Comitè Europeu de Protecció de Dades (CEPD)

Directrius 9/2022 sobre la notificació de les violacions de la seguretat de les dades personals segons l'RGPD

Versió 2.0

Adoptades el 28 de març de 2023

(versió actualitzada de les directrius WP250 adoptades pel Grup de treball de l'article 29 el 25 de maig de 2018)

(Traducció no oficial al català del text oficial publicat en anglès)
Guidelines 9/2022 on personal data breach notification under GDPR (version 2.0)

Historial de versions

Versió 1.0	10 d'octubre de 2022	Adopció de les Directrius (versió actualitzada de les directrius prèvies WP205 (rev.01), aprovades pel Grup de treballa de l'article 29 i confirmades per l'EDPB el 25 de maig de 2018) per a exposició pública
Versió 20.	28 de març de 2023	Adopció de les Directrius sobre la notificació de violacions de seguretat per a responsables del tractament, després de l'exposició pública

ÍNDEX

El Comitè Europeu de Protecció de Dades

Vist l'article 70.1, lletres *e* i *l*, del Reglament 2016/679/UE del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (RGPD),

Vist l'Acord sobre l'EEA (Àrea Econòmica Europea) i, en particular, l'annex XI i el seu protocol 37, modificat per la decisió de l'EEA juntament amb el Comitè núm. 154/2018, de 6 de juliol de 2018,[1]

Vistos l'article 12 i l'article 22 del seu Reglament,

Vistes les Directrius del Grup de treball de l'article 29 sobre la notificació de violacions de dades personals d'acord amb el Reglament 2016/679, WP250 rev. 01,

Ha adoptat les directrius següents

0. Prefaci

1. El 3 d'octubre de 2017, el Grup de l'article 29 (WP29) va adoptar les Directrius sobre la notificació de la violació de seguretat de les dades personals segons el Reglament 2016/679 (WP250),[2] que el Comitè Europeu de Protecció de Dades (CEPD) va aprovar en la seva primera reunió plenària.[3] Aquest document una versió lleugerament actualitzada d'aquelles directrius. D'ara endavant, qualsevol referència a les Directrius sobre la notificació de la violació de seguretat de les dades personals segons el Reglament 2016/679 (WP250) s'ha d'interpretar com una referència a aquestes Directrius 9/2022 del CEPD.

2. El CEPD es va adonar que calia aclarir els requisits de notificació de les violacions de seguretat de les dades personals en organitzacions no comunitàries. El paràgraf referent a aquesta qüestió s'ha revisat i actualitzat; a la resta del document no s'hi han introduït canvis, tret dels editorials. La revisió afecta, més concretament, el paràgraf 73 de la secció II.C.2 d'aquest document.

INTRODUCCIÓ

3. El Reglament general de protecció de dades (RGPD) va introduir el requeriment que les violacions de les dades personals (d'ara endavant, "violacions") s'han de notificar a l'autoritat de control competent[4] (o, en cas de violació transfronterera, a l'autoritat d'origen) i, en determinats casos, comunicar-la a les persones titulars de les dades que s'han vist afectades per la violació.

[1] Les referències a "estats membres" fetes al llarg d'aquest document s'han d'entendre com a referències als estats membres de l'Àrea Econòmica Europea.
[2] Revisades i actualitzades el 6 de febrer de 2018, disponibles a https://ec.europa.eu/newsroom/article29/items/612052.
[3] Vegeu https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en.
[4] Vegeu l'article 4.21 de l'RGPD.

4. L'obligació de notificar les violacions ja era un requeriment per a determinades organitzacions, com ara proveïdors de serveis de comunicacions electròniques públicament disponibles (com especifiquen la Directiva 2009/136/EC i el Reglament (UE) 611/2013).[5] També hi ha alguns estats membres de la UE que ja tenien establerta una obligació de notificació de les violacions d'àmbit nacional. Això podia incloure l'obligació de notificar violacions que impliquen categories de responsables, a més de proveïdors de serveis de comunicació electròniques públicament disponibles (per exemple, a Alemanya i Itàlia), o bé una obligació d'informar de totes les violacions que afecten dades personals (com als Països Baixos). Altres estats membres podien tenir codis de bones pràctiques aplicables (per exemple, Irlanda).[6] Mentre que hi havia un cert nombre d'autoritats de protecció de dades de la UE que instaven els responsables a comunicar violacions, la Directiva de protecció de dades 95/46/EC,[7] que l'RGPD substitueix, no contenia una obligació específica de notificació de violació i, per això, aquest requisit va ser nou per a moltes organitzacions. L'RGPD converteix en obligatòria la notificació per a tots els responsables, tret que sigui improbable que una violació ocasioni un risc per als drets i llibertats de les persones.[8] Els encarregats del tractament també hi tenen un paper important i han de notificar qualsevol violació al seu responsable.[9]

5. El CEPD considera que el requeriment de notificació té nombrosos beneficis. En fer la notificació a l'autoritat de control, els responsables poden obtenir recomanacions respecte de si cal informar les persones afectades. En efecte, l'autoritat de control pot ordenar al responsable que informi aquests afectats de la violació.[10] El fet de comunicar una violació a les persones afectades permet al responsable proporcionar informació sobre els riscos existents com a resultat de la violació, així com sobre les accions que aquests afectats poden dur a terme per protegir-se de les seves conseqüències potencials. El focus de qualsevol pla de resposta a una violació ha de ser protegir les persones afectades i les seves dades personals. Consegüentment, la notificació de la violació s'ha de veure com una eina de reforç del compliment en relació amb la protecció de les dades personals. Alhora, d'acord amb l'article 83 cal tenir en compte que l'omissió de comunicació d'una violació, tant a una persona afectada com a una autoritat de control, pot significar que s'apliqui una sanció al responsable.

6. S'insta els responsables i els encarregats del tractament a planificar i aplicar procediments per detectar i contenir ràpidament una violació, avaluar el risc per a les persones afectades[11] i determinar si cal notificar-la a l'autoritat de control competent i

[5] Vegeu http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0136 i http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R0611.
[6] Vegeu https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm.
[7] Vegeu http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046.
[8] Els drets consagrats a la Carta dels Drets Fonamentals de la UE, disponible a http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT.
[9] Vegeu l'article 33.2 RGPD. És similar en concepte a l'article 5 del Reglament (UE) núm. 611/2013, que estableix que un proveïdor que es contracta per prestar part d'un servei de comunicacions electròniques (sense tenir una relació contractual directa amb els subscriptors) està obligat a notificar al proveïdor de contractació un incident de dades personals.
[10] Vegeu els articles 34.4 i 58.2.*e* RGPD.
[11] Això es pot garantir sota el requisit de supervisió i revisió d'una AIPD, necessària per a operacions de tractament que puguin provocar un risc alt per als drets i llibertats de les persones físiques (article 35, apartats 1 i 11).

comunicar-la a les persones afectades. La notificació a l'autoritat de control ha de formar part del pla de resposta a l'incident.

7. L'RGPD preveu quan cal notificar una violació, i a qui, així com la informació que cal proporcionar a la notificació. Aquesta informació es pot proporcionar per fases, però els responsables han d'actuar sense dilació enfront de qualsevol violació.

8. En la seva Opinió 03/2014 sobre la notificació de violacions de dades personals,[12] el WP29 proporcionava orientacions per ajudar els responsables a decidir si cal la violació a les persones afectades. L'opinió analitzava l'obligació dels proveïdors de comunicacions electròniques segons la Directiva 2002/58/EC i oferia exemples de múltiples sectors, en el context del que llavors era l'esborrany d'RGPD, i presentava bones pràctiques per a tots els responsables.

9. Les directrius actuals expliquen la notificació obligatòria de la violació i els requisits de la comunicació establerts a l'RGPD, així com alguns dels passos que poden fer els responsables i els encarregats del tractament per complir aquestes obligacions. També ofereixen exemples de diversos tipus de violacions i a qui caldria notificar-les, en supòsits diferents.

I. La notificació de violació de dades personals a l'RGPD

A. Consideracions de seguretat bàsiques

10. Un dels requisits de l'RGPD és que, emprant les mesures tècniques i organitzatives apropiades, les dades personals s'han de tractar de la manera adequada per garantir-ne la seguretat, inclosa la protecció contra el tractament no autoritzat o il·lícit i contra la pèrdua, la destrucció o el dany accidentals.[13]

11. Consegüentment, l'RGPD exigeix que tant els responsables com els encarregats del tractament implantin les mesures tècniques i organitzatives necessàries per garantir un nivell de seguretat apropiat al risc per a les dades personals tractades. Han de tenir en compte la tecnologia avançada, els costos de la implementació i la naturalesa, l'abast, el context i la finalitat del tractament, així com la variació de la probabilitat i la gravetat del risc per als drets i llibertats de les persones.[14] L'RGPD també exigeix la protecció tecnològica i les mesures organitzatives adequades per poder establir immediatament si hi ha hagut una violació, cosa que determina si hi ha l'obligació de notificació.[15]

12. En conseqüència, un element clau de qualsevol política de seguretat de dades és, en la mesura del possible, ser capaç d'evitar una violació i, si tot i això es produeix, reaccionar-hi amb celeritat.

---

[12] Vegeu l'Opinió 03/2014 sobre la notificació d'incompliment de dades personals http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf.
[13] Vegeu els articles 5.1.*f* i 32 RGPD.
[14] Article 32; vegeu també el considerant 83 RGPD.
[15] Vegeu el considerant 87 RGPD.

B. Què és una violació de seguretat de dades personals?

1. Definició

13. Com a part de qualsevol intent de contenir una violació, primerament el responsable ha de ser capaç de reconèixer-la. A l'article 4.12, l'RGPD defineix una "violació de seguretat de dades personals" com:

> "Qualsevol violació de la seguretat que ocasiona la destrucció accidental o il·legal, la pèrdua, l'alteració, la revelació no autoritzada o l'accés a dades personals transmeses, emmagatzemades o sotmeses a qualsevol tractament."

14. Ha de quedar clar què s'entén per "destrucció" de dades personals: quan les dades ja no existeixen, o no existeixen en una forma en què el responsable en pot fer ús. El concepte "dany" també ha de ser clar: quan les dades personals han estat alterades, malmeses o ja no són completes. En termes de "pèrdua" de dades personals s'ha d'interpretar que pot ser que les dades encara existeixin, però el responsable n'ha perdut el control o l'accés, o ja no les té. Finalment, el tractament no autoritzat o il·legal pot incloure revelació de dades personals (o accés) a destinataris que no estan autoritzats a rebre-les o a accedir-hi, o qualsevol altra forma de tractament que infringeixi l'RGPD.

> **Exemple**
>
> Un exemple de pèrdua de dades personals pot incloure un dispositiu que s'ha perdut o ha estat sostret i que conté una còpia de la base de dades de clients d'un responsable. Un altre exemple de pèrdua pot ser que l'única còpia d'un conjunt de dades personals hagi estat encriptada amb un programari de segrest (*ransomware*), o hagi estat encriptada pel responsable amb una clau que ja no té.

15. El que cal tenir clar és que una violació és un tipus d'incident de seguretat. No obstant això, d'acord amb l'article 4.12, l'RGPD només és d'aplicació quan hi ha una violació de *dades personals*. La conseqüència d'aquesta violació és que el responsable no pot garantir que es compleixen els principis relatius al tractament de les dades personals, tal com es detallen a l'article 5 de l'RGPD. Això remarca la diferència entre un incident de seguretat i una violació de dades personals, que és, en essència, que així com totes les violacions de dades personals són violacions de seguretat, no totes les vulneracions de seguretat són necessàriament violacions de dades personals.[16]

16. A continuació, s'analitzen els possibles efectes adversos d'una violació per a les persones.

[16] Cal assenyalar que un incident de seguretat no es limita als models d'amenaces en què es produeix un atac en una organització des d'una font externa, sinó que inclou incidències de tractament intern que incompleixen els principis de seguretat.

