PÍNDOLA 1.- LES VIOLACIONS DE SEGURETAT DE LES DADES

Què és una violació de la seguretat de les dades personals?

L'article 4.12 del Reglament General de Protecció de Dades (en endavant "RGPD") defineix una "violació de la seguretat de les dades personals" com:

"Qualsevol violació de la seguretat que ocasiona la destrucció[1], la pèrdua[2] 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 autoritzat[3] a aquestes dades".

Una violació és un tipus d'incident de seguretat. No obstant això, d'acord amb l'article 4.12 del RGPD, aquest només s'aplica als incidents de seguretat quan hi ha una violació de dades personals. La conseqüència d'aquesta violació és que el RESPONSABLE no pot garantir el compliment dels principis relatius al tractament de les dades personals (article 5 del RGPD).

Tipus de violacions de seguretat de les dades personals:

- "Violació de la confidencialitat": quan hi ha una revelació no autoritzada o accidental o accés a les dades personals.
- "Violació de la integritat": quan hi ha una alteració no autoritzada o accidental de les dades personals.
- "Violació de disponibilitat": quan hi ha una pèrdua d'accés accidental o no autoritzada o la destrucció de dades personals.

Per tant una violació de seguretat que impedeixi que les dades personals estiguin disponibles durant un període de temps és un tipus de violació, ja que la manca d'accés a les dades pot tenir un impacte significatiu en els drets i llibertats de les persones. En el context d'un hospital, si les dades mèdiques crítiques sobre els pacients no estan disponibles, fins i tot de manera temporal, això pot suposar un risc per als drets i les llibertats de les persones; per exemple, es poden haver de cancel·lar les operacions, i per tant, les vides es posen en risc.

Notificació a l'APDCAT

Si es produeix una violació de la seguretat, el RESPONSABLE l'ha de notificar a l'APDCAT, tret que sigui improbable que constitueixi un risc per als drets i les llibertats de les persones. D'aquesta forma, cal ponderar quan un incident de seguretat té afectació a dades personals i, quan així sigui, si aquesta afectació comporta un risc als drets i llibertats de les persones.

[1] S'entén per "destrucció" de dades personals: quan les dades ja no existeixen, o no existeixen en una forma en què el responsable del tractament en pot fer ús.

[2] S'entén per "pèrdua" de dades personals quan les dades encara existeixin, però el responsable del tractament n'ha perdut el control o l'accés, o ja no les té.

[3] S'entén per tractament no autoritzat o il·legal la revelació de dades personals (o accés) a destinataris que no estan autoritzats a rebre les dades o a accedir-hi, o qualsevol altra forma de tractament que violi el RGPD.

La ponderació del risc

La ponderació del risc requereix que qualsevol incident de seguretat que afecti dades personals s'analitzi des de la perspectiva de si aquest comporta un risc per al drets i llibertats dels afectats.

Per exemple:

(i) una manca de disponibilitat que no afecti a la prestació del servei concret i, per tant, no impliqui afectació en els drets i llibertats del afectats, no serà necessària la seva comunicació (ex. caiguda del sistema del Pla de Medicació menor a x hores, quan es disposa d'un pla de contingència per imprimir les receptes en local). No obstant, aquesta incidència haurà de quedar degudament registrada en el sistema com s'indica a continuació: Traçabilitat.

(ii) una incidència a la integritat que no afecti al diagnòstic concret basada en processos automatitzats pel control periòdic del sistema i la detecció d'incidències (ex. expedients duplicats quan aquests es detecten de forma automàtica i es corregeixen sense que tingui afectacions per a la persona afectada - –aquesta duplicació no comporta un diagnòstic erroni per part dels serveis assistencials). No obstant, aquesta incidència també haurà de quedar degudament registrada en el sistema com s'indica a continuació: Traçabilitat.

(iii) una comunicació no autoritzada de les dades és possible que no calgui notificar-la quan les dades personals ja estan disponibles públicament i una divulgació d'aquestes no constitueixi un risc probable per als afectats. O, si aquestes dades són essencialment inintel·ligibles (ex. encriptades) per a persones no autoritzades i són una còpia o n'hi ha una còpia de seguretat, ja que és poc probable que aquesta violació suposi un risc per las drets i les llibertats dels afectats. No obstant, aquestes incidències també hauran de quedar degudament registrades en el sistema com s'indica a continuació: Traçabilitat.

