“Parlem de Dades”, un pòdcast de l’Escola d’Administració Pública de Catalunya i l’Autoritat Catalana de Protecció de Dades.

Capítol 4: Qüestions pràctiques sobre les violacions de seguretat de les dades.

Bon dia! En aquest quart capítol de “Parlem de dades”, analitzarem un aspecte clau per als responsables del tractament de dades personals: les violacions de seguretat de les dades. Què és una violació de dades en termes del Reglament general de protecció de dades? Com ha d’actuar la nostra organització, quan en pateix una? En el temps que dura aquest pòdcast, intentarem resumir els passos clau que cal dur a terme en les 72 hores que marca la normativa.

Per fer-ho, ens acompanya l’Olga Rierola. L’Olga és coordinadora de la unitat de gestió de notificacions de violacions de seguretat de l'Autoritat Catalana de Protecció de Dades. Hola, Olga, i benvinguda!

Hola, moltes gràcies!

Molt bé! Comencem, doncs. Si parlem de violacions de la seguretat de les dades, vol dir que ja s’ha produït un incident i, per tant, que alguna cosa ha fallat, oi?

Efectivament, tots sabem que les mesures de seguretat no són 100% infal·libles, i que les violacions de dades es poden produir. En aquest sentit, el Reglament europeu exigeix a les organitzacions tenir implementades mesures i procediments per tal que, en cas que succeeixin, puguem reaccionar-hi de manera adequada. Això inclou: detectar-la i contenir-la ràpidament, analitzar els riscos que suposa per als titulars de les dades i determinar ràpidament si cal notificar la violació a l’Autoritat i, fins i tot, si cal comunicar-la a les persones afectades.

En definitiva, les obligacions sobre violacions de dades previstes al Reglament tenen com a objectiu protegir les persones i evitar que aquest fet pugui causar-los danys. Per això, ens hem d’assegurar que la nostra organització disposa d’un pla de resposta robust per fer front a qualsevol violació de seguretat, assignar-ne la gestió a una persona o equip de l’organització i que tot el personal n’estigui informat.

Per tant, queda clar que cal estar preparats per abordar ràpidament una violació de la seguretat de les dades. Per fer-ho, el primer que ens cal és saber reconèixer-la.

Així és, primer de tot cal identificar-la. Per fer-ho hem d'anar a la definició del Reglament, que estableix que una violació de la seguretat de les dades és qualsevol incident de seguretat que ocasiona la destrucció accidental o il·lícita, la pèrdua, l'alteració, la divulgació o l'accés no autoritzat a les dades personals, tant en format paper com en digital.

En resum, és qualsevol incident que compromet la seguretat de les dades. Per tant, aquestes violacions es poden classificar en tres tipus. En primer lloc, ens trobarem davant d'una violació de la confidencialitat quan algú que no devia té o pot tenir accés a les dades; un exemple típic és la tramesa de dades personals a un destinatari erroni, o bé el robatori d'un dispositiu mòbil amb dades personals. En segon lloc, ens trobarem davant una violació de la integritat quan algú que no devia modifica o canvia les dades; un exemple és la suplantació d'identitat, el que coneixem com a phishing. I, per últim, ens trobarem davant una violació de la disponibilitat quan hi ha una pèrdua d'accés a les dades. Aquesta pèrdua pot ser tan temporal, si per exemple fallen els sistemes d'un hospital i les bases de dades mèdiques no estan disponibles durant unes hores, com definitiva, si patim una infecció per ransomware que encripta les dades i no en tenim còpia de seguretat.

Per tant, entenem que és qualsevol incident de seguretat que afecta les dades personals i que pot tenir tant un origen accidental com deliberat.

Efectivament, en termes del Reglament, és una violació tant el fet que un treballador enviï accidentalment un correu amb dades personals a la persona equivocada, com si ho fa deliberadament. També ho és tant si un hacker accedeix a les dades, com si les dades queden al descobert per un error de configuració. De fet, gran part de les violacions que es notifiquen a l'Autoritat tenen com a origen errors humans. D'aquí, doncs, la importància cabdal de la formació constant del personal, també en matèria de ciberseguretat, per evitar caure en paranys.

Cal tenir en compte també, que una violació de dades és sempre una violació en termes del Reglament, tot i que no impliqui danys o perjudicis per a les persones titulars de les dades. Un exemple seria una supressió accidental de dades si es disposa de còpia de seguretat i s'han pogut recuperar ràpidament, o un tall breu d'energia que, per unes hores, impedeix la prestació de serveis no essencials. Com hem vist, la definició de violacions de dades no ens parla de risc. El risc apareix en les obligacions que se'n deriven per als responsables, com ara veurem.