2. Tipus de violacions de dades personals

17. En la seva Opinió 03/2014 sobre la notificació de la violació, el WP29 explicava que les violacions es poden classificar d'acord amb els següents tres principis de seguretat de la informació:[17]

- **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[18] o la destrucció de dades personals.

18. També cal assenyalar que, depenent de les circumstàncies, una violació pot afectar alhora la confidencialitat, la integritat i la disponibilitat de dades personals, així com qualsevol combinació de les tres.

19. Mentre que determinar si hi ha hagut una violació de la confidencialitat o la integritat resulta relativament clar, determinar si s'ha produït un incident de disponibilitat pot ser menys evident. Quan hi ha hagut una pèrdua permanent o la destrucció de dades personals, la violació sempre es considera incident de disponibilitat.

> **Exemple**
>
> Els exemples de pèrdua de disponibilitat inclouen quan les dades han estat eliminades accidentalment o per una persona no autoritzada o, en l'exemple de dades xifrades de forma segura, la clau de desxifratge s'ha perdut. Si el responsable no pot restaurar l'accés a les dades, per exemple a partir d'una còpia de seguretat, es considera que hi ha una pèrdua permanent de disponibilitat.
>
> També hi pot haver una pèrdua de disponibilitat quan hi ha hagut una interrupció significativa del servei normal d'una organització; per exemple, si es produeix una fallada o un atac de denegació de servei, cosa que deixa dades personals no disponibles.

20. El que es pot preguntar és si una pèrdua temporal de la disponibilitat de dades personals s'ha de considerar com una violació i, en cas afirmatiu, si cal notificar-la.

---

[17] Vegeu l'Opinió 03/2014.

[18] Està ben establert que "accés" és fonamentalment part de "disponibilitat". Vegeu, per exemple, NIST SP800-53rev4, que defineix "disponibilitat" com: "Garantir l'accés i l'ús de la informació a temps i fiable", disponible a http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. El CNSSI-4009 també es refereix a: "la propietat de ser accessible i utilitzable a petició d'una entitat autoritzada". Vegeu https://rmf.org/images/4-CNSS-Publications/CNSSI-4009.pdf. La ISO / IEC 27000: 2016 també defineix la "disponibilitat" com a "Propietat de ser accessible i utilitzable sota demanda per una entitat autoritzada": https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en.

L'article 32 de l'RGPD, "seguretat del tractament", explica que quan s'implementen mesures tècniques i organitzatives per garantir un nivell de seguretat adequat al risc cal considerar, entre altres coses, "la capacitat de garantir permanentment la confidencialitat, la integritat, la disponibilitat i la capacitat de recuperació dels sistemes i serveis de tractament", així com "la capacitat de restaurar la disponibilitat i l'accés a les dades personals amb celeritat, en cas d'un incident físic o tècnic".

21. Per tant, una violació de seguretat que impedeix que les dades personals estiguin disponibles durant un període de temps també és un tipus de violació, ja que la manca d'accés a les dades pot tenir un impacte significatiu en els drets i les llibertats de les persones. Perquè quedi clar, quan les dades personals no estan disponibles a causa del manteniment planificat del sistema, no es tracta d'un "incident de seguretat" tal com es defineix a l'article 4.12.

22. Igual com amb la pèrdua permanent o la destrucció de dades personals (o, de fet, qualsevol altre tipus de violació), cal documentar una violació que comporta la pèrdua temporal de disponibilitat d'acord amb l'article 33.5. Això ajuda el responsable a demostrar la responsabilitat proactiva (*accountability*) davant l'autoritat de control, que pot demanar veure aquests registres.[19] No obstant això, depenent de les circumstàncies, pot caldre o no notificar la violació a l'autoritat de control i comunicar-la a les persones afectades. El responsable ha d'avaluar la probabilitat i la gravetat de l'impacte sobre els drets i les llibertats de les persones, com a conseqüència de la manca de disponibilitat de les dades personals. De conformitat amb l'article 33, el responsable l'ha de notificar, tret que sigui poc probable que la violació constitueixi un risc per als drets i llibertats de les persones. Per descomptat, això s'ha d'avaluar cas per cas.

Exemples

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.

A la inversa, en el cas que els sistemes d'una empresa de mitjans de comunicació no estiguin disponibles durant diverses hores (per exemple, a causa d'un tall d'energia), si es preveu que l'empresa no podria enviar butlletins d'informació (*newsletter*) als seus subscriptors, és poc probable que això suposi un risc per als drets i les llibertats de les persones.

23. Cal assenyalar que, tot i que la pèrdua de la disponibilitat dels sistemes d'un responsable pot ser només temporal i pot no tenir un impacte sobre les persones, és important que el responsable analitzi totes les possibles conseqüències d'una violació, ja que pot caldre notificar-la per altres raons.

[19] Vegeu l'article 33.5 RGPD.

Exemple

La infecció per *ransomware* (programari maliciós que encripta les dades fins que es paga un rescat) pot provocar una pèrdua temporal de la disponibilitat, si les dades es poden restaurar a partir de còpies de seguretat. Tot i això, encara es produeix una intrusió a la xarxa i, si l'incident es qualifica com a violació de la confidencialitat (és a dir, l'atacant accedeix a dades personals) i això implica un risc per als drets i les llibertats de les persones, pot caldre notificar-la.

3. Les possibles conseqüències d'una violació de dades personals

24. Una violació pot tenir potencialment un ventall d'efectes adversos significatius sobre les persones, que poden provocar danys físics, materials o no materials. L'RGPD explica que això pot incloure pèrdua de control sobre les seves dades personals, limitació dels seus drets, discriminació, robatori d'identitat o frau, pèrdua financera, reversió no autoritzada de pseudonimització, dany per a la reputació i pèrdua de confidencialitat de dades personals protegides pel secret professional. També pot incloure qualsevol altre desavantatge econòmic o social important per a aquestes persones.[20]

25. En conseqüència, l'RGPD requereix que el responsable notifiqui una violació a l'autoritat de control competent, tret que no sigui probable que es produeixin efectes tan adversos. Quan hi ha un alt risc probable d'aquests efectes adversos, l'RGPD exigeix que el responsable comuniqui la violació a les persones afectades tan aviat com sigui raonablement possible.[21]

26. El considerant 87 de l'RGPD remarca la importància de poder identificar una violació, avaluar-ne el risc per a les persones i, si escau, notificar-la:

"Cal saber si s'han implementat totes les mesures de protecció tecnològica i organitzatives adequades per determinar immediatament si s'ha produït una violació de dades personals, i informar-ne ràpidament l'autoritat de control i les persones afectades. S'hauria de notificar sense dilació indeguda, tenint en compte, en particular, la naturalesa i la gravetat de la violació de dades personals i les seves conseqüències i efectes adversos per als afectats. Aquesta notificació pot tenir com a conseqüència una intervenció de l'autoritat de control, d'acord amb les seves funcions i competències establertes en aquest Reglament."

27. A la secció IV s'analitzen altres pautes d'avaluació del risc d'efectes adversos per a les persones.

28. Si, tot i que es compleixen els requisits dels articles 33 i/o 34, els responsables no notifiquen una violació de seguretat de les dades a l'autoritat de control o als afectats, o a cap dels dos, l'autoritat de control pot considerar totes les mesures correctores al

[20] Vegeu també els considerants 85 i 75 RGPD.
[21] Vegeu també el considerant 86 RGPD.

seu abast, ja sigui únicament una sanció administrativa,[22] o bé la sanció acompanyada d'una mesura correctora d'acord amb l'article 58.2. Si s'opta per una multa administrativa, el valor pot ser d'un màxim de 10.000.000 euros o fins a un 2 % de la facturació global anual d'una empresa, a l'empara de l'article 83.4.*a* de l'RGPD. També és important tenir en compte que, en alguns casos, la manca de notificació d'una violació pot revelar l'absència de mesures de seguretat o bé que les mesures existents són insuficients. Les directrius del WP29 sobre sancions administratives afirmen: "L'aparició de diverses violacions diferents en un mateix cas significa que l'autoritat de control pot aplicar les multes administratives a un nivell eficaç, proporcionat i dissuasiu dins del límit de les infraccions més greus." En aquest cas, l'autoritat de control també pot imposar sancions per no haver notificat o comunicat la violació (articles 33 i 34 RGPD), d'una banda, i d'altra banda per l'absència de mesures de seguretat adequades (article 32 RGPD), ja que són dues infraccions separades.

II. Article 33 - Notificació a l'autoritat de control

A. Quan cal fer la notificació

1. Requeriments de l'article 33

29. L'article 33.1 estableix que:

> "En el cas d'una violació de dades personals, sense demora i, quan sigui factible, a partir de les 72 hores posteriors a la seva notificació, el responsable ha de notificar la violació de les dades personals a l'autoritat de control competent d'acord amb l'article 55, tret que sigui poc probable que la violació de dades personals comporti un risc per als drets i les llibertats de les persones físiques. Quan la notificació a l'autoritat de control no es dugui a terme en el termini de 72 hores, ha d'anar acompanyada dels motius de la demora."

30. El considerant 87 afirma:[23]

> "Cal saber si s'han implementat totes les mesures de protecció tecnològica i organitzatives adequades per determinar immediatament si s'ha produït una violació de dades personals, i informar-ne ràpidament l'autoritat de control i les persones afectades. La notificació s'hauria de fer sense dilació indeguda, tenint en compte, en particular, la naturalesa i la gravetat de la violació de dades personals i les conseqüències i els efectes adversos que pot tenir per a les persones afectades. Aquesta notificació pot tenir com a conseqüència una intervenció de l'autoritat de control, d'acord amb les seves funcions i competències establertes en aquest Reglament."

[22] Per a més informació, consulteu les guies del WP29 sobre l'aplicació i definició de les multes administratives, disponibles aquí: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889.
[23] Aquí el considerant 85 RGPD també és important.

2. Quan un responsable “en pren consciència"?

31. Tal com s'ha detallat anteriorment, l’RGPD requereix que, en cas de violació, el responsable notifiqui aquesta violació sense dilació indeguda i, quan sigui possible, com a màxim al cap de 72 hores d’haver-la detectat. Això pot plantejar la pregunta de quan es pot considerar que un responsable “ha pres consciència” d'una violació. L’EDPB considera que un responsable n’és conscient quan té un grau de certesa raonable que s'ha produït un incident de seguretat que ha compromès les dades personals.

32. Tot i això, com ja s'ha indicat, l’RGPD requereix que el responsable implementi totes les mesures tècniques i organitzatives adequades per determinar immediatament si s'ha produït una violació, i informar-ne ràpidament l'autoritat de control i els afectats. També estableix que el fet que la notificació es faci sense demora injustificada ha de tenir en compte, en particular, la naturalesa i la gravetat de la violació i les seves conseqüències i efectes adversos per a les persones afectades.[24] Això obliga el responsable a assegurar-se que “prendrà consciència" de qualsevol violació a temps per poder prendre les mesures oportunes.

33. El moment exacte en què es pot considerar que un responsable “pren consciència" d'una violació concreta depèn de les circumstàncies d’aquella violació. En alguns casos, serà relativament clar des del principi que hi ha hagut una violació, mentre que en d'altres pot caldre un cert temps per determinar si les dades personals han

Exemples

1. En cas de pèrdua d’una memòria USB amb dades personals no xifrades, sovint no es pot determinar si persones no autoritzades han accedit a aquestes dades. Això no obstant, tot i que el responsable no pugui establir si s'ha produït una violació de la confidencialitat, s'ha de notificar perquè hi ha un grau raonable de certesa que s'ha produït una violació de la disponibilitat; el responsable n’ha “pres consciència" quan s’ha adonat que l’USB s'havia perdut.

2. Un tercer informa un responsable que ha rebut accidentalment les dades personals d'un dels seus clients i proporciona l’evidència de la divulgació no autoritzada. Atès que al responsable se li ha presentat l’evidència clara d’una violació de la confidencialitat, no hi ha dubte que n’ha “pres consciència".

