CEPD
Comitetul european pentru protecția datelor

Orientări

Orientările 9/2022 privind notificarea încălcării securității datelor cu caracter personal în temeiul RGPD

Versiunea 2.0

adoptată la 28 martie 2023

Istoricul versiunii

Versiunea 1.0	10 octombrie 2022	Adoptarea Orientărilor (în versiunea actualizată a orientărilor anterioare WP250 (ed.01) adoptată de Grupul de lucru 29 și ulterior de CEPD la 25 mai 2018) pentru o consultare publică specifică.
Versiunea 2.0	28 martie 2023	Adoptarea Orientărilor în urma consultării publice specifice cu privire la subiectul notificării încălcării securității datelor cu caracter personal pentru operatorii din afara SEE.

Traducerea dată nu este o traducere oficială a Comitetului European pentru Protecția Datelor (EDPB) și a fost asigurată, în cadrul unui schimb între GIZ și EDPB, ca rezultat al unui acord reciproc între GIZ și CNPDCP, cu sprijinul financiar al GIZ în cadrul proiectului "Re-ingineria serviciilor publice în cadrul Parteneriatului Estic" din cadrul Fondului Regional pentru Reformele Administrației Publice al Parteneriatului Estic, comandat și finanțat de BMZ.

Cuprins

Comitetul European pentru Protecția Datelor

Luând în considerare prevederile de la articolul 70 alineatul (1) litera (e) și (l) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (denumit în continuare „RGPD”),

Având în vedere Acordul privind SEE, în special Anexa XI și Protocolul 37 la acesta, astfel cum a fost modificat prin Decizia nr. 154/2018 a Comitetului mixt al SEE din 6 iulie 2018[1],

Luând în considerare prevederile articolului 12 și articolului 22 din Regulamentul său de procedură,

A ADOPTAT URMĂTOARELE ORIENTĂRI

0. PREFAȚĂ

1. La 3 octombrie 2017 Grupul de lucru 29 (denumit în continuare „WP29”) a adoptat Orientările sale privind notificarea încălcării securității datelor cu caracter personal în temeiul Regulamentului 2016/679 (WP250 ed.01)[2], care au fost aprobate de Comitetul European pentru Protecția Datelor (denumit în continuare „CEPD”) la prima sa Ședință plenară[3]. Documentul de față este o versiune puțin actualizată a acestor orientări. Orice referire la Orientările WP29 privind notificarea încălcării securității datelor cu caracter personal în temeiul Regulamentului 2016/679 (WP250 ed.01) ar trebui, de acum înainte, să fie interpretată ca o referire la aceste Orientări 9/2022 ale CEPD.

2. CEPD a observat necesitatea de a clarifica cerințele de notificare a încălcării securității datelor cu caracter personal la entitățile din afara UE. Punctul, în care era abordat acest subiect, a fost revizuit și actualizat, iar restul documentului a fost lăsat fără modificări, cu excepția modificărilor editoriale. Revizuirea se referă, mai exact, la punctul 73 din secțiunea II.C.2 din prezentul document.

INTRODUCERE

3. RGPD a introdus cerința ca o încălcare a securității datelor cu caracter personal (denumită în continuare „încălcare”) să fie notificată autorității naționale de supraveghere competente[4] (sau, în cazul unei încălcări

[1] Referințele la „state membre” din acest document ar trebui înțelese ca referințe la „statele membre ale SEE”.
[2] Orientările WP29 privind notificarea încălcării securității datelor cu caracter personal în temeiul Regulamentului 2016/679 (WP250 ed.01) (ultima revizuire și actualizare la 6 februarie 2018), disponibile la https://ec.europa.eu/newsroom/article29/items/612052.
[3] A se vedea https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en.
[4] A se vedea articolul 4 alienatul (21) din RGPD.

transfrontaliere, autorității principale) și, în anumite cazuri, să fie comunicată persoanelor, ale căror date cu caracter personal au fost afectate de încălcare.

4. Au existat obligații de notificare a încălcărilor pentru anumite organizații, cum ar fi prestatorii de servicii de comunicații electronice accesibile publicului (după cum este specificat în Directiva 2009/136/CE și Regulamentul (UE) nr. 611/2013)[5]. Au fost, de asemenea, unele State membre care aveau propria obligație de notificare a încălcării prevăzută în cadrul legal național. Aceasta putea include obligația de a notifica încălcările, care implicau categorii de operatori în afară de prestatorii serviciilor de comunicații electronice accesibile publicului (de exemplu, în Germania și Italia) sau obligația de a raporta toate încălcările, care implică date cu caracter personal (cum ar fi Țările de Jos). Alte State membre puteau avea Coduri de practică relevante (de exemplu, Irlanda[6]). Dacă unele autorități de protecție a datelor din UE încurajau operatorii să raporteze încălcările, Directiva privind protecția datelor cu caracter personal 95/46/CE[7], care a fost înlocuită de RGPD, nu prevedea o obligație specifică de notificare a încălcării și, prin urmare, o astfel de cerință era nouă pentru multe organizații. Conform RGPD, notificarea este obligatorie pentru toți operatorii, cu excepția cazului în care este puțin probabil ca o încălcare să genereze un risc pentru drepturile și libertățile persoanelor fizice[8]. Persoanele împuternicite de operator au, de asemenea, un rol important și trebuie să notifice orice încălcare operatorului lor[9].