Molt bé, ara que ja som capaços de reconèixer una violació de les dades, com hem
d'actuar quan detectem que n'hem patit una?

Som-hi. Intentaré resumir-ho en 6 passos, però abans vull ressaltar algunes qüestions, si em permets.

La primera és que, un cop el responsable detecta que s'ha produït una violació de dades, el rellotge comença a córrer i la normativa estableix que tenim 72 hores per notificar-ho. Tot i això, pot ser que finalment no ho haguem d'acabar fent perquè, com hem vist, no totes les violacions impliquen danys o perjudicis per als titulars de les dades.

La segona qüestió que vull remarcar és que, quan detectem una violació, cal informar-ne ràpidament el nostre delegat de protecció de dades, que és qui ens ajudarà a gestionar-la i prendre les decisions oportunes. Serà, a més, qui actuï com a interlocutor de l'Autoritat, si escau.

A l'últim, cal tenir en compte que, si bé és el responsable del tractament qui té les obligacions que es derivin de la notificació davant de l'Autoritat, si la violació la pateix el seu encarregat del tractament, com ara l'empresa TIC a qui hagi contractat la prestació de serveis al núvol, aquest encarregat té l'obligació de comunicar-la de seguida al responsable.

Perfecte, dit tot això, anem ara als 6 passos clau.

Molt bé. El primer pas és intentar contenir ràpidament la violació i limitar-ne els possibles efectes adversos per als titulars de les dades. La prioritat ha de ser protegir les persones. Alguns d'aquests exemples poden ser: recuperar ràpidament les dades eliminades indegudament o que han estat encriptades per ransomware, canviar les contrasenyes en cas d'atacs o contactar ràpidament amb els destinataris de les dades i demanar-los que les eliminin.

Paral·lelament, cal seguir investigant els fets per determinar-ne l'abast.

Seguidament, cal avaluar el risc de la violació per als drets i llibertats de les persones; és a dir, cal determinar la probabilitat que la violació els ocasioni danys i, si és així, de quina gravetat són. El nivell de risc o dany determinarà, doncs, les següents actuacions del responsable.

Per tant, en cas que sigui improbable que la violació comporti danys o conseqüències adverses per a les persones, no caldrà notificar-la a l'Autoritat. Per exemple, si perdem un USB amb dades personals dels treballadors, però està xifrat de manera segura, la clau no està compromesa i disposem de còpia de les dades, és poc probable que els causi danys, doncs no hem perdut l'accés a les dades, i el fet que estiguin protegides amb un nivell de xifratge adequat fa que siguin inintel·ligibles per a persones no autoritzades.

Per contra, si és probable que la violació els ocasioni danys, caldrà notificar-la a l'Autoritat, i fer-ho al més aviat possible i en un termini màxim de 72 hores. Seria el cas que l'USB no estigués xifrat i qualsevol persona no autoritzada pogués accedir a les dades, de manera que hi ha un risc de dany.

A més a més, si és probable que la violació comporti danys importants per a les persones, és a dir, en cas d'alt risc, com ara si l'USB contingués dades especialment sensibles, caldrà també comunicar-ho als afectats. I caldrà fer-ho ràpidament, perquè puguin prendre les mesures necessàries per protegir-se d'aquests possibles danys, seguint sempre les recomanacions del responsable, com ara estar alerta davant possibles xantatges, canviar les contrasenyes en cas de ciberatac o verificar moviments estranys dels comptes, depenent del cas.

Per últim, les organitzacions han de prendre les mesures correctores necessàries per evitar, en la mesura del possible, que es torni a produir un incident similar. I cal documentar totes les violacions al registre intern de violacions, tant les que cal notificar a l'Autoritat com les que no. En aquest registre, s'hi han d'incloure tots els fets que hi estiguin relacionats, les mesures correctores adoptades i les decisions preses, com ara la raó per la qual es considera que és improbable que la violació causi danys a les persones titulars de les dades. Aquest registre ha d'estar sempre a disposició de l'Autoritat, que pot haver-lo de supervisar.

Perfecte. Ara bé, no m'ha quedat del tot clar com cal avaluar el risc. Hi ha alguna fórmula per fer-ho?

No, avaluar el risc és una tasca complexa, ja que com hem dit hi ha violacions que no impliquen danys i d'altres que poden tenir múltiples conseqüències adverses sobre les persones. És a dir que poden causar-los danys que poden ser tant físics, materials com immaterials.