3. Un responsable detecta que hi ha hagut una possible intrusió a la seva xarxa. El responsable comprova els seus sistemes, per determinar si les dades personals emmagatzemades en aquest sistema s'han vist compromeses, i confirma que sí. Una vegada més, el responsable té proves clares d'una violació i no hi ha dubte que n’ha “pres consciència".

4. Un ciberdelinqüent es posa en contacte amb el responsable després d'haver piratejat el seu sistema, per sol·licitar un rescat. En aquest cas, després de comprovar que el seu sistema ha estat atacat, el responsable té l’evidència clara que s'ha produït una violació i no hi ha cap dubte que n’és conscient.

[24] Vegeu el considerant 87 RGPD.

estat compromeses. Tot i això, l'èmfasi s'hauria posar en una ràpida acció per investigar un incident, a fi de determinar si les dades personals han estat afectades per la violació i, si és així, prendre mesures correctores i notificar-ho, si escau.

34. Després que una persona, un mitjà de comunicació o una altra font hagin informat d'una possible violació, o quan s'ha detectat una violació de seguretat, el responsable pot obrir un breu període d'investigació per determinar si s'ha produït o no una violació. Durant aquest període, el responsable no es pot considerar "conscient". Tot i això, cal esperar que la investigació inicial comenci al més aviat possible i determini amb un cert grau de certesa si s'ha produït una violació; després, es pot continuar amb una investigació més detallada.

35. Una vegada el responsable n'ha tingut coneixement, l'ha de notificar sense dilació indeguda i, quan sigui possible, com a màxim al cap de 72 hores. Durant aquest període, el responsable ha d'avaluar el possible risc per a les persones, per determinar si s'ha activat el requeriment de notificació, així com dur a terme les accions necessàries per fer front a la violació. Tot i això, pot ser que un responsable ja tingui una avaluació inicial del risc potencial que es podria derivar d'una violació, com a part d'una avaluació d'impacte relativa a la protecció de dades (AIPD)[25] executada abans de l'operació de tractament en qüestió. Això no obstant, l'AIPD pot ser més general, en comparació amb les circumstàncies específiques de la violació real, de manera que cal fer una avaluació addicional tenint en compte aquestes circumstàncies. Per a més informació sobre l'avaluació del risc, consulteu la secció IV.

36. En la majoria dels casos, aquestes accions preliminars s'han de completar poc temps després de l'alerta inicial (és a dir, quan el responsable o l'encarregat sospita que hi ha hagut una violació de seguretat que pot afectar dades personals).

> **Exemple**
>
> Una persona informa el responsable que ha rebut un correu electrònic que suplanta la identitat d'aquest responsable, que conté dades personals relacionades amb l'ús (real) del servei del responsable i que suggereix que la seguretat del responsable s'ha vist compromesa. El responsable obre un curt període d'investigació, identifica una intrusió a la seva xarxa i obté proves d'accés no autoritzat a dades personals. Ara el responsable es pot considerar "conscient" i cal que ho notifiqui a l'autoritat de control, tret que sigui poc probable que presenti un risc per als drets i les llibertats de les persones. El responsable ha de prendre les mesures correctores adequades per fer front a la violació.

37. Per tant, el responsable hauria de tenir procediments interns per detectar i tractar una violació. Per exemple, a fi de trobar irregularitats en el tractament de les dades, el responsable o l'encarregat poden utilitzar determinades mesures tècniques, com ara el flux de dades i l'anàlisi dels registres de sessió (*logs*), amb les quals es poden

[25] Vegeu les directrius del WP29 sobre AIPD aquí: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137.

identificar incidents i alertes.[26] És important que, quan es detecta una violació, la informació arribi fins al nivell adequat de gestió, de manera que es pugui abordar i, si cal, notificar-la d'acord amb l'article 33 i, si escau, l'article 34. Aquests mecanismes d'informació i mesures es poden detallar en els plans de resposta a les violacions elaborats pel responsable i/o en els acords de govern. Això ajudarà el responsable a fer una planificació efectiva i determinar qui, dins de l'organització, té la responsabilitat operativa per gestionar una violació, i com escalar-la als nivells de responsabilitat adequats.

38. El responsable també ha d'establir acords amb qualsevol encarregat, el qual ja té l'obligació de notificar al responsable qualsevol cas de violació (vegeu més avall).

39. Si bé és responsabilitat dels responsables i encarregats del tractament establir mesures adequades per poder prevenir, reaccionar i abordar una violació, hi ha alguns passos pràctics que cal seguir en qualsevol cas.

- La informació relativa a tots els esdeveniments relacionats amb la seguretat s'hauria d'adreçar a la persona o persones que tenen assignada la tasca d'abordar incidències, establir l'existència d'una violació i avaluar-ne el risc.

- Cal avaluar el risc per a les persones afectades com a conseqüència d'una violació (és a dir, la probabilitat que no hi hagi risc, que n'hi hagi o que sigui alt) i informar-ne els nivells pertinents de l'organització.

- Cal notificar-la a l'autoritat de control i, si escau, es pot comunicar als afectats.

- Al mateix temps, el responsable ha d'actuar per frenar la violació i recuperar-se'n.

40. En conseqüència, ha de quedar clar que el responsable té l'obligació d'actuar sobre qualsevol alerta inicial i determinar si s'ha produït o no una violació. Aquest breu període permet fer alguna investigació i que el responsable reculli proves i altres detalls rellevants. No obstant això, una vegada el responsable ha establert amb un grau raonable de certesa que s'ha produït una violació, si hi concorren les condicions que estableix l'article 33.1 l'ha de notificar a l'autoritat de control sense dilació indeguda i, si és possible, com a màxim al cap de 72 hores.[27] Si un responsable no actua amb promptitud i es fa evident que s'ha produït una violació, es podria considerar que ha omès la notificació que estableix l'article 33.

41. L'article 32 deixa clar que el responsable i l'encarregat han de tenir implantades les mesures tècniques i organitzatives apropiades per garantir un nivell adequat de seguretat de les dades personals: la capacitat de detectar, atendre i comunicar una infracció amb promptitud s'ha de considerar un element essencial d'aquestes mesures.

[26] Cal assenyalar que les dades de registre que faciliten l'auditoria de l'emmagatzematge, les modificacions o l'esborrat de dades, per exemple, també poden qualificar-se de dades personals relacionades amb la persona que va iniciar l'operació de tractament.
[27] Vegeu el Reglament núm. 1182/71, pel qual es determinen les normes aplicables als períodes, dates i terminis, disponible a: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31971R1182&from=EN.

3. Corresponsables

42. L'article 26 de l'RGPD es refereix als corresponsables i especifica que han d'establir les seves respectives responsabilitats respecte del compliment de l'RGPD.[28] Això inclou determinar quina de les parts es responsabilitza del compliment de les obligacions establertes als articles 33 i 34. El CEPD recomana que els acords contractuals entre els corresponsables incloguin disposicions que estableixin quin responsable ha de prendre la iniciativa o és responsable de complir l'obligació de notificació, d'acord amb l'RGPD.

4. Obligacions de l'encarregat

43. El responsable manté la responsabilitat general de protegir les dades personals, però el rol de l'encarregat és molt important perquè el responsable pugui complir amb les seves obligacions; això inclou notificar una violació. De fet, l'article 28.3 de l'RGPD disposa que un encàrrec de tractament s'ha de regir per un contracte o un altre acte jurídic. L'article 28.3.*f* estableix que el contracte o acte jurídic ha d'estipular 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 de què disposa l'encarregat."

44. L'article 33.2 deixa clar que si un responsable té un encarregat i aquest encarregat detecta una violació de les dades personals que està tractant per compte del responsable, l'hi ha de notificar "sense dilació indeguda". Cal assenyalar que l'encarregat no necessita avaluar la probabilitat de risc derivat d'una violació, abans de notificar-la al responsable; és el responsable qui ha de fer aquesta valoració, en conèixer la violació. L'encarregat només ha de determinar si s'ha produït la violació i, després, notificar-ho al responsable. El responsable utilitza l'encarregat per aconseguir els seus objectius; per tant, en principi, s'hauria de considerar que el responsable n'és "conscient" una vegada l'encarregat l'ha informat de la violació. L'obligació que l'encarregat n'informi el responsable permet al responsable fer front a la violació i determinar si cal o no notificar-la a l'autoritat de control, d'acord amb l'article 33.1, i a les persones afectades, d'acord amb l'article 34.1. El responsable també pot voler investigar la violació, ja que pot ser que l'encarregat no estigui en condicions de conèixer tots els fets rellevants relacionats amb la qüestió; per exemple, si el responsable encara conserva una còpia de seguretat de les dades personals destruïdes o perdudes. Això pot afectar la determinació de si el responsable l'ha de notificar.

45. L'RGPD no proporciona un límit de temps explícit dins del qual l'encarregat ha d'advertir el responsable, tret que ho ha de fer "sense dilació indeguda". Per tant, el CEPD recomana que l'encarregat ho notifiqui ràpidament al responsable i que proporcioni més informació per fases, a mesura que es disposi de més informació.

[28] Vegeu també el considerant 79 RGPD.

Això és important per ajudar el responsable a complir el requeriment de notificació a l'autoritat de control en un termini de 72 hores.

46. Com s'explica més amunt, el contracte entre el responsable i l'encarregat ha d'especificar com s'han de complir els requeriments expressats a l'article 33.2, a més d'altres disposicions de l'RGPD. Això pot incloure requeriments perquè l'encarregat faci una primera i ràpida notificació, que ajuda el responsable en les seves obligacions d'informar l'autoritat de control en un termini de 72 hores.

47. Quan l'encarregat proporciona serveis a diversos responsables que es veuen afectats per la mateixa violació, l'encarregat ha d'informar dels detalls de la violació a cadascun d'ells.

48. Un encarregat pot fer una notificació en nom del responsable, si el responsable l'ha autoritzat i això forma part dels acords contractuals entre el responsable i l'encarregat. Aquesta notificació s'ha de fer d'acord amb els articles 33 i 34. Això no obstant, és important tenir en compte que la responsabilitat jurídica de notificar recau en el responsable.

B. Proporcionar informació a l'autoritat de control

1. Informació que cal proporcionar

49. Quan un responsable notifica una violació a l'autoritat de control, l'article 33.3 estableix que, com a mínim, ha de:

> "(a) Descriure la naturalesa de la violació de dades personals, incloent-hi, quan sigui possible, les categories i el nombre aproximat d'afectats i les categories i el nombre aproximat de bases de dades personals.
>
> (b) Comunicar el nom i les dades de contacte del delegat de protecció de dades o un altre punt de contacte on es pot obtenir més informació.
>
> (c) Descriure les possibles conseqüències de la violació de dades personals.
>
> (d) Descriure les mesures adoptades o proposades pel responsable per fer front a la violació de dades personals, incloses, si escau, mesures per mitigar-ne els possibles efectes adversos."

50. L'RGPD no defineix categories d'afectats o bases de dades personals. Tot i això, el CEPD suggereix *categories d'afectats* per referir-se als diferents tipus d'afectats les dades personals dels quals han estat afectades per una violació: depenent dels descriptors utilitzats, això pot incloure menors i altres col·lectius vulnerables, persones discapacitades, empleats o clients. De la mateixa manera, les categories de bases de dades personals poden fer referència a les diferents bases de dades que el responsable pot tractar, com ara dades de salut, historials educatius, informació sobre assistència social, informació financera, números de compte bancari, números de passaports, etc.

51. El considerant 85 de l'RGPD deixa clar que una de les finalitats de la notificació és limitar el dany als individus. En conseqüència, si els tipus d'afectats o els tipus de dades personals indiquen que hi ha un risc de dany particular com a conseqüència d'una violació (per exemple, suplantació d'identitat, frau, pèrdua financera o amenaça per al secret professional), és important que la notificació indiqui aquestes categories. D'aquesta manera, queda vinculat al requeriment de descriure les possibles conseqüències de la violació.

52. El fet que no hi hagi informació precisa (per exemple, el nombre exacte d'afectats) no ha d'impedir notificar la violació amb promptitud. L'RGPD permet fer aproximacions sobre el nombre de persones afectades i el nombre de bases de dades personals. L'enfocament s'ha d'orientar a abordar els efectes adversos de la violació, més que a proporcionar dades precises.