5. CEPD consideră că cerința de notificare are o serie de avantaje. Atunci când notifică autoritatea de supraveghere, operatorii pot obține sfaturi dacă persoanele afectate ar trebui informate. Într-adevăr, autoritatea de supraveghere poate ordona operatorului să informeze aceste persoane despre încălcare[10]. Datorită informării persoanelor fizice despre o încălcare, operatorul poate transmite informații despre riscurile generate de încălcare și despre acțiunile, pe care acestea le pot întreprinde pentru a se proteja de consecințele posibile. Accentul oricărui plan de răspuns la încălcare ar trebui să fie pus pe protejarea persoanelor fizice și a datelor lor cu caracter personal. Astfel, notificarea încălcării ar trebui percepută ca un instrument de îmbunătățire a conformității pentru asigurarea protecției datelor cu caracter personal. În același timp, trebuie remarcat faptul că neinformarea unei persoane fizice sau unei autorități de supraveghere despre o încălcare poate însemna că, în temeiul articolului 83 din RGPD, operatorul ar putea fi sancționat.

6. Prin urmare, operatorii și persoanele împuternicite de operatori sunt încurajați să planifice în prealabil și să pună în aplicare procese de depistare și limitare rapidă a încălcării, pentru a evalua riscul pentru persoane fizice[11], și apoi pentru a determina dacă este necesar să fie notificată autoritatea de supraveghere competentă, și să comunice încălcarea persoanelor în cauză atunci când este necesar. Notificarea autorității de supraveghere ar trebui să facă parte din acest plan de răspuns la incidente.

7. Prevederile RGPD clarifică când trebuie notificată o încălcare și cui anume, precum și ce informații trebuie să conțină notificarea. Informațiile necesare pentru notificare pot fi transmite în etape, dar, în orice caz, operatorii ar trebui să acționeze în cazul oricărei încălcări în timp util.

---

[5] A se vedea http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0136 și http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A32013R0611

[6] A se vedea https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

[7] A se vedea http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046

[8] Drepturile prevăzute în Carta drepturilor fundamentale a UE, disponibilă la adresa http://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

[9] A se vedea articolul 33 alineatul (2) GDPR. După concept este similar cu articolul 5 din Regulamentul (UE) nr. 611/2013, care prevede că dacă un alt prestator este contractat pentru a furniza o parte a serviciului de comunicații electronice (fără a avea o relație contractuală directă cu abonații) acest alt prestator informează imediat prestatorul care l-a contractat în cazul în care are loc o încălcare a securității datelor cu caracter personal.

[10] A se vedea articolul 34 alienatul (4) și articolul 58 alineatul (2) litera (e) din RGPD.

[11] Acest lucru poate fi asigurat prin cerința de monitorizare și revizuire a unei EIPD, care este necesară pentru operațiunile de prelucrare susceptibile de a genera un risc înalt pentru drepturile și libertățile persoanelor fizice (articolul 35 alineatele (1) și (11).

8. În Avizul 03/2014 privind notificarea încălcării securității datelor cu caracter personal[12], WP29 a oferit îndrumări operatorilor pentru a-i ajuta să decidă să anunțe sau nu persoanele vizate în cazul unei încălcări. În Aviz a fost luată în considerare obligația prestatorilor de comunicații electronice cu privire la Directiva 2002/58/CE și au fost prezentate exemple din mai multe sectoare, în contextul proiectului RGPD de atunci, și au fost prezentate bune practici pentru toți operatorii.

9. În Orientările actuale sunt explicate cerințele obligatorii de notificare și comunicare a încălcării prevăzute în RGPD și unele acțiuni, pe care operatorii și persoanele împuternicite de operatori le pot efectua pentru a îndeplini aceste obligații. De asemenea, în Orientări sunt prezentate exemple de diferite tipuri de încălcări și cine ar trebui să fie notificat în diferite scenarii.