El DPD de Salut pot donar suport i assessorament en aquestes situacions, però com veurem en el punt següent, la immediatesa en l'intercanvi d'informació és essencial.

Quin és el termini per notificar una violació de seguretat a l'APDCAT?

D'acord amb l'establert a l'article 33.1 del RGPD, la notificació de la violació a l'APDCAT s'ha de produir sense dilació indeguda i, si és possible, dins de les 72 hores següents que el RESPONSABLE n'ha tingut constància.

Es considera que es *té constància* d'una violació de seguretat quan hi ha *una certesa que s'ha produït i se'n té un coneixement suficient de la naturalesa i l'abast.*

La mera sospita que hi ha hagut una fallada o la constatació que ha succeït algun tipus d'incident, sense que se'n coneguin mínimament les circumstàncies, encara no haurien de donar lloc a la notificació ja que, en la majoria dels casos, en aquestes

condicions no es pot determinar fins a quin punt hi pot haver un risc per als drets i les llibertats de les persones interessades. No obstant això, en casos de fallades que per les seves característiques puguin tenir un gran impacte, sí que pot ser recomanable, un cop consultat el DPD, comunicar a l'APDCAT tan aviat com hi hagi evidències que s'ha produït una situació irregular respecte de la seguretat de les dades.

En els casos en què la notificació no es pugui fer en aquestes 72 hores, per causa de la complexitat a l'hora de determinar-ne completament l'abast, la notificació es pot fer posteriorment, acompanyada d'una explicació dels motius que han ocasionat el retard.

Quin ha de ser el contingut de la notificació d'una violació de seguretat a l'APDCAT?
L'article 33.3 del RGPD estableix que la notificació ha d'incloure un contingut mínim:

- Descriure la naturalesa de la violació de la seguretat de les dades personals, incloent-hi, si és possible, les categories i el nombre aproximat d'interessats afectats, i les categories i el nombre aproximat de registres de dades personals afectats.
- Comunicar el nom i les dades de contacte del DPD de Salut.
- Descriure les possibles conseqüències de la violació de seguretat de les dades personals.
- Descriure les mesures adoptades o proposades pel RESPONSABLE 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.

Tanmateix, l'article 33.4. del RGPD preveu que la informació també es pot proporcionar de forma escalonada, quan no es pugui fer al mateix moment de la notificació.

L'APDCAT disposa d'un formulari estandarditzat accessible a: apdcat.gencat.cat/web/.content/seu/formulari_NVS.pdf

Notificació a l'interessat
Un cop notificada a l'APDCAT, quan sigui probable que la violació comporti un alt risc[4] per als drets de les persones interessades, el RESPONSABLE l'ha de comunicar a les persones afectades sense dilacions indegudes i en un llenguatge clar i senzill, i contindrà com a mínim el nom i les dades de contacte del DPD de Salut, les possibles conseqüències de la violació de la seguretat de les dades personals i les mesures adoptades o proposades per fer front a la violació, incloses, si escau, les mesures adoptades per mitigar-ne els possibles efectes negatius.

Aquesta comunicació a/als l'interessat/interessats no serà necessària quan:

- El RESPONSABLE hagi adoptat mesures de protecció adequades, com ara que les dades siguin intel·ligibles per a persones no autoritzades, com el xifrat.

[4] S'entén per l'alt risc quan sigui probable que la violació de seguretat ocasioni danys importants a les persones interessades.

- El RESPONSABLE hagi aplicat mesures posteriors que garanteixen que ja no hi ha la probabilitat que es materialitzi l'alt risc.
- Suposi un esforç desproporcionat. En aquest cas, cal optar per una comunicació pública o una mesura semblant, que informi els interessats de manera igualment efectiva.

Traçabilitat

Cal tenir en consideració que d'acord amb l'establert a l'article 33.5 del RGPD, els RESPONSABLES han de documentar totes les violacions de seguretat de les dades personals, siguin objecte de notificació a l'APCAT o no, incloent els fets relacionats, el seus efectes, si n'hi ha, i les mesures correctores que s'han adoptat.

-Per qualsevol dubte o aclariment addicional podeu adreçar-vos al DPD de Salut-

dpd@ticsalutsocial.cat
https://ticsalutsocial.cat/oficina-dpd/
Tel.: 93 553 26 42 (9:00 a 14:00 h.)