53. Per tant, quan ha quedat clar que s'ha produït una violació, però encara no se'n coneix l'abast, la notificació per fases (vegeu a continuació) és una manera segura de complir les obligacions de notificació.

54. L'article 33.3 de l'RGPD estableix que el responsable ha de proporcionar "com a mínim" aquesta informació amb una notificació; per tant, un responsable pot triar proporcionar més detalls, si escau. Els diferents tipus de violacions (confidencialitat, integritat o disponibilitat) poden requerir que es proporcioni més informació, per explicar completament les circumstàncies de cada cada cas.

> **Exemple**
>
> Com a part de la notificació a l'autoritat de control, un responsable pot considerar útil esmentar el seu encarregat, si és a l'origen de la violació, sobretot si ha comportat una violació que afecta les bases de dades personals d'altres responsables que utilitzen el mateix encarregat.

55. En qualsevol cas, com a part de la seva investigació sobre una violació, l'autoritat de control pot demanar més detalls.

2. Notificació per fases

56. Segons quina sigui la naturalesa de la violació, pot caldre que el reponsable faci una investigació addicional per establir tots els fets rellevants relacionats amb la violació. Respecte d'això, l'article 33.4 de l'RGPD estableix:

> "Quan no és possible proporcionar la informació al mateix temps, la informació es pot proporcionar en fases, sense demora addicional indeguda."

57. Això significa que l'RGPD reconeix que els responsables no sempre poden tenir tota la informació necessària sobre una violació dins de les 72 hores posteriors a haver-ne pres consciència, ja que és possible que durant aquest període inicial no disposi de la informació completa i detallada de la violació. En aquest cas, pot fer una notificació per fases. És probable que aquest sigui el cas de violacions més

complexes, com ara algun tipus d'incidents de ciberseguretat en els quals, per exemple, pot caldre una investigació forense en profunditat per establir plenament la naturalesa de la violació i el grau en què s'han compromès les dades personals. En conseqüència, en molts casos el responsable haurà de fer-ne un seguiment i facilitar informació addicional en un moment posterior. Això és admissible, sempre que el responsable motivi la demora, d'acord amb l'article 33.1 de l'RGPD. El CEPD recomana que, quan el responsable fa la notificació inicial a l'autoritat de control, també informi aquesta autoritat del fet que encara no disposa de tota la informació requerida i que, més endavant, li proporcionarà més detalls. L'autoritat de control ha d'acordar com i quan s'ha de proporcionar la informació addicional. Això no impedeix que el responsable faciliti més informació en qualsevol altra fase, quan conegui detalls rellevants addicionals sobre la violació que cal que proporcioni a l'autoritat de control.

58. El requeriment de notificació està enfocat a encoratjar els responsables a actuar amb promptitud en una violació, contenir-la i, si és possible, recuperar les dades personals compromeses i buscar l'assessorament de l'autoritat de control. El fet de notificar-ho a l'autoritat de control en les primeres 72 hores pot permetre al responsable assegurar-se que la decisió de notificar o no la violació a les persones afectades és correcta.

59. Això no obstant, l'objectiu de la notificació a l'autoritat de control no és únicament obtenir orientacions sobre si cal fer la notificació a les persones afectades. És evident que, en alguns casos, per la naturalesa de la violació i la gravetat del risc, el responsable l'haurà de notificar sense demora a les persones afectades. Per exemple, si hi ha una amenaça immediata de robatori d'identitat o les categories especials de dades personals[29] es divulguen en línia, el responsable ha d'actuar sense demora injustificada per contenir la violació i comunicar-la a les persones interessades (vegeu la secció III). En circumstàncies excepcionals, això es pot fer fins i tot abans de notificar-ho a l'autoritat de control. La notificació a l'autoritat de control no pot servir de justificació per no comunicar la violació als afectats, quan cal fer-ho.

60. També hauria de quedar clar que, després de fer una notificació inicial, si una investigació de seguiment evidencia que la violació de seguretat s'ha contingut i que, de fet, no s'ha produït cap violació, el responsable pot informar-ne l'autoritat de control. Aquesta informació es pot afegir a la que ja se li havia proporcionat i, en conseqüència, quedarà registrat que no ha estat una violació. No hi ha cap penalització per informar d'un incident que, finalment, no és una violació.

[29] Vegeu l'article 9 RGPD.

Exemple

Un responsable notifica a l'autoritat de control, dins de les 72 hores des que s'ha detectat, que ha perdut una memòria USB que conté una còpia de les dades personals d'alguns dels seus clients. Més endavant, l'USB es troba dins de les instal·lacions del responsable i es recupera la informació. El responsable actualitza la informació a l'autoritat de control i demana que es modifiqui la notificació.

61. Cal assenyalar que la notificació per fases ja és un cas previst en les obligacions vigents de la Directiva 2002/58/CE, en el Reglament 611/2013 i en d'altres incidents notificats.

3. Notificacions fora de termini

62. L'article 33.1 de l'RGPD deixa clar que, si la notificació a l'autoritat de control no es fa en un termini de 72 hores, cal explicitar els motius de la demora. Això, juntament amb el concepte de notificació per fases, reconeix que un responsable no sempre pot notificar una violació en aquest termini de temps i que es pot permetre una notificació fora de termini.

63. Aquest escenari es pot produir, per exemple, quan un responsable pateix diverses violacions de confidencialitat similars durant un període curt de temps, que afecten un gran nombre d'afectats de la mateixa manera. El responsable pot prendre consciència d'una violació i, en iniciar la investigació i abans de la notificació, detectar altres violacions similars que tenen causes diferents. Depenent de les circumstàncies, el responsable pot necessitar un cert temps per establir l'abast de les violacions i, en lloc de notificar cada violació individualment, pot fer una notificació completa que representi diverses violacions molt similars, amb possibles causes diferents. Això pot comportar que la notificació a l'autoritat de control s'endarrereixi més enllà de les 72 hores després que el responsable hagi tingut coneixement d'aquestes violacions.

64. En sentit estricte, cada violació individual és una violació que cal notificar. Això no obstant, per evitar resultar reiteratiu, el responsable pot enviar una notificació "agrupada" que representi totes aquestes violacions. Això, sempre que es tracti del mateix tipus de dades personals que han sofert la mateixa mena de violació durant un període relativament curt de temps. Si es produeixen una sèrie de violacions que afecten diferents tipus de dades personals, i les violacions són de mena diferent, cadascuna de les violacions s'ha de notificar d'acord amb l'article 33.

65. Tot i que l'RGPD permet les notificacions retardades, això no s'hauria de veure com una cosa que es produeix regularment. Convé assenyalar que també es poden fer notificacions agrupades per a múltiples violacions similars comunicades en un termini de 72 hores.

C. Violacions transfrontereres i violacions en establiments no comunitaris

1. Violacions transfrontereres

66. En els tractaments transfronterers[30] de dades personals, una violació pot afectar les dades de persones en més d'un estat membre. L'article 33.1 deixa clar que, si es produeix una violació, el responsable l'ha de notificar a l'autoritat de control competent d'acord amb l'article 55 de l'RGPD.[31] L'article 55.1 diu:

> "Cada autoritat de control és competent per complir les tasques assignades i exercir les competències que té conferides d'acord amb aquest Reglament en el territori del seu propi Estat membre."

67. Això no obstant, l'article 56.1 estableix:

> "Sens perjudici de l'article 55, l'autoritat de control de l'establiment principal o de l'establiment únic del responsable o l'encarregat és competent per actuar com a autoritat de control principal per al tractament transfronterer efectuat per aquest responsable o encarregat, d'acord amb el procediment previst a l'article 60."

68. A més, l'article 56.6 estableix:

> "L'autoritat de control principal és l'únic interlocutor del responsable o encarregat per al tractament transfronterer efectuat per aquest responsable o encarregat."

69. Això significa que sempre que es produeixi una violació en el context d'un tractament transfronterer, el responsable l'ha de notificar a l'autoritat de control principal.[32] Per tant, en el moment de redactar el seu pla de resposta a la violació, el responsable ha d'avaluar quina és l'autoritat de control a la qual l'ha de notificar.[33] Això permetrà al responsable respondre amb promptitud a una violació i complir les seves obligacions respecte de l'article 33. Ha de quedar clar que una violació d'un tractament transfronterer s'ha de notificar a l'autoritat de control principal, que no necessàriament és el lloc on són els afectats, o fins i tot on s'ha produït la violació. En fer la notificació a l'autoritat principal, el responsable ha d'indicar, si escau, si la violació implica establiments situats en altres estats membres, i en quins d'aquests estats membres hi pot haver persones afectades per la violació. Si el responsable té dubtes sobre quina és l'autoritat de control principal, com a mínim ha de fer la notificació a l'autoritat de control local del lloc on s'ha produït la violació.

2. Violacions en establiments no comunitaris

[30] Vegeu l'article 4.23 RGPD.
[31] Vegeu també el considerant 122 RGPD.
[32] Vegeu les directrius del WP29 per identificar l'autoritat de control d'un responsable o un encarregat, disponible a http://ec.europa.eu/newsroom/document.cfm?doc_id=44102.
[33] Podeu trobar una llista de dades de contacte de totes les autoritats europees de protecció de dades nacionals a: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm.

70. L'article 3 es refereix a l'àmbit territorial de l'RGPD, inclòs quan s'aplica al tractament de dades personals fet per un responsable o encarregat que no està establert a la UE. En particular, l'article 3.2 estableix:[34]

> "Aquest Reglament s'aplica al tractament de dades personals d'afectats que resideixen a la Unió efectuat per un responsable o un encarregat no establert a la Unió, quan les activitats de tractament estan relacionades amb:
>
> a) L'oferta de béns o serveis als esmentats afectats a la Unió, independentment de si se'n requereix pagament o no.
>
> b) El control del seu comportament, si aquest comportament té lloc a la Unió."

71. L'article 3.3 també és rellevant i estableix el següent:[35]

> "Aquest Reglament s'aplica al tractament de dades personals efectuat per un responsable que no estigui establert a la Unió, però sí en un lloc on el dret dels estats membres és d'aplicació en virtut del dret internacional públic."

72. Quan un responsable no establert a la UE està subjecte als apartats 2 o 3 de l'article 3 de l'RGPD i pateix una violació, manté les obligacions de notificació establertes als articles 33 i 34. Quan és d'aplicació l'article 3.2, l'article 27 de l'RGPD requereix que el responsable i l'encarregat del tractament designin un representant a la Unió.

73. Tanmateix, la mera presència d'un representant en un Estat membre no activa el sistema de finestreta única.[36] Per aquest motiu, la violació s'ha de notificar a cada autoritat de control que tingui persones afectades residents al seu estat membre. Aquesta notificació o notificacions són responsabilitat del responsable.[37]

74. De la mateixa manera, quan un encarregat està subjecte a l'article 3.2 de l'RGPD, ha de complir les obligacions dels encarregats del tractament; especialment rellevant aquí, el deure de notificar una violació al responsable d'acord amb l'article 33.2 de l'RGPD.

D. Condicions en què no es requereix la notificació

75. L'article 33.1 deixa clar que les violacions que "no puguin causar un risc per als drets i llibertats de les persones físiques" no requereixen notificació a l'autoritat de control. Un exemple pot ser quan les dades personals ja estan disponibles públicament i el

[34] Vegeu també els considerants 23 i 24 RGPD.
[35] Vegeu també el considerant 25 RGPD.
[36] Vegeu les directrius del WP29 per identificar l'autoritat de control d'un responsable o un encarregat, disponible a http://ec.europa.eu/newsroom/document.cfm?doc_id=44102
[37] D'acord amb les Directrius 3/2018 sobre l'àmbit territorial de l'RGPD (art. 3), disponible a https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope%20-gdpr-article-3-version_en, l'EDPB considera que la funció de representant a la Unió no és compatible amb la funció d'un delegat extern de protecció de dades (DPD). Per tant, la responsabilitat de notificar a l'autoritat de control si es produeix una violació de dades personals continua essent del responsable del tractament, d'acord amb l'article 27.5 de l'RGPD. Tanmateix, un representant pot participar en el procés de notificació, si s'ha establert així explícitament per escrit.

fet de divulgar-les no constitueix un risc probable per als afectats. Això contrasta amb els requisits de notificació de violació per als proveïdors de serveis de comunicacions electròniques disponibles públicament establerts a la Directiva 2009/136/CE, que disposa que totes les violacions rellevants s'han de notificar a l'autoritat competent.