I. NOTIFICAREA ÎNCĂLCĂRII DATELOR CU CARACTER PERSONAL ÎN TEMEIUL RGPD

A. Considerații de bază legate de securitate

10. Conform unei cerințe prevăzute în RGPD, datele cu caracter personal trebuie să fie prelucrate prin măsuri tehnice și organizatorice adecvate într-un mod, care să asigure securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, distrugerii sau deteriorării accidentale.[13]

11. Astfel, RGPD obligă atât operatorii, cât și persoanele împuternicite de operator să dispună de măsuri tehnice și organizatorice adecvate pentru a asigura un nivel de securitate corespunzător riscului pentru datele cu caracter personal, care sunt prelucrate. Aceștia ar trebui să țină cont de nivelul actual de dezvoltare a tehnologiilor, costurile de implementare și tipul, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscul de probabilitate și severitate variabile pentru drepturile și libertățile persoanelor.[14] De asemenea, conform RGPD toate măsurile tehnologice de protecție și organizatorice adecvate trebuie să fie puse în aplicare pentru a stabili imediat dacă a avut loc o încălcare, și apoi a determina dacă există obligația de notificare[15].

12. Astfel, un element-cheie al oricărei politici de securitate a datelor cu caracter personal este capacitatea, atunci când este posibil, de a preveni o încălcare și, în cazul în care aceasta are loc, de a reacționa la aceasta în timp util.

B. Ce este o încălcare a securității datelor cu caracter personal?

1. Definiție

13. Ca parte a oricărei încercări de a aborda o încălcare, operatorul ar trebui să poată mai întâi să o recunoască. RGPD definește „încălcarea securității datelor cu caracter personal” la articolul 4 alineatul (12) astfel:

> *„o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea.”*

[12] A se vedea Avizul 03/2014 al WP29 cu privire la notificarea privind încălcarea securității datelor cu caracter personal http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2014/wp213_en.pdf
[13] A se vedea articolul 5 alienatul (1) litera (f) și articolul 32 din RGPD.
[14] Articolul 32; a se vedea, de asemenea Considerentul 83 din RGPD.
[15] A se vedea Considerentul 87 din RGPD.

14. Ceea ce se înțelege prin „distrugerea” datelor cu caracter personal ar trebui să fie destul de clar: datele nu mai există sau nu mai există într-o formă care poate, de obicei, să fie folosită de operator. „Prejudiciul” ar trebui să fie, de asemenea, relativ clar: datele cu caracter personal au fost modificate, corupte sau nu mai sunt complete. În ceea ce privește „pierderea” datelor cu caracter personal, aceasta ar însemna că datele încă mai pot exista, dar operatorul a pierdut controlul asupra lor sau accesul la acestea sau nu le mai posedă. În cele din urmă, prelucrarea neautorizată sau ilegală poate include dezvăluirea datelor cu caracter personal (sau accesul la acestea de către) destinatarilor, care nu sunt autorizați să primească (sau să acceseze) datele, sau orice altă formă de prelucrare care încalcă prevederile RGPD.

Exemplu
Un exemplu de pierdere a datelor cu caracter personal poate fi situația, în care un dispozitiv care conține o copie a bazei de date ale clienților unui operator a fost pierdut sau furat. Un alt exemplu de pierdere poate fi cazul în care unica copie a unui set de date cu caracter personal a fost criptată de către un ransomware sau de către operator folosind o cheie, care nu mai este în posesia sa.

15. Ceea ce ar trebui să fie clar este că o încălcare este un tip de incident de securitate. Cu toate acestea, astfel cum este specificat la articolul 4 alineatul (12), RGPD se aplică doar în cazul în care există o încălcare a securității datelor cu caracter personal. Consecința unei astfel de încălcări este că operatorul nu va putea asigura conformitatea cu principiile referitoare la prelucrarea datelor cu caracter personal, conform articolului 5 din RGPD. Aceasta evidențiază diferența dintre un incident de securitate și o încălcare a securității datelor cu caracter personal, cu alte cuvinte dacă toate încălcările securității datelor cu caracter personal sunt incidente de securitate, nu toate incidentele de securitate sunt neapărat încălcări ale securității datelor cu caracter personal.[16]

16. Efectele adverse potențiale ale unei încălcări asupra persoanelor sunt analizate mai jos.

2. Tipurile de încălcări ale securității datelor cu caracter personal

17. În Avizul său 03/2014 privind notificarea încălcării, WP29 a explicat că încălcările pot fi clasificate în conformitate cu următoarele trei principii binecunoscute de securitate a informațiilor[17]:

- „**Încălcarea confidențialității**” – în cazul unei dezvăluiri neautorizate sau accidentale a datelor cu caracter personal sau accesului la acestea.
- „**Încălcarea integrității**” – în cazul unei modificări neautorizate sau accidentale a datelor cu caracter personal.
- „**Încălcarea disponibilității**” – în cazul unei pierderi accidentale sau neautorizate a accesului la[18] datele cu caracter personal sau distrugerea acestora.

18. De asemenea, trebuie menționat faptul că, în dependență de circumstanțe, o încălcare poate afecta confidențialitatea, integritatea și disponibilitatea datelor cu caracter personal în același timp, precum și orice combinație a acestora.

