha de documentar totes les violacions de seguretat, tant si és preceptiu notificar-les a l'Autoritat com si no.

En concret, ha de fer constar tota la informació relativa als fets, els efectes i les mesures correctores adoptades. Aquesta documentació ha d'estar a disposició de l'Autoritat.

CAMPS REGISTRE D'INCIDENTS

A continuació es mostren els camps mínim que hauria de contenir el registre d'incidents:

- Número d'incidència
- Data
- Hora
- Tipus d'incident
- Descripció de l'incident
- Efectes de l'incident
- Persona que notifica/detecta l'incident
- Persona a qui es notifica/trasllada l'incident
- Implica dades personals (SI/NO)
- Naturalesa de la violació (confidencialitat/integritat/disponibilitat)
- Categoria de dades afectades
- Número de persones afectades
- Tractament de dades afectat
- Conseqüències probables
- Mesures correctores adoptades(solucionar problema o limitar els efectes)
- Comunicació a l'Autoritat de control (SI/NO) justificació
- Comunicació afectats (SI/NO) justificació

Com avaluem el risc i l'alt risc?

Un cop el responsable del tractament té constància de la violació de seguretat ha de contenir-la en primer lloc i avaluar el risc per determinar si cal notificar la violació a l'autoritat de control i si escau, a les persones afectades.

Per avaluar el risc s'ha de tenir en compte la probabilitat i la gravetat del risc per als drets i llibertats de les persones.

Per tant, necessitem conèixer el nivell de risc per prendre les decisions pertinents.

CONCEPTE CLAU:

Cal assenyalar que l'avaluació del risc per als drets i llibertats de les persones com a conseqüència d'una violació té un enfocament diferent del risc que s'avalua en una AIPD.

L'AIPD avalua tant els riscos del tractament de dades tal com es preveu fer, com els riscos en cas de violació.

Quan s'avalua una violació potencial, en general s'enfoca a la probabilitat que succeeixi i al dany que es pot produir per als afectats; en altres paraules, és la valoració d'un incident hipotètic. Amb una violació real, l'incident ja s'ha produït, de manera que l'enfocament està totalment relacionat amb el risc que comporta l'impacte de la violació en les persones.

La normativa no disposa, ni preveu, una manera específica de gestionar o avaluar els riscos derivats del tractament de dades personals, per tant, es pot donar el cas que les organitzacions avaluïn i tractin els riscos amb criteris diferents.

És molt important que el responsable d'avaluar el risc consideri **les circumstàncies específiques de la violació**, inclosa la gravetat de la probabilitat de que això succeeixi i la gravetat de l'impacte potencial.

CONCEPTE CLAU:

- **Risc**: El risc és la possibilitat que alguna cosa o algú causi dany.

El risc es pot preveure com el resultat de la combinació de dos conceptes:

- **Possibilitat** entès com la probabilitat de que passi alguna cosa.
- **Gravetat** (conseqüències o danys esperats) entès com el producte de la vulnerabilitat intrínseca al perill concret i l'exposició al perill concret.

RISC = Probabilitat x Conseqüències

En avaluar el risc probable de que es produeixi una violació, caldrà avaluar la combinació de la gravetat de l'impacte potencial sobre els drets i llibertats de les persones i la possibilitat que es produeixi l'incident, atenent que quan les conseqüències o danys esperats d'una violació són més greus, els risc és més elevat i de igual manera, quan la probabilitat de que es produeixi una violació és més gran, el risc també augmenta.

CRITERIS A TENIR EN COMPTE EN L'AVALUACIÓ DEL RISC EN EL CONTEXT DE SALUT		
Tipus de violació	**Confidencialitat**	Una violació de la confidencialitat mitjançant la qual s'ha revelat informació mèdica a usuaris no autoritzats pot tenir un conjunt diferent de conseqüències per a una persona, que una violació en què s'han perdut les dades mèdiques d'un individu i ja no estan disponibles.
	Integritat	
	Disponibilitat	
Categoria de dades	**Dades no sensibles:** enteses com les dades de contacte, educació, familiars, professionals, econòmiques.	Com més sensibles són les dades, més alt és el risc de dany per a les persones afectades. A l'àmbit de la salut es tracten un gran volum da dades sensibles. Per exemple, una divulgació inadequada de la informació de salut del pacient pot suposar un risc més alt que, per exemple, el seu nom o adreça de manera aïllada.
	Dades sensibles: salut, biomètriques, vida sexual, religió.	
Tipologia de dades	**Llegible**	Fins i tot quan les dades estan xifrades, una pèrdua o alteració pot tenir conseqüències negatives per a les persones afectades, si el responsable del tractament no té les còpies de seguretat adequades.
	Il·legible: pseudoanonimitzada, xifrada, hash.	
Origen de l'incident	**Font interna**: organització.	En cas de font interna, hi ha més possibilitat de controls els danys o conseqüències. Per tant, el risc de danys pot ser menor quan la violació de seguretat és involuntària o accidental, en lloc de intencionada o malintencionada.
	Font externa: proveïdors de serveis, ciutadà, encarregat de tractament).	
Nivell criticitat sistemes afectats	**Crític**: afecta a dades valuoses o gran volum i poc temps.	Com més crític sigui el nivell d'afectació, més probable és el risc d'afectació a dades personals.
	Molt Alt: volum apreciable i pot afectar a dades valuoses.	
	Alt: pot afectar a dades valuoses.	
	Mitjana: afecta a un volum apreciable.	
	Baix: escassa o nul·la capacitat a d'afectar a dades valuoses o volum apreciable.	
Conseqüències afectats	**Molt alta**: les persones poden enfrontar conseqüències significatives o inclús irreversibles que no poden superar.	Com mes alta sigui la probabilitat de conseqüències pels afectats, més alt el risc de dany per les persones afectades.
	Alta: les persones poden trobar conseqüències importants, que deurien poder superar amb serioses dificultats.	
	Mitja: les persones poden trobar inconvenients importants, que podran superar tot i tenir dificultats.	
	Baixa: les persones no es veuran afectades o poden trobar inconvenients que es superin sense problemes.	

Identificació afectats	**Facilitat identificació**	Valorar com de fàcil resulta deduir la identitat dels individus a partir de les dades involucrades en l'incident.
Categoria especials afectats	**Característiques especials**	Tenir en compte categories especials com menors, discapacitats o individus vulnerables que poden estar en un risc superior.
Qui a tingut accés a la informació dels afectats	**Context intern**	La sensibilitat de la informació personal també depèn del context. Per exemple, divulgar certa informació a persones conegudes del pacient amb qui té una relació difícil és més probable que provoqui humiliació o dany a la persona. Es diferent, si el destinatari és una entitat o persona de confiança, coneguda, que raonablement s'espera que retorni o destrueixi la informació sense revelar-la o utilitzar-la.
	Context extern	
Perfil afectats	**Usuaris interns entitat**	
	Pacients	
	Altres	
Volum afectats	**Menys de 100 registres**	En general, com més gran és el nombre d'afectats, més gran pot ser l'impacte d'una violació. No obstant, una violació pot tenir un impacte greu en un sol individu, segons quina sigui la naturalesa de les dades personals i el context en el qual s'han vist compromeses.
	Més 1.000	
	Entre 1.000 i 100.000	
	Més de 100.000	
	Més de 1.000.000