76. En la seva Opinió 03/2014 sobre la notificació de violacions,[38] el WP29 explicava que la violació de la confidencialitat de les dades personals encriptades amb un algorisme de tecnologia avançada continua essent una violació de dades personals, i s'ha de notificar. Tot i això, si la confidencialitat de la clau està intacta, és a dir, si la clau no s'ha vist compromesa en cap violació de la seguretat i s'ha generat de manera que cap persona que no estigui autoritzada a accedir-hi no la pot determinar per mitjans tècnics disponibles, en principi les dades són inintel·ligibles. Per tant, és poc probable que la violació afecti negativament les persones i, per tant, no requeriria comunicació a aquests afectats.[39] Això no obstant, fins i tot quan les dades estan xifrades, una pèrdua o alteració pot tenir conseqüències negatives per a les persones afectades, si el responsable no té les còpies de seguretat adequades. En aquest cas, es requeriria la comunicació als afectats, fins i tot si les dades estaven subjectes a mesures de xifratge adequades.

77. El WP29 també explicava que seria semblant al cas que les dades personals, com ara contrasenyes, estiguessin xifrades mitjançant una funció resum amb un *salt* (*hashed and salted*, en anglès) i el valor de la funció resum s'hagués calculat amb una funció resum encriptada amb una clau de tecnologia avançada, la clau utilitzada per a aquesta funció no hagués estat compromesa en cap violació i la clau utilitzada per encriptar les dades s'hagués generat de manera que una persona no autoritzada per accedir a les dades no la pogués esbrinar.

78. En conseqüència, si les dades personals han esdevingut essencialment inintel·ligibles per a parts no autoritzades i són una còpia o n'hi ha una còpia de seguretat, és possible que no calgui notificar a l'autoritat de control una violació de la confidencialitat que afecti dades personals correctament encriptades, ja que és poc probable que aquesta violació suposi un risc per als drets i les llibertats de les persones. Això significa que no caldria informar-ne els afectats, ja que probablement no hi ha cap risc alt. Tot i això, cal tenir en compte que, si bé és possible que inicialment la notificació no sigui exigible si no hi ha risc probable per als drets i les llibertats de les persones, això pot canviar amb el temps i llavors caldria reavaluar el risc. Per exemple, si posteriorment la clau es veu compromesa o si hi ha una vulnerabilitat en el programari de xifrat, pot ser que la notificació encara sigui necessària.

79. A més, cal assenyalar que si es produeix una violació i no hi ha cap còpia de seguretat de les dades personals encriptades es produirà una violació de disponibilitat, que podria suposar riscos per a les persones i, per tant, pot caldre notificar-la. De la mateixa manera, si es produeix una violació que implica la pèrdua de dades xifrades, encara que hi hagi una còpia de seguretat de les dades personals pot caldre informar-ne, depenent del temps que es trigui a restaurar les dades

[38] WP29, Opinió 03/2014, sobre notificació de violacions, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf.
[39] Vegeu també els articles 4.1 i 4.2 del Reglament 611/2013.

d'aquesta còpia de seguretat i l'efecte que la manca de la disponibilitat tingui per als afectats. Tal com estableix l'article 32.1.*c*, un factor important de seguretat és "la capacitat de restaurar la disponibilitat i l'accés a les dades personals amb promptitud, en cas d'incidència física o tècnica."

Exemple

Una violació que no requeriria la notificació a l'autoritat de control seria la pèrdua d'un dispositiu mòbil encriptat de manera segura, utilitzat pel responsable i el seu personal. Si la clau de xifrat es manté en possessió segura del responsable i no és l'única còpia de les dades personals, aquestes dades serien inaccessibles per a un atacant. Això significa que la violació no tindrà cap risc per als drets i llibertats dels titulars d'aquestes dades. Si més endavant es fa evident que la clau de xifrat s'ha vist compromesa o que el programari o l'algorisme de xifratge és vulnerable, el risc per als drets i les llibertats de les persones canviarà i, per tant, la notificació pot ser exigible.

80. Tanmateix, si el responsable no notifica a l'autoritat de control una situació en què les dades no s'han encriptat de manera segura, es produirà un incompliment de l'article 33 de l'RGPD. Per tant, quan els responsables seleccionin el programari de xifratge han d'avaluar amb cura la qualitat i la correcta implementació del xifrat que s'ofereix, entendre el nivell de protecció que realment proporciona i determinar si això és adequat als riscos presentats. Els responsables també han d'estar familiaritzats amb els detalls sobre com funciona el seu producte de xifrat. Per exemple, un dispositiu pot estar xifrat quan està apagat, però no mentre està en mode d'espera (*stand-by*). Alguns productes que utilitzen xifratge tenen "claus predeterminades" que cada client ha de canviar perquè siguin eficaces. Els experts en seguretat poden considerar que actualment el xifratge és adequat, però pot quedar obsolet en pocs anys, cosa que implica que és qüestionable que les dades estiguin prou xifrades per a aquest producte i proporcionin un nivell de protecció adequat.

III. Article 34 - Comunicació a les persones afectades

A. Informar els afectats

81. En alguns casos, a més de notificar una violació a l'autoritat de control, el responsable també l'ha de comunicar a les persones afectades.

    L'article 34.1 estableix:

> "Quan la violació de la seguretat de les dades personals pot comportar un alt risc per als drets i les llibertats de les persones físiques, el responsable del tractament l'ha de comunicar a l'afectat sense dilació indeguda."

82. Els responsables han de recordar que la notificació a l'autoritat de control és obligatòria, tret que com a conseqüència d'una violació no sigui probable que hi hagi risc per als drets i llibertats de les persones. A més, si hi ha un alt risc per als drets i

les llibertats de les persones com a conseqüència d'una violació, també cal informar-ne els afectats. Per tant, el llindar per comunicar una violació a les persones és més alt que per notificar-la a les autoritats de control; per això, no es requereix que totes les violacions es comuniquin a les persones, que d'aquesta manera estan protegides de la càrrega de notificacions innecessàries.

83. L'RGPD afirma que una violació s'ha de comunicar a les persones "sense dilació indeguda", cosa que significa al més aviat possible. L'objectiu principal de la notificació als afectats és proporcionar-los informació específica sobre les mesures que haurien de prendre per protegir-se.[40] Tal com s'ha assenyalat anteriorment, depenent de la naturalesa de la violació i el risc que es planteja, la comunicació en el temps oportú ajudarà les persones a prendre mesures per protegir-se de les conseqüències negatives de la violació.

84. L'annex B d'aquestes directrius proporciona una llista no exhaustiva d'exemples en què és probable que una violació produeixi un alt risc per a les persones i, en conseqüència, el responsable l'ha de notificar als afectats.

B. Informació que cal proporcionar

85. Quan cal fer la notificació a les persones afectades, l'article 34.2 especifica el següent:

> "La comunicació a l'afectat que preveu l'apartat 1 d'aquest article ha de descriure la naturalesa de la violació de la seguretat de les dades personals, en un llenguatge clar i senzill, i ha de contenir com a mínim la informació i les mesures a què es refereix l'article 33.3, lletres *b*, *c* i *d*."

86. D'acord amb aquesta disposició, el responsable ha de proporcionar almenys la informació següent:

- Una descripció de la naturalesa de la violació.
- El nom i les dades de contacte del delegat de protecció de dades o un altre punt de contacte.
- Una descripció de les possibles conseqüències de la violació.
- Una descripció de les mesures preses o proposades pel responsable per abordar la violació, incloses, si escau, mesures per mitigar-ne els possibles efectes adversos.

87. Com a exemple de les mesures adoptades per fer front a la violació i per mitigar-ne els possibles efectes adversos, el responsable podria afirmar que, després d'haver notificat la violació a l'autoritat de control competent, ha rebut recomanacions sobre com gestionar la violació i disminuir-ne l'impacte. El responsable també ha de proporcionar, si escau, una recomanació específica perquè les persones físiques es protegeixin de les possibles conseqüències adverses de la violació, com ara restablir les contrasenyes si les seves credencials d'accés s'han vist compromeses. De nou,

[40] Vegeu també el considerant 86 RGPD.

el responsable pot optar per proporcionar més informació de la que es requereix aquí.

C. Contactar amb els afectats

88. En principi, la violació rellevant s'ha de comunicar directament als afectats, tret que això impliqui un esforç desproporcionat. En aquest cas, hi ha d'haver una comunicació pública o una mesura similar mitjançant la qual s'informi els afectats de manera igualment efectiva (article 34.3.*c* RGPD).

89. Els missatges per comunicar la violació als titulars de les dades han d'anar adreçats als afectats i no han d'incloure altres informacions, com ara actualitzacions periòdiques, butlletins informatius o missatges estàndard. Això contribueix a fer que la comunicació de la violació sigui clara i transparent.

90. Alguns exemples de sistemes de comunicació transparents inclouen missatgeria directa (per exemple, correu electrònic, SMS, missatge directe), bàners o notificacions de llocs web destacats, comunicacions postals i anuncis destacats en mitjans impresos. Una notificació exclusivament limitada a un comunicat de premsa o a un bloc corporatiu no seria un mitjà eficaç de comunicar una violació a un afectat. El CEPD recomana que els responsables triïn un mitjà que maximitzi la possibilitat de comunicar correctament la informació a totes les persones afectades. Depenent de les circumstàncies, això pot significar que el responsable utilitzi diversos canals de comunicació, en lloc d'un de sol.

91. Els responsables també s'han d'assegurar que la comunicació és accessible en formats alternatius i en un llenguatge apropiat per garantir que els afectats entenguin la informació que se'ls proporciona. Per exemple, si es comunica una violació a un afectat, generalment el llenguatge que s'hagi utilitzat anteriorment per comunicar-s'hi serà adequat. Tanmateix, si la violació afecta persones amb les quals el responsable no ha interaccionat prèviament, o especialment els que resideixen en un altre estat membre o en un altre país que no pertany a la UE diferent d'on està establert el responsable, la comunicació en la llengua nacional local pot ser acceptable, tenint en compte els recursos requerits. La clau és ajudar els afectats a comprendre la naturalesa de la violació i les mesures que poden prendre per protegir-se.

92. Els responsables estan en millors condicions per determinar el canal de contacte més adequat per comunicar una violació a les persones afectades, especialment si interactuen freqüentment amb els seus clients. Això no obstant, és evident que el responsable ha d'anar en compte de no utilitzar un canal de contacte compromès per la violació, ja que els atacants que suplantin el responsable també podrien utilitzar aquest mateix canal.

93. Al mateix temps, el considerant 86 de l'RGPD explica que:

"Aquestes comunicacions als afectats s'han de fer tan aviat com sigui raonablement possible i en estreta col·laboració amb l'autoritat de control, respectant les orientacions proporcionades per aquesta o per altres autoritats pertinents, com ara les autoritats policials. Per exemple, la necessitat de mitigar un risc immediat de danys requereix una comunicació ràpida als afectats, mentre que la necessitat d'implementar mesures apropiades per evitar violacions de dades personals continuades o similars pot justificar que es trigui més temps a fer la comunicació."

94. És possible que els responsables vulguin contactar i consultar l'autoritat de control no únicament per demanar assessorament per informar els afectats sobre una violació, d'acord amb l'article 34. També poden consultar-la sobre els missatges que s'han d'enviar a les persones afectades i sobre la manera més adequada de contactar-hi.