[16] Trebuie remarcat faptul că un incident de securitate nu se limitează la modelele de amenințare în care un atac este făcut asupra unei organizații dintr-o sursă externă, ci include incidente din prelucrarea internă care încalcă principiile de securitate.
[17] A se vedea Avizul 03/2014 al WP29.
[18] Este stabilit că „accesul” face parte fundamentală din „disponibilitate”. A se vedea, de exemplu, NIST SP80053rev4, care definește „disponibilitatea” ca: „Asigurarea accesului în timp util și fiabil la informații și utilizarea acestora”, disponibil la adresa http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. CNSSI-4009 de asemenea, se referă la: „Acces în timp util, fiabil la servicii de date și de informații pentru utilizatorii autorizați”. A se vedea https://rmf.org/wpcontent/uploads/2017/10/CNSSI-4009.pdf. ISO/IEC 27000:2016, de asemenea, definește „disponibilitatea” ca „Proprietatea de a fi accesibil și utilizabil la cererea unei entități autorizate”: https://www.iso.org/obp/ui/#iso:std:isoiec:27000:ed-4:v1:en

19. Dacă procesul de stabilire a faptului dacă a existat o încălcare a confidențialității sau a integrității este relativ clar, stabilirea faptului dacă a existat o încălcare a disponibilității poate fi mai puțin clar. O încălcare va fi întotdeauna considerată o încălcare a disponibilității, dacă datele cu caracter personal au fost pierdute sau distruse definitiv.

Exemplu
Exemplele de pierdere a disponibilității includ cazurile, în care datele au fost șterse fie accidental, fie de către o persoană neautorizată sau, în exemplul datelor criptate în siguranță, a fost pierdută cheia de decriptare. În cazul în care operatorul nu poate restabili accesul la date, de exemplu, dintr-o copie de rezervă, atunci aceasta este considerată o pierdere definitivă a disponibilității.

O pierdere a disponibilității poate exista și în cazul unei întreruperi semnificative a serviciului normal al unei organizații, de exemplu, o cădere de curent sau un atac de refuzare a serviciului, din cauza cărora datele personale nu sunt disponibile.

20. Se poate pune întrebarea dacă o pierdere temporară a disponibilității datelor cu caracter personal ar trebui considerată o încălcare și, în caz afirmativ, una care trebuie notificată. Articolul 32 din RGPD, „securitatea prelucrării", explică că atunci când se implementează măsuri tehnice și organizatorice pentru a asigura un nivel de securitate adecvat riscului, ar trebui să fie luată în considerare, printre altele, *„capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare"* și *„capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică".*

21. Prin urmare, un incident de securitate, din cauza căruia datele cu caracter personal nu sunt accesibile o perioadă de timp este, de asemenea, un tip de încălcare, deoarece lipsa accesului la date poate avea un impact semnificativ asupra drepturilor și libertăților persoanelor fizice. Pentru claritate, dacă datele cu caracter personal nu sunt disponibile din cauza lucrărilor de mentenență planificate a sistemului, aceasta nu reprezintă o „încălcare a securității", astfel cum este definit la articolul 4 alineatul (12) din RGPD.

22. Ca și în cazul pierderii sau distrugerii permanente a datelor cu caracter personal (sau în cazul oricărui alt tip de încălcare), o încălcare care implică pierderea temporară a disponibilității ar trebui documentată în conformitate cu prevederile articolului 33 alineatul (5) din RGPD. Aceasta ajută operatorul să demonstreze răspunderea față de autoritatea de supraveghere, care poate solicita acces la aceste înregistrări[19]. Cu toate acestea, în dependență de circumstanțele încălcării, ar poate fi necesară notificarea autorității de supraveghere și a persoanelor afectate. Operatorul va trebui să evalueze probabilitatea și gravitatea impactului asupra drepturilor și libertăților persoanelor al indisponibilității datelor cu caracter personal. În conformitate cu articolul 33 din RGPD, operatorul va trebui să notifice, cu excepția cazului în care este puțin probabil ca încălcarea să genereze un risc pentru drepturile și libertățile persoanelor. Desigur, fiecare caz trebuie evaluat individual.

Exemplu
În contextul unui spital, dacă datele medicale critice despre pacienți nu sunt disponibile, chiar și temporar, acest fapt ar putea prezenta un risc pentru drepturile și libertățile persoanelor; de exemplu, intervențiile pot fi anulate și viețile pot fi puse în pericol.

În schimb, în cazul în care sistemele unei companii media nu sunt accesibile timp de câteva ore (de exemplu, din cauza unei pene de curent), dacă compania dată ulterior nu poate trimite buletine informative abonaților săi, este puțin probabil să existe un risc pentru drepturile și libertățile persoanelor.

[19] A se vedea articolul 33 alienatul (5) din RGPD.