D'acord amb el Reglament, aquestes conseqüències poden ser la pèrdua de control sobre les seves dades personals, la restricció dels seus drets, la discriminació, la usurpació d'identitat o frau, pèrdues financeres, dany per a la reputació o qualsevol altre desavantatge econòmic o social. Així doncs, la probabilitat que la violació ocasioni algun d'aquests efectes adversos sobre els titulars de les dades s'ha d'avaluar cas per cas.

Cal tenir en compte que, en el cas que la violació afecti categories especials de dades, com ara opinió política, religió, afiliació sindical o dades de salut, és molt probable que aquestes conseqüències siguin molt significatives, és a dir que els ocasioni danys importants. Particularment, es considera que ens trobarem en situacions d'alt risc sempre que la violació pugui causar conseqüències com ara suplantacions d'identitat o frau, dany físic, angoixa psicològica o humiliació per a

les persones. Com hem dit, cal avaluar-ho cas per cas, en funció de les circumstàncies concurrents i considerant tots els factors rellevants.

Em pots posar alguns exemples d'aquests factors?

Sí, i tant. A l'hora d'avaluar el risc, o la probabilitat que la violació ocasioni danys o conseqüències adverses sobre les persones, i la seva gravetat, cal tenir en compte, per exemple, els factors següents: el tipus de violació patida, és a dir, si afecta la confidencialitat, la integritat o la disponibilitat de les dades, o qualsevol combinació de les tres; la naturalesa, la sensibilitat, i el volum de dades afectades; els col·lectius a qui fan referència, aquí cal tenir especialment en compte que el fet que la violació afecti col·lectius vulnerables, com ara menors, n'augmentarà el risc potencial. Un altre factor és l'origen de la violació, és a dir, si és accidental o deliberada. No és el mateix que les dades s'hagin enviat per error a una tercera persona, especialment si és de confiança, que si estan en mans d'un hacker que no sabem quines intencions té. Finalment, també cal analitzar la facilitat o dificultat amb què els tercers no autoritzats poden identificar els titulars de les dades afectades.

I en cas que calgui notificar la violació a l'Autoritat, com s'ha de fer i quina informació cal proporcionar?

A la seu electrònica de l'APDCAT hi podreu trobar el formulari de notificació. S'hi ha d'incloure, entre d'altres, una descripció de la violació, quan s'ha produït, el tipus de dades i col·lectius afectats, les possibles conseqüències adverses per a les persones, si s'ha comunicat o no als afectats i les mesures que s'han pres. Aquesta informació permetrà a l'Autoritat analitzar si el responsable ha actuat adequadament per fer front a la violació, i si no és així, l'Autoritat li requerirà que ho faci sense dilació. També si considera que cal comunicar la violació a les persones afectades.

Què passa si en el termini de 72 hores no disposem encara de tota la informació?

Si el responsable no té tota la informació, pot fer la notificació per fases: una primera notificació inicial i, després, complementar-la i justificar els motius del retard.

Té conseqüències el fet de no notificar a l'Autoritat una violació quan és obligatori fer-ho?

Sí, efectivament. Pot donar lloc a sancions econòmiques molt elevades, a banda de perjudicar la reputació de qui hagi patit la violació de seguretat i no ho notifiqui. Per tant, davant del dubte, és millor notificar-ho o bé consultar-ho a l'APDCAT.

Ja per tancar, i tenint en compte tot el que hem parlat fins ara, què consideres que és imprescindible perquè una organització pugui fer front a una violació de la seguretat de les dades personals amb garanties?

Com ja he dit al principi, és indispensable disposar d'avant mà d'un pla de resposta que
prevegi tot els passos que cal fer, i de quina manera s'ha de fer. Aquest pla de resposta ha de tenir com a focus la protecció de les persones.

Perfecte, moltes gràcies per aclarir-nos tots els dubtes.

A vosaltres!

I fins aquí el quart capítol de "Parlem de dades personals", el pòdcast de l'Escola d'Administració Pública de Catalunya i l'Autoritat Catalana de Protecció de Dades. Avui amb l'Olga Rierola, coordinadora de la unitat de gestió de notificacions de violacions de seguretat de l'Autoritat Catalana de Protecció de Dades, hem aclarit què cal fer en cas d'una violació de la seguretat de les dades. Una situació que, com hem vist, mai podrem prevenir al 100%. I és per això que és clau saber com reaccionar, si es produeix, i com evitar que ens torni a passar en un futur. Us esperem en el pròxim capítol de "Parlem de dades personals", on continuarem aprofundint en aspectes relacionats amb el tractament i la protecció de dades. Fins aviat!