95. En relació amb això, es recomana l'opinió que dona el considerant 88 de l'RGPD: "si una comunicació prematura pot obstaculitzar innecessàriament la recerca de les circumstàncies d'una violació de la seguretat de les dades personals, aquestes normes i procediments han de tenir en compte els interessos legítims de les autoritats policials." Això pot significar que en determinades circumstàncies, quan estigui justificat i d'acord amb l'assessorament de les autoritats policials, el responsable pot ajornar la comunicació de la violació als afectats fins al moment que no perjudiqui aquestes investigacions. Això no obstant, a partir d'aquest moment caldria informar ràpidament aquests afectats.

96. Si el responsable no pot comunicar una violació a un afectat perquè no disposa de dades suficients per contactar-hi, en aquesta circumstància particular el responsable ha d'informar la persona afectada tan aviat com sigui raonablement possible (per exemple, quan un afectat exerceix el dret d'accés a les dades personals de l'article 15 i proporciona al responsable informació addicional per contactar-hi).

D. Condicions en què no es requereix comunicació

97. L'article 34.3 estableix tres condicions en què no es requereix que una violació es notifiqui a les persones afectades:

- El responsable ha aplicat les mesures tècniques i organitzatives adequades per protegir les dades personals abans de la violació, en particular les mesures per fer ininteL·ligibles les dades personals a qualsevol persona que no estigui autoritzada per accedir-hi. Això podria, per exemple, incloure la protecció de dades personals amb xifratge de tecnologia avançada, o amb un testimoni d'autenticació (*tokenization*).

- Immediatament després d'una violació, el responsable ha pres mesures per assegurar que l'alt risc que suposa per als drets i llibertats de les persones ja no és probable que es materialitzi. Per exemple, depenent de les circumstàncies del cas, el responsable pot haver identificat immediatament l'individu que ha accedit a les dades personals i haver pres mesures per fer-hi front, abans que pogués fer res amb les dades. A més, cal tenir en compte les possibles conseqüències de

qualsevol violació de la confidencialitat, de nou depenent de la naturalesa de les dades afectades.

- Contactar amb les persones físiques exigeix esforços desproporcionats,[41] potser perquè les seves dades de contacte s'han perdut com a conseqüència de la violació o perquè des del principi no es coneixien. Per exemple, el magatzem d'una oficina d'estadística s'ha inundat i els documents que contenen dades personals només estaven emmagatzemats en paper. Com a alternativa, el responsable ha de fer una comunicació pública o adoptar una mesura similar, per la qual cosa se n'informa els afectats d'una manera igualment eficaç. En el cas d'un esforç desproporcionat, també es poden preveure mesures tècniques perquè la informació sobre la violació estigui disponible si es demana, cosa que pot ser útil per a les persones afectades per una violació, però amb les quals el responsable no té manera de contactar.

98. D'acord amb el principi de responsabilitat proactiva (*accountability*), els responsables han de poder demostrar a l'autoritat de control que compleixen una o més d'aquestes condicions.[42] Cal tenir en compte que, tot i que inicialment la notificació pot no ser necessària, perquè no hi ha risc per als drets i les llibertats de persones físiques, aquesta situació pot canviar amb el temps i el risc s'haurà de reavaluar.

99. Si un responsable decideix no comunicar una violació als afectats, l'article 34.4 de l'RGPD indica que l'autoritat de control li pot exigir que ho faci, si considera que la violació probablement generarà un alt risc per a les persones. Per altra banda, es pot considerar que es compleixen les condicions de l'article 34.3 i, en aquest cas, no es requereix la notificació als afectats. Si l'autoritat de control determina que la decisió de no notificar a les persones afectades no està ben fonamentada, pot considerar fer ús de les seves competències i de les sancions disponibles.

IV. Avaluació de riscos i alt risc

A. El risc com a desencadenant de la notificació

100. Tot i que l'RGPD introdueix l'obligació de notificar una violació, no en tots els casos cal fer-ho:

- Cal fer una notificació a l'autoritat de control competent, tret que no sigui probable que la violació comporti un risc per als drets i les llibertats de les persones.

- La comunicació d'una violació als afectats únicament es duu a terme quan és probable que generi un risc alt per als seus drets i llibertats.

101. Això significa que, immediatament després d'haver pres consciència d'una violació, és de vital importància que el responsable no només procuri contenir la violació,

[41] Vegeu les directrius WP29 sobre transparència, que consideren la qüestió d'un esforç desproporcionat, disponible a http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850.
[42] Vegeu l'article 5.2 RGPD.

sinó també que avaluï el risc que se'n pot derivar. Hi ha dos motius importants: en primer lloc, el fet de conèixer la probabilitat i la gravetat potencial de l'impacte en l'afectat ajudarà el responsable a prendre mesures efectives per contenir la violació i fer-hi front; en segon lloc, l'ajudarà a determinar si cal notificar la violació a l'autoritat de control i, si escau, a les persones afectades.

102. Tal com s'ha explicat anteriorment, la violació s'ha de notificar tret que no sigui probable que comporti un risc per als drets i llibertats de les persones; així mateix, el desencadenant clau perquè calgui comunicar-la als afectats és la probabilitat que generi un risc alt per als drets i llibertats de les persones. Aquest risc existeix quan la violació pot comportar un dany físic, material o no material, per a les persones titulars de les dades afectades per la violació. Alguns exemples d'aquests danys són la discriminació, el robatori d'identitat o el frau, la pèrdua financera i el dany a la reputació. Si la violació implica dades personals que revelen origen racial o ètnic, opinió política, religió o creences filosòfiques o afiliació sindical, o inclou dades genètiques, dades relatives a la salut o dades relatives a la vida sexual o condemnes i delictes penals o mesures de seguretat relacionades, s'ha de considerar probable que es produeixi aquest dany.[43]

B. Factors a tenir en compte a l'hora d'avaluar el risc

103. Els considerants 75 i 76 de l'RGPD suggereixen que, en general, quan s'avalua el risc s'ha de tenir en compte la probabilitat i la gravetat del risc per als drets i llibertats de les persones. A més, afirma que ha de ser una avaluació objectiva.

104. 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.[44] 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.

[43] Vegeu els considerants 75 i 85 RGPD.
[44] Vegeu les directrius del WP sobre AIPD: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137.

Exemple

Una AIPD suggereix que la proposta d'ús d'un determinat producte de programari de seguretat per protegir dades personals és una mesura adequada per garantir un nivell de seguretat adequat al risc que el tractament pot presentar per a les persones. Tot i això, si posteriorment se'n coneix una vulnerabilitat, la idoneïtat del programari per evitar el risc de les dades personals protegides canviarà i, per tant, caldrà reavaluar-lo com a part d'una AIPD en curs.

Més endavant, s'aprofita una vulnerabilitat en el producte i es produeix una violació. El responsable hauria d'avaluar les circumstàncies específiques de la violació, les dades afectades i el possible nivell d'impacte sobre les persones, així com la probabilitat que aquest risc es materialitzi.

105. En conseqüència, en avaluar el risc per a les persones com a conseqüència d'una violació, el responsable n'ha de considerar les circumstàncies específiques, inclosa la gravetat de l'impacte potencial i la probabilitat que això succeeixi. Per tant, el CEPD recomana que l'avaluació tingui en compte els criteris següents:[45]

- El tipus de violació

106. El tipus de violació que s'ha produït pot afectar el nivell de risc presentat als afectats. Per exemple, una violació de la confidencialitat mitjançant la qual s'ha revelat informació mèdica a usuaris no autoritzats pot tenir un conjunt de conseqüències per a una persona, diferent de les d'una violació en què s'han perdut les dades mèdiques d'un individu i ja no estan disponibles.

- La naturalesa, el grau de sensibilitat i el volum de dades personals

107. Quan s'avalua el risc, un factor clau és el tipus i la sensibilitat de les dades personals que han quedat compromeses per la violació. Generalment, com més sensibles són les dades, més alt és el risc de dany per a les persones afectades; també cal tenir en compte, però, altres dades personals sobre l'afectat que ja poden estar disponibles. Per exemple, en circumstàncies ordinàries és poc probable que la divulgació del nom i l'adreça d'un afectat causi danys substancials. Això no obstant, si el nom i l'adreça d'uns pares adoptius es divulga a uns pares biològics, les conseqüències poden ser molt greus tant per als pares adoptius com per al menor.

108. Les violacions que afecten dades de salut, documents d'identitat o dades financeres, com ara detalls de la targeta de crèdit, poden causar un dany per si soles, però si s'utilitzen conjuntament es podrien utilitzar per suplantar la identitat. Una combinació de dades personals acostuma ser més sensible que una sola informació personal.

[45] L'article 3.2 del Reglament 611/2013 proporciona orientació sobre els factors que s'han de tenir en compte en relació amb la notificació de violacions en el sector dels serveis de comunicacions electròniques, que poden ser útils en el context de la notificació segons l'RGPD. Vegeu http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF.

109. Alguns tipus de dades personals inicialment poden semblar relativament innòcues, però el que aquestes dades poden revelar sobre l'afectat s'ha de considerar acuradament. Una llista de clients que accepten enviaments regulars pot no ser especialment sensible, però les mateixes dades sobre els clients que han demanat que es deixin de fer les entregues durant les seves vacances pot ser informació útil per als delinqüents.

110. De la mateixa manera, una petita quantitat de dades personals altament sensibles pot tenir un gran impacte en una persona, i un ampli rang de detalls pot revelar molta més informació sobre aquesta persona. A més, una violació que afecta un gran volum de dades personals sobre moltes persones pot produir efectes sobre un gran nombre de persones.

- Facilitat per identificar les persones

111. Un factor important a tenir en compte és com de fàcil resulta que un tercer que tingui accés a dades personals compromeses pugui identificar persones concretes, o les faci coincidir amb altres dades per tal d'identificar persones. Depenent de les circumstàncies, la identificació pot ser possible directament a partir de les dades personals violades, sense que calgui una investigació especial per descobrir la identitat de l'afectat; o pot ser extremadament difícil relacionar dades personals amb un afectat determinat, però fins i tot així seria possible en certes condicions. La identificació pot ser possible directament o indirectament a partir de les dades violades, però això també depèn del context específic de la violació i de la disponibilitat pública de dades personals relacionades. Això pot ser més rellevant en el cas de les violacions de confidencialitat i disponibilitat.

112. Com s'ha dit anteriorment, les dades personals protegides per un nivell de xifratge adequat són inintel·ligibles per a persones no autoritzades, sense la clau de desxifratge. Addicionalment, la pseudonimització implementada adequadament (definida a l'article 4.5 de l'RGPD com "el tractament de les dades personals de manera que les dades personals ja no es puguin atribuir a un titular de dades específic sense utilitzar informació addicional, sempre que aquesta informació addicional es mantingui per separat i estigui sotmesa a mesures tècniques i organitzatives per garantir que les dades personals no s'atribueixen a una persona física identificable o identificable") també pot reduir la probabilitat que, en cas de violació, les persones puguin ser identificades. Això no obstant, no es pot considerar que les tècniques de pseudonimització aconsegueixen, per si soles, que les dades siguin inintel·ligibles.

- Gravetat de les conseqüències per als afectats

113. Segons quina sigui la naturalesa de les dades personals implicades en una violació, per exemple categories especials de dades, en pot resultar un dany potencial especialment greu per a les persones, en particular quan la violació pot provocar suplantacions d'identitat o frau, dany físic, angoixa psicològica, humiliació o dany a la reputació. Si la violació es refereix a dades personals sobre persones vulnerables, el risc de dany pot ser superior.