23. Trebuie remarcat faptul că, deși o pierdere a disponibilității sistemelor unui operator poate fi doar temporară și poate să nu aibă un impact asupra persoanelor fizice, este important ca operatorul să ia în considerare toate consecințele posibile ale unei încălcări, deoarece totuși ar putea fi necesară o notificare din alte considerente.

Exemplu
Infectarea cu ransomware (software rău intenționat, care criptează datele operatorului până când se achită o recompensă) ar putea cauza o pierdere temporară a disponibilității, dacă datele pot fi restabilite din copia de rezervă. Cu toate acestea, a avut loc o intruziune în rețea, iar notificarea ar putea fi necesară dacă incidentul este calificat drept încălcare a confidențialității (adică datele cu caracter personal sunt accesate de atacator) și aceasta prezintă un risc pentru drepturile și libertățile persoanelor.

3. Consecințele posibile ale unei încălcări a datelor cu caracter personal

24. O încălcare poate avea o serie de efecte adverse semnificative asupra persoanelor, care pot cauza prejudicii fizice, materiale sau nemateriale. În RGPD se explică că aceasta poate include pierderea controlului asupra datelor lor personale, limitarea drepturilor lor, discriminarea, furtul de identitate sau frauda, pierdere financiară, inversarea neautorizată a pseudonimizării, deteriorarea imaginii și pierderea confidențialității datelor personale protejate de secretul profesional. Încălcarea mai poate include, de asemenea, orice alt dezavantaj economic sau social semnificativ pentru persoanele respective.[20]

25. Astfel, RGPD obligă operatorul să notifice o încălcare autorității de supraveghere competente, cu excepția cazului în care este puțin probabil să genereze un risc de producere a unor astfel de efecte adverse. Dacă există un risc potențial înalt de apariție a acestor efecte adverse, RGPD solicită operatorului să informeze despre încălcare persoanele afectate de îndată ce este posibil în mod rezonabil.[21]

26. Importanța de a putea identifica o încălcare, de a evalua riscul pentru persoane și apoi de a notifica dacă este necesar, este subliniată în Considerentul 87 din RGPD:

„Ar trebui să se stabilească dacă au fost implementate toate măsurile tehnologice de protecție și organizatorice corespunzătoare în scopul de a se stabili imediat dacă s-a produs o încălcare a securității datelor cu caracter personal și de a se informa cu promptitudine autoritatea de supraveghere și persoana vizată. Faptul că notificarea a fost efectuată fără întârziere nejustificată ar trebui stabilit luându-se în considerare, în special, natura și gravitatea încălcării securității datelor cu caracter personal, precum și consecințele și efectele negative ale acesteia asupra persoanei vizate. Această notificare poate conduce la o intervenție a autorității de supraveghere, în conformitate cu sarcinile și competențele specificate în prezentul regulament.”

27. Alte orientări privind evaluarea riscului producerii efectelor adverse asupra persoanelor sunt prezentate în secțiunea IV.

28. În cazul în care operatorii nu notifică nici autoritatea de supraveghere, nici persoanele vizate cu privire la o încălcare a securității datelor sau ambele, chiar dacă sunt îndeplinite cerințele articolelor 33 și/sau 34 din RGPD, autorității de supraveghere i se prezintă o alegere, care trebuie să făcută luând în considerare toate măsurile corective de care dispune, precum luarea în considerare a aplicării amenzii administrative corespunzătoare[22], fie împreună cu o măsură corectivă în temeiul articolului 58 alineatul (2) din RGPD, fie individual. Dacă se alege o amendă administrativă, valoarea acesteia poate fi de până la 10.000.000 euro sau, în cazul unei întreprinderi, de până la 2 % din cifra de afaceri mondială totală anuală în conformitate cu articolul 83 alineatul (4) litera (a) din RGPD. De asemenea, este important de reținut faptul că, în unele

[20] A se vedea, de asemenea Considerentele 85 și 75 din RGPD.
[21] A se vedea, de asemenea Considerentul 86 din RGPD.
[22] Pentru mai multe detalii, consultați Orientările WP29 privind aplicarea și stabilirea amenzilor administrative, disponibile aici: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

cazuri, dacă o încălcare nu este notificată, ar putea fi dezvăluită lipsa măsurilor de securitate sau neadecvarea măsurilor de securitate existente. Orientările WP29 privind amenzile administrative precizează: *„Apariția mai multor încălcări diferite comise împreună într-un caz particular înseamnă că autoritatea de supraveghere poate aplica amenzile administrative la un nivel, care este eficient, proporțional și disuasiv, în limita celei mai grave încălcări*". În acest caz, autoritatea de supraveghere va avea, de asemenea, posibilitatea de a aplica sancțiuni pentru nenotificarea sau necomunicarea încălcării (articolele 33 și 34 din RGPD), pe de o parte, și pentru lipsa măsurilor de securitate (adecvate) (articolul 32 din RGPD) pe de altă parte, deoarece sunt două încălcări separate.