114. Si el responsable és conscient que les dades personals estan en mans de persones de les quals no se'n coneixen les intencions o que poden ser malicioses, això pot afectar el nivell de risc potencial. Pot haver-hi una violació de la confidencialitat a causa de la qual les dades personals, per error, es divulguin a un tercer tal com es defineix a l'article 4.10, o un altre destinatari. Això pot passar, per exemple, quan les dades personals s'envien accidentalment a un departament erroni dins d'una organització, o a una organització proveïdora comuna. El responsable pot sol·licitar al destinatari que retorni o destrueixi de forma segura les dades que ha rebut. En ambdós casos, atès que el responsable hi té una relació permanent i pot conèixer els seus procediments, història i altres detalls rellevants, el destinatari es pot considerar "de confiança". Dit d'una altra manera, el responsable pot tenir un nivell de seguretat amb motiu del qual pugui esperar que el destinatari no llegirà o accedirà a les dades enviades per error, i que complirà les instruccions per retornar-les. Fins i tot si s'ha accedit a les dades, el responsable encara pot confiar que el destinatari no hi faci cap acció addicional, les retorni al responsable amb promptitud i cooperi per recuperar-les. En aquests casos, a l'hora de fer l'avaluació de riscos després de la violació, el responsable pot tenir en compte que el fet que el destinatari sigui de confiança pot erradicar la gravetat de les conseqüències de la violació, cosa que no implica que la violació no s'hagi produït. Això també pot eliminar la probabilitat de risc per a les persones afectades i, per tant, ja no requereix que la violació es notifiqui a l'autoritat de control o als afectats. Una vegada més, això dependrà de cada cas. Tot i això, el responsable ha de conservar la informació relativa a la violació, com a part del deure general de mantenir registres de violacions (vegeu la secció V, a continuació).

115. També cal tenir en compte la durada de les conseqüències per a les persones afectades, ja que l'impacte es pot considerar més gran si els efectes són a llarg termini.

- Característiques especials de la persona afectada

116. Una violació pot afectar les dades personals sobre infants o altres individus vulnerables que, com a resultat, poden estar en un risc superior. Hi pot haver altres factors sobre l'afectat que poden afectar el nivell d'impacte que la violació tingui sobre ell.

- Característiques especials del responsable de dades

117. La naturalesa i les funcions del responsable i les seves activitats poden afectar el nivell de risc per a les persones, com a conseqüència d'una violació. Per exemple, una organització mèdica tracta categories especials de dades de caràcter personal, cosa que implica una amenaça més gran per a les persones, si les seves dades personals són violades, si ho comparem amb una llista de correu d'un diari.

- El nombre de persones afectades

118. Una violació pot afectar una o poques persones, o bé milers o més. En general, com més gran és el nombre d'afectats, més gran pot ser l'impacte d'una violació. Això 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. De nou, la clau és considerar la probabilitat i la gravetat de l'impacte en els afectats.

- Punts generals

119. Per tant, en avaluar el risc probable que es produeixi a causa d'una violació, el responsable ha d'avaluar la combinació de la gravetat de l'impacte potencial sobre els drets i llibertats de les persones i la probabilitat que es produeixi l'incident. És evident que, quan les conseqüències d'una violació són més greus, el risc és més elevat i, de la mateixa manera, quan la probabilitat que es produeixi una violació és més gran, el risc també augmenta. En cas de dubte, el responsable ha d'optar per la precaució i notificar-ho. L'annex B ofereix alguns exemples útils de diferents tipus de violacions que impliquen risc o alt risc per a les persones.

120. L'Agència de Seguretat de la Informació i de la Xarxa de la Unió Europea (ENISA) ha elaborat recomanacions per a una metodologia d'avaluació de la gravetat d'una violació, que poden ser útils per als responsables i els encarregats del tractament a l'hora de dissenyar el seu pla de resposta a una violació.[46]

V. Responsabilitat proactiva i manteniment de registres de violacions

A. Documentar les violacions

121. Independentment de si una violació s'ha de notificar o no a l'autoritat de control, el responsable ha de mantenir la documentació de totes les violacions, tal com explica l'article 33.5 de l'RGPD:

> "El responsable ha de documentar qualsevol violació de la seguretat de les dades personals, cosa que inclou els fets que hi estan relacionats, els seus efectes i les mesures correctores que s'han adoptat. Aquesta documentació permetrà a l'autoritat de control verificar que es compleix el que disposa aquest article."

122. Això està relacionat amb el principi de responsabilitat proactiva (*accountability*) de l'RGPD, establert a l'article 5.2. L'objectiu de registrar tant les violacions no notificables com les notificables també remet a les obligacions del responsable d'acord amb l'article 24 de l'RGPD, i l'autoritat de control pot requerir veure aquests registres. Per tant, es recomana als responsables que estableixin un registre intern de violacions, independentment de si cal notificar-les o no.[47]

123. Tot i que depèn del responsable decidir el mètode i l'estructura que utilitzarà per documentar una violació, en termes d'informació registrable hi ha elements clau que

[46] ENISA, Recomanacions per a una metodologia d'avaluació de la gravetat de les violacions de dades personals, https://www.enisa.europa.eu/publications/dbn-severity.
[47] El responsable pot optar per documentar les violacions com a part del registre d'activitats de tractament que es manté d'acord amb l'article 30. No es requereix un registre diferent, sempre que la informació rellevant de la infracció sigui clarament identificable com a tal i es pugui extreure, si és requerida.

cal incloure en qualsevol cas. Tal com exigeix l'article 33.5 de l'RGPD, el responsable ha de registrar els detalls sobre la violació, que ha d'incloure les causes, què ha succeït i les dades personals afectades. També ha d'incloure els efectes i les conseqüències de la violació, juntament amb les mesures correctores que ha adoptat.

124. L'RGPD no especifica un període de conservació per a aquesta documentació. Quan aquests registres contenen dades personals, correspon al responsable determinar-ne el període de conservació adequat, d'acord amb els principis relatius al tractament de dades de caràcter personal,[48] i tractar-les d'acord amb una base legal.[49] Cal conservar la documentació de conformitat amb l'article 33.5 de l'RGPD, ja que l'autoritat de control pot demanar al responsable proves que compleix aquest article o, de manera general, que compleix amb el principi de responsabilitat proactiva. Clarament, si els registres no contenen dades personals, el principi de limitació del termini de conservació[50] de l'RGPD no s'aplica.

125. A més d'aquests detalls, el CEPD recomana que el responsable també documenti el seu raonament respecte de les decisions preses per respondre a una violació. En particular, si no es notifica la violació, cal documentar la justificació d'aquesta decisió. Això hauria d'incloure els motius pels quals el responsable considera que no és probable que la violació comporti un risc per als drets i les llibertats de les persones.[51] Alternativament, si el responsable considera que es compleix alguna de les condicions de l'article 34.3 de l'RGPD, ha de poder proporcionar proves adequades que és així.

126. Quan el responsable notifica una violació a l'autoritat de control, però la notificació es demora, el responsable ha de poder motivar aquest retard; la documentació que hi està relacionada pot ajudar a demostrar que està justificada i no és excessiva.

127. Quan el responsable comunica una violació a les persones afectades, ha de ser transparent sobre la violació i comunicar-la de manera efectiva i oportuna. En conseqüència, conservar les proves d'aquesta comunicació el pot ajudar a demostrar tant la responsabilitat proactiva com el compliment.

128. Per ajudar en el compliment dels articles 33 i 34 de l'RGPD, pot ser avantatjós que tant el responsable com l'encarregat disposin d'un procediment de notificació documentat, que estableixi el procés que cal seguir un cop s'ha detectat una violació. Això inclou la manera de contenir, gestionar i recuperar-se de l'incident, així com avaluar el risc i notificar la violació. En aquest sentit, per mostrar el compliment de l'RGPD, també pot ser útil demostrar que els empleats han estat informats sobre l'existència d'aquests procediments i mecanismes i que saben com reaccionar davant les violacions.

129. Cal assenyalar que el fet de no documentar adequadament una violació pot comportar que l'autoritat de control exerceixi les seves competències en virtut de

[48] Vegeu l'article 5 RGPD.
[49] Vegeu l'article 6 i també l'article 9 RGPD.
[50] Vegeu l'article 5.1.*e* RGPD.
[51] Vegeu el considerant 85 RGPD.

l'article 58 de l'RGPD i/o imposar una sanció administrativa, de conformitat amb l'article 83.

B. Funcions del delegat de protecció de dades

130. Un responsable o un encarregat pot tenir un delegat de protecció de dades (DPD),[52] ja sigui com a requeriment de l'article 37 de l'RGPD o voluntàriament, com a bona pràctica. L'article 39 estableix diverses tasques obligatòries per al DPD però no impedeix que, si escau, el responsable n'hi assigni de noves.

131. Com a aspecte rellevant per a la notificació de violacions, les tasques obligatòries del DPD inclouen, entre d'altres funcions, proporcionar assessorament i informació sobre la protecció de dades al responsable o l'encarregat, fer el seguiment del compliment de l'RGPD i assessorar sobre les AIPD. Així mateix, el DPD ha de cooperar amb l'autoritat de control i actuar com a punt de contacte d'aquesta autoritat i dels titulars de les dades. També cal assenyalar que, a l'hora de notificar una violació a l'autoritat de control, l'article 33.3.*b* de l'RGPD requereix que el responsable proporcioni el nom i les dades de contacte del seu DPD, o un altre punt de contacte.

132. Pel que fa a la documentació de violacions, al responsable o l'encarregat els pot interessar conèixer l'opinió del seu DPD respecte de l'estructura, la configuració i l'administració d'aquesta documentació. Al DPD també pot se li pot assignar la tasca de mantenir aquests registres.

133. Tot això significa que el DPD ha de ser una figura clau a l'hora d'ajudar a prevenir o a preparar-se per a una violació, proporcionant assessorament i fent el seguiment del compliment. També durant una violació (és a dir, a l'hora de notificar-la a l'autoritat de control) i durant qualsevol investigació posterior que faci l'autoritat de control. En aquest sentit, el CEPD recomana que, si es produeix una violació, se n'informi el DPD ràpidament i que intervingui en tot el procés de gestió i notificació de la violació.

VI. Obligacions de notificació en virtut d'altres instruments jurídics

134. A més de la notificació i la comunicació de violacions en virtut de l'RGPD, els responsables també han de conèixer qualsevol altre requeriment de notificació d'incidents de seguretat establert en altres legislacions que els puguin ser d'aplicació, i si aquesta legislació també els exigeix que notifiquin la violació de les dades personals a l'autoritat de control. Aquests requeriments poden variar entre els estats membres, però alguns exemples de requeriments de notificació en altres instruments jurídics, i com estan vinculats a l'RGPD, són els següents:

- Reglament (UE) 910/2014 sobre identificació electrònica i serveis de confiança per a transaccions electròniques en el mercat interior (Reglament eIDAS).[53]

[52] Vegeu les directrius del WP sobre els DPD aquí: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.
[53] Vegeu http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG.

135. L'article 19.2 del Reglament eIDAS exigeix que els proveïdors de serveis de confiança notifiquin al seu òrgan de supervisió una violació de seguretat o una pèrdua d'integritat que tingui un impacte significatiu en el servei de confiança que presten, o en les dades personals que conserva. En els casos en què sigui d'aplicació, és a dir quan aquesta violació o pèrdua constitueixi una violació de les dades personals en virtut de l'RGPD, el proveïdor de serveis de confiança també l'ha de notificar a l'autoritat de control.

- Directiva (UE) 2016/1148 relativa a mesures per a un alt nivell comú de seguretat dels sistemes de xarxa i d'informació a la Unió (Directiva NIS).[54]

136. Els articles 14 i 16 de la Directiva NIS exigeixen als operadors de serveis essencials i proveïdors de serveis digitals que notifiquin les violacions de seguretat a la seva autoritat competent. Tal com reconeix el considerant 63 del NIS,[55] els incidents de seguretat sovint impliquen que les dades personals quedin compromeses. Tot i que el NIS requereix que, en aquest context, les autoritats competents i les autoritats de supervisió cooperin i intercanviin informació, continua sent el cas que, quan aquesta mena d'incidents es produeixen o es converteixen en violacions de les dades personals en virtut de l'RGPD, aquests operadors i/o proveïdors ho han de notificar a l'autoritat de control, de manera separada del requeriment de notificació del NIS.