II. ARTICOLUL 33 – NOTIFICAREA AUTORITĂŢII DE SUPRAVEGHERE

A. Când este necesară notificarea

1. Cerințele articolului 33

29. Articolul 33 alineatul (1) din RGPD prevede următoarele:

> *„ În cazul în care are loc o încălcare a securității datelor cu caracter personal, operatorul notifică acest lucru autorității de supraveghere competente în temeiul articolului 55, fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta, cu excepția cazului în care este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice. În cazul în care notificarea nu are loc în termen de 72 de ore, aceasta este însoțită de o explicație motivată a întârzierii din partea autorității de supraveghere."*

30. Considerentul 87 din RGPD precizează[23]:

> *„Ar trebui să se stabilească dacă au fost implementate toate măsurile tehnologice de protecție și organizatorice corespunzătoare în scopul de a se stabili imediat dacă s-a produs o încălcare a securității datelor cu caracter personal și de a se informa cu promptitudine autoritatea de supraveghere și persoana vizată. Faptul că notificarea a fost efectuată fără întârziere nejustificată ar trebui stabilit luându-se în considerare, în special, natura și gravitatea încălcării securității datelor cu caracter personal, precum și consecințele și efectele negative ale acesteia asupra persoanei vizate. Această notificare poate conduce la o intervenție a autorității de supraveghere, în conformitate cu sarcinile și competențele specificate în prezentul regulament."*

2. Când un operator „a luat cunoștință"?

31. După cum este prezentat detaliat mai sus, RGPD obligă operatorul, în cazul unei încălcări, să notifice încălcarea fără întârzieri nejustificate și, dacă este posibil, în cel mult 72 de ore după ce a luat cunoștință de aceasta. Astfel, poate apărea întrebarea când se poate considera că operatorul „a luat cunoștință" de o încălcare. CEPD consideră că un operator ar trebui să fie considerat că „a luat cunoștință" atunci când operatorul are un grad rezonabil de certitudine că a avut loc un incident de securitate, care a dus la compromiterea datelor cu caracter personal.

32. Cu toate acestea, după cum s-a indicat anterior, RGPD obligă operatorul să pună în aplicare toate măsurile tehnice și organizatorice adecvate pentru a stabili imediat dacă a avut loc o încălcare și pentru a informa cu promptitudine autoritatea de supraveghere și persoanele vizate. De asemenea, acesta precizează că faptul că notificarea a fost efectuată fără întârzieri nejustificate ar trebui stabilit ținând cont, în special, de natura și gravitatea încălcării și de consecințele și efectele negative ale acesteia pentru

[23] Considerentul 85 din RGPD, de asemenea, este important aici.

persoana vizată[24]. Astfel, operatorul este obligat să asigure că va „lua cunoștință” de orice încălcare în timp util, astfel încât să poată lua măsurile corespunzătoare.

33. Când, exact, se poate considera că un operator „a luat cunoștință” de o anumită încălcare, va depinde de circumstanțele încălcării respective. În unele cazuri, va fi relativ clar de la început că a existat o încălcare, în timp ce în alte cazuri, poate dura ceva timp pentru a stabili dacă datele cu caracter personal au fost compromise. Cu toate acestea, accentul ar trebui să se pună pe acțiunile prompte de investigare a unui incident pentru a determina dacă securitatea datelor cu caracter personal a fost într-adevăr încălcată și, dacă da, pentru a lua măsuri de remediere și a notifica, dacă este necesar.

Exemple

1. În cazul pierderii unei chei USB cu date personale necriptate, deseori nu este posibil să se stabilească dacă persoane neautorizate au obținut acces la aceste date. Totuși, chiar dacă operatorul nu poate stabili dacă a avut loc o încălcare a confidențialității, un astfel de caz trebuie notificat, deoarece există un grad rezonabil de certitudine că a avut loc o încălcare a disponibilității; operatorul probabil „a luat cunoștință” atunci când a conștientizat că cheia USB a fost pierdută.

2. O parte terță informează un operator că a primit accidental datele cu caracter personal ale unuia dintre clienții săi și prezintă dovezi ale dezvăluirii neautorizate. Deoarece operatorului i-au fost prezentate dovezi clare ale încălcării confidențialității, nu poate exista nicio îndoială că „a luat cunoștință” de încălcare.

3. Un operator suspectează o intruziune posibilă în rețeaua sa. Operatorul își verifică sistemele pentru a stabili dacă datele cu caracter personal din sisteme au fost compromise și află că suspiciunea sa s-a confirmat. Astfel, deoarece acum operatorul are dovezi clare ale unei încălcări, nu poate exista nicio îndoială că „a luat cunoștință” de aceasta.

4. Un criminal cibernetic contactează operatorul după ce i-a spart sistemul pentru a cere o recompensă. În acest caz, după ce și-a verificat sistemul pentru a stabili cu certitudine că a fost atacat, operatorul are dovezi clare că a avut loc o încălcare și nu există nicio îndoială că „a luat cunoștință”.

34. După ce operatorul a fost informat despre o încălcare potențială mai întâi de către o persoană fizică, o organizație media sau o altă sursă, sau când a depistat el însuși un incident de securitate, operatorul poate întreprinde o investigație pe o perioadă scurtă de timp pentru a stabili dacă de fapt a avut loc o încălcare. În această perioadă de investigație, operatorul poate să nu fie considerat că „a luat cunoștință” de încălcare. Cu toate acestea, este de așteptat ca investigația inițială să înceapă cât mai curând posibil și să stabilească cu un grad rezonabil de certitudine, dacă a avut loc o încălcare; ulterior poate urma o investigație mai detaliată.

35. Odată ce operatorul a luat cunoștință, o încălcare care poate fi notificată trebuie notificată fără întârzieri nejustificate și, dacă este fezabil, nu mai târziu de 72 de ore. În această perioadă, operatorul ar trebui să evalueze riscul probabil pentru persoane fizice pentru a determina dacă cerința de notificare a fost declanșată, precum și acțiunile necesare pentru a aborda încălcarea. Cu toate acestea, un operator poate avea deja o evaluare inițială a riscului potențial, care ar putea fi generat de o încălcare, efectuată în cadrul unei evaluări a impactului privind protecția datelor (EIPD)[25] înainte de operațiunea de prelucrare în cauză. Cu toate acestea, EIPD poate fi mai generală în comparație cu circumstanțele specifice ale oricărei încălcări efective și, prin urmare, în orice caz, va trebui efectuată o evaluare suplimentară ținând cont aceste circumstanțe. Pentru mai multe detalii despre evaluarea riscului, consultați secțiunea IV.

[24] A se vedea Considerentul 87 din RGPD.

[25] A se vedea Orientările WP29, WP248 privind EIPD-urile aici: http://ec.europa.eu/newsroom/document.cfmPdoc id=44137

36. În majoritatea cazurilor, aceste acțiuni preliminare ar trebui finalizate imediat după alerta inițială (adică atunci când operatorul sau persoana împuternicită de operator are suspiciuni că a avut loc un incident de securitate, care poate afecta date cu caracter personal), ar trebui să dureze mai mult doar decât în cazuri excepționale.

Exemplu
O persoană informează operatorul că a primit un mesaj e-mail, care imită identitatea operatorului și conține date cu caracter personal referitoare la utilizarea (reală) a serviciului operatorului, sugerând că securitatea operatorului a fost compromisă. Operatorul efectuează o investigație o perioadă scurtă de timp și identifică o intruziune în rețeaua sa și dovezi de acces neautorizat la datele cu caracter personal. Acum se consideră că operatorul ar fi „luat cunoștință" și autoritatea de supraveghere trebuie notificată despre incident, cu excepția cazului în care este puțin probabil să prezinte un risc pentru drepturile și libertățile persoanelor. Operatorul va trebui să ia măsuri corective adecvate pentru a soluționa încălcarea.

37. Prin urmare, operatorul ar trebui să aibă procese interne puse în aplicare pentru a putea depista și soluționa o încălcare. De exemplu, pentru identificarea unor nereguli în prelucrarea datelor, operatorul sau persoana împuternicită de operator poate utiliza anumite măsuri tehnice cum ar fi fluxul de date și analizoare de jurnal, din care pot fi identificate evenimente și alerte prin corelarea oricăror date de jurnal[26]. Este important ca atunci când este depistată o încălcare, să fie raportată la nivelul corespunzător de conducere, astfel încât să poată fi soluționată și, dacă este necesar, notificată în conformitate cu articolul 33 și, în caz de necesitate, conform articolului 34. Astfel de măsuri și mecanisme de raportare ar putea fi prevăzute detaliat în planurile de răspuns la incidente și/sau în aranjamentele de gestionare ale operatorului. Acestea vor ajuta operatorul să planifice și să determine eficient cine din cadrul organizației are responsabilitatea operațională pentru gestionarea unei încălcări și cum sau dacă ar trebui să raporteze un incident, în dependență de caz.

38. Operatorul ar trebui, de asemenea, să încheie acorduri cu orice persoane împuternicite de operator și implicate de acesta, care trebuie să prevadă că ele însăși au obligația de a notifica operatorul în cazul unei încălcări (a se vedea mai jos).

39. Deși operatorii și persoanele împuternicite de operatori au responsabilitatea de a pune în aplicare măsuri adecvate pentru a putea preveni, reacționa și soluționa o încălcare, există câțiva pași practici, care ar trebui efectuați în toate cazurile.