> **Exemple**
>
> Un proveïdor de serveis al núvol que notifica una violació en virtut de la Directiva NIS també pot haver-la de notificar a un responsable, si inclou una violació de les dades personals. De la mateixa manera, un proveïdor de serveis de confiança que notifica d'acord amb l'eIDAS, en cas de violació pot haver-la de notificar també a l'autoritat de protecció de dades corresponent.

- Directiva 2009/136/CE (Directiva sobre drets dels ciutadans) i Reglament 611/2013 (Reglament de notificació de violacions).

137. Els proveïdors de serveis de comunicació electrònica disponibles públicament en el context de la Directiva 2002/58/EC52[56] han de notificar les violacions a les autoritats nacionals competents.

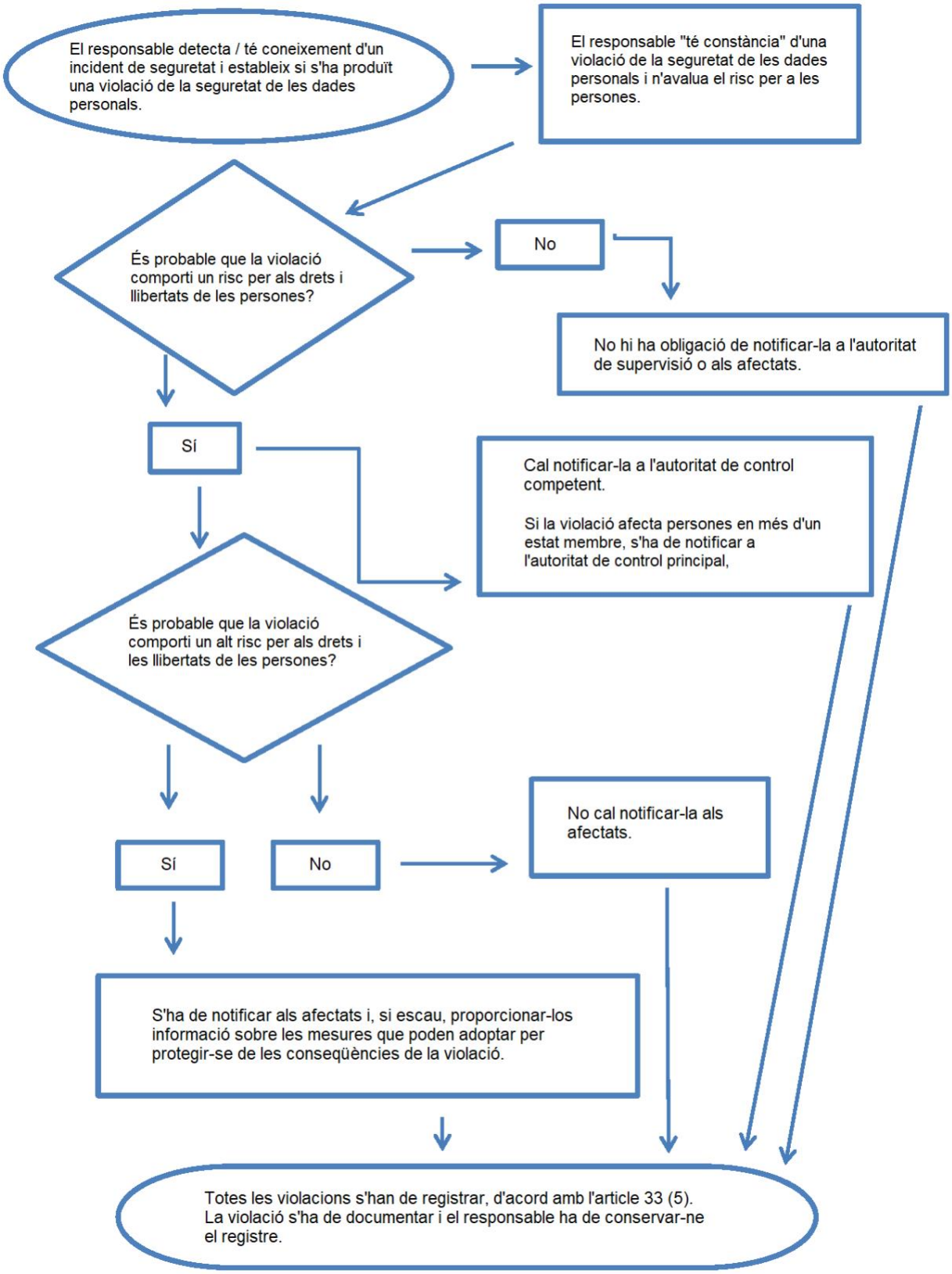
138. Els responsables també han de ser conscients de les obligacions addicionals de notificació legal, mèdica o professional, en virtut d'altres règims aplicables.

---

[54] Vegeu http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG.
[55] Considerant 63: "En molts casos, les dades personals es troben compromeses com a conseqüència d'incidents. En aquest context, les autoritats competents i les autoritats de protecció de dades han de cooperar i intercanviar informació sobre totes les qüestions pertinents per fer front a les violacions de dades personals derivades d'incidències."
[56] El 10 de gener de 2017, la Comissió Europea va proposar un Reglament sobre privadesa i comunicacions electròniques que substituirà la Directiva 2009/136/CE i eliminarà els requisits de notificació. No obstant això, fins que el Parlament Europeu aprovi aquesta proposta, el requisit de notificació existent continua vigent. Vegeu https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.

VII. Annex

A. Diagrama de flux dels requeriments de notificació



B. Exemples de violacions de dades personals i a qui s'han de notificar

Els exemples següents no exhaustius poden ajudar els responsables a determinar si cal fer la notificació, en diferents escenaris de violació de les dades personals. Aquests exemples també poden ajudar a distingir entre el risc i l'alt risc per als drets i llibertats de les persones.

Exemple	Cal notificar-ho a l'autoritat de control?	Cal notificar-ho als afectats?	Notes / recomanacions
i. Un responsable emmagatzema una còpia de seguretat d'un arxiu de dades personals xifrat en una memòria USB. La clau és robada durant una violació.	No	No	Mentre les dades estiguin encriptades amb un algorisme de tecnologia avançada, hi hagi còpies de seguretat de les dades, la clau única no es comprometi i les dades es puguin restaurar en un termini de temps breu, pot no ser necessari notificar la violació. Això no obstant, si més tard la clau es veu compromesa, cal notificar-ho.
ii. Un responsable manté un servei en línia. Com a resultat d'un ciberatac a aquest servei, les dades personals s'han filtrat a l'exterior. El responsable té clients en un sol estat membre.	Sí, cal informar-ne l'autoritat de control, si és probable que hi hagi conseqüències per a les persones.	Sí, cal informar-ne les persones afectades, segons la naturalesa de les dades personals afectades i si la gravetat de les conseqüències probables per a les persones és alta.	
iii. Un breu tall d'energia d'uns minuts de durada al centre d'atenció telefònica del responsable, que significa que els clients no poden trucar al responsable ni accedir als seus registres.	No.	No.	Això no és una violació de declaració obligatòria, però continua sent un incident que cal registrar en virtut de l'article 33.5. El responsable ha de mantenir els registres adequats.
iv. Un responsable pateix un atac amb un programari de segrest (*ransomware*) que xifra totes les	Sí, cal informar-ne l'autoritat de control si hi ha conseqüències probables per a les persones, ja que es	Sí, cal informar-ne les persones, segons la naturalesa de les dades personals afectades i el possible efecte de la manca de	Si hi havia una còpia de seguretat i les dades es poden restaurar ràpidament, no cal notificar-ho a l'autoritat de control ni

dades. No hi ha còpies de seguretat i les dades no es poden restaurar. En la investigació, queda clar que l'única funció del segrestador era xifrar les dades i que no hi ha cap altre programari maliciós (*malware*) al sistema.	tracta d'una pèrdua de disponibilitat.	disponibilitat, així com altres conseqüències probables.	als afectats, ja que no hi hauria hagut cap pèrdua permanent de disponibilitat ni confidencialitat. Això no obstant, si l'autoritat de control ha tingut coneixement de l'incident per altres mitjans, pot considerar fer una investigació per avaluar el compliment dels requisits de seguretat establerts a l'article 32.
v. Un telèfon personal truca a la central telefònica d'un banc per denunciar una violació de dades. El denunciant ha rebut l'extracte mensual del compte d'una altra persona. El responsable fa una breu investigació (és a dir, finalitzada en un termini de 24 hores) i estableix amb una confiança raonable que s'ha produït una violació de dades personals i si hi ha un defecte sistèmic que pot significar que altres persones s'hi vegin o s'hi puguin veure afectades.	Sí.	Només es notifica a les persones afectades si hi ha un alt risc i està clar que altres persones no estan afectades.	Si, després d'una investigació addicional, s'identifica que hi ha més persones afectades, cal actualitzar la informació a l'autoritat de control i el responsable ha de fer l'acció addicional de notificar-ho a altres persones, si hi ha un alt risc.
vi. Un responsable opera en un mercat en línia i té clients en diversos estats membres. El mercat pateix un ciberatac i l'atacant publica els noms d'usuari, contrasenyes i historial de compra dels clients.	Sí, cal notificar-ho a l'autoritat de control, si es tracta d'un tractament transfronterer.	Sí, ja que pot comportar un alt risc.	El responsable ha d'actuar, per exemple obligant a restablir la contrasenya dels comptes afectats, així com altres accions per mitigar el risc. El responsable també ha de tenir en compte qualsevol altra obligació de notificació, per exemple d'acord amb la directiva NIS com a proveïdor de serveis digitals.

vii. Una empresa d'allotjament web que actua com a encarregada del tractament identifica un error en el codi que controla l'autorització de l'usuari. L'efecte de l'error implica que qualsevol usuari pot accedir als detalls del compte de qualsevol altre usuari.	Com a encarregat del tractament, l'empresa d'allotjament web ho ha de notificar als seus clients afectats (els responsables) sense dilació indeguda. Si l'empresa d'allotjament web ha fet la seva pròpia investigació, els responsables afectats poden estar raonablement segurs sobre si cadascú ha patit una violació i, per tant, és probable que es consideri que se n'ha "adonat" una vegada que l'empresa d'allotjament els ho ha notificat (l'encarregat). Llavors el responsable ho ha de notificar a l'autoritat de control.	Si no és probable que hi hagi un alt risc per a les persones, no cal que se'ls notifiqui.	L'empresa d'allotjament web (encarregat) ha de tenir en compte qualsevol altra obligació de notificació (per exemple, d'acord amb la Directiva NIS, com a proveïdor de serveis digitals). Si no hi ha cap evidència que aquesta vulnerabilitat s'estigui aprofitant amb cap dels seus responsables, pot ser que no s'hagi produït una violació notificable. Però probablement s'ha de registrar o es tracta d'un incompliment de l'article 32.
viii. Les bases de dades mèdiques d'un hospital no estan disponibles per un període de 30 hores, a causa d'un ciberatac.	Sí, l'hospital està obligat notificar-ho com a risc alt per al benestar i la privacitat del pacient.	Sí, cal informar-ne les persones afectades.	
ix. Les dades personals d'un gran nombre d'estudiants s'envien per error a una llista de correu equivocada amb més de 1.000 destinataris.	Sí, cal notificar-ho a l'autoritat de control.	Sí, cal informar-ne les persones, segons l'abast i el tipus de dades personals implicades i la gravetat de possibles conseqüències.	

x. S'envia un correu electrònic de màrqueting directe als destinataris en els camps "A:" o "CC:". Això permet a cada destinatari veure l'adreça electrònica d'altres destinataris.	Sí, la notificació de l'autoritat de control pot ser obligatòria, si hi ha una gran quantitat d'individus afectats, si es revelen dades confidencials (per exemple, una llista de correu d'un psicoterapeuta) o si hi ha altres factors que presenten riscos elevats (per exemple, si el correu conté les contrasenyes inicials).	Sí, cal informar-ne les persones afectades, segons l'abast i el tipus de dades personals implicades i la gravetat de les possibles conseqüències.	Pot ser que no calgui notificar-la, si no es revelen dades confidencials i si només es revela un nombre reduït d'adreces electròniques.