- Informațiile referitoare la toate evenimentele legate de securitate ar trebui să fie transmise unei persoane sau persoanelor responsabile, care au sarcina de a aborda incidente, de a stabili existența unei încălcări și de a evalua riscul.
- Riscul pentru persoane fizica generat de o încălcare ar trebui ulterior evaluat (probabilitatea neexistenței unui risc, existenței unui risc sau unui risc ridicat), informând unitățile relevante ale organizației.
- În caz de necesitate, autoritatea de supraveghere și, eventual, persoanele afectate trebuie notificate.
- În același timp, operatorul ar trebui să acționeze pentru a limita și a remedia încălcarea. Documentarea încălcării ar trebui să aibă loc pe măsura derulării.

40. Astfel, trebuie să fie clar că operatorul este obligat să acționeze în cazul oricărei semnalări inițiale și să stabilească dacă a avut loc sau nu o încălcare efectivă. În această perioadă scurtă de timp poate fi efectuată o anumită investigație, iar operatorul ar putea prezenta dovezi și alte detalii relevante. Cu toate acestea, odată ce operatorul a stabilit cu un grad rezonabil de certitudine că a avut loc o încălcare, dacă au fost îndeplinite condițiile prevăzute la articolul 33 alineatul (1) din RGPD, operatorul trebuie să notifice

[26] Trebuie menționat faptul că datele de jurnal, care facilitează auditabilitatea, de exemplu, stocarea, modificările sau ștergerea datelor pot fi, de asemenea, calificate drept date cu caracter personal referitoare la persoana care a inițiat operațiunea de prelucrare respectivă.

autoritatea de supraveghere fără întârzieri nejustificate și, dacă este fezabil, nu mai târziu de 72 de ore[27]. În cazul în care un operator nu întreprinde acțiuni în timp util și devine evident că a avut loc o încălcare, se poate considera că încălcarea nu a fost notificată în conformitate cu articolul 33 din RGPD.

41. Articolul 32 din RGPD precizează că operatorul și persoana împuternicită de operator ar trebui să dispună de măsuri tehnice și organizatorice adecvate pentru a asigura un nivel adecvat de securitate a datelor cu caracter personal: capacitatea de a depista, a soluționa și a raporta o încălcare în timp util ar trebui văzută ca element esenţial al acestor măsuri.

3. Operatorii asociați

42. Articolul 26 din RGPD se referă la operatorii asociați și precizează că operatorii asociași trebuie să stabilească responsabilitățile lor respective pentru a asigura conformitatea cu prevederile RGPD[28]. Acestea vor include determinarea părții, care va fi responsabilă pentru îndeplinirea obligațiilor prevăzute la articolele 33 și 34 din RGPD. CEPD recomandă ca aranjamentele contractuale dintre operatorii asociați să includă prevederi, care stabilesc care operator va prelua conducerea sau va fi responsabil pentru îndeplinirea obligațiilor de notificare a încălcării prevăzute de RGPD.

4. Obligațiile persoanei împuternicite de operator

43. Operatorul are responsabilitatea generală pentru protecția datelor cu caracter personal, însă persoana împuternicită de operator are un rol important în asigurarea îndeplinirii obligațiilor de către operator, care include notificarea încălcării. Într-adevăr, articolul 28 alineatul (3) din RGPD specifică că prelucrarea de către un operator este reglementată de un contract sau de un alt act juridic. Conform articolului 28 alineatul (3) litera (f), contractul sau un alt act juridic trebuie să prevadă că persoana împuternicită „ajută operatorul să asigure respectarea obligațiilor prevăzute la articolele 32-36, ținând seama de caracterul prelucrării și informațiile aflate la dispoziția persoanei împuternicite de operator”.

44. Articolul 33 alineatul (2) din RGPD precizează clar că, în cazul în care un operator implică o persoană împuternicită de operator și aceasta ia cunoștință de o încălcare a securității datelor cu caracter personal, pe care le prelucrează în numele operatorului, ea trebuie să notifice operatorul „fără întârzieri nejustificate”. Trebuie menționat faptul că operatorul nu trebuie mai întâi să evalueze probabilitatea riscului, care decurge dintr-o încălcare înainte de a notifica operatorul; operatorul este cel care trebuie să efectueze această evaluare în momentul în care a luat cunoștință de încălcare. Persoana împuternicită de operator trebuie doar să stabilească dacă a avut loc o încălcare și apoi să notifice operatorul. Operatorul implică persoana pe care a împuternicit-o pentru a-și atinge scopurile; prin urmare, în principiu, ar trebui să fie considerat că operatorul „a luat cunoștință” după ce a fost informat de persoana împuternicită despre încălcare. Obligația persoanei împuternicite de operator de a-și notifica operatorul îi permite operatorului să remedieze încălcarea și să determine dacă este sau nu obligat să notifice autoritatea de supraveghere în conformitate cu articolul 33 alineatul (1) și persoanele afectate în conformitate cu articolul 34 alineatul (1). Operatorul ar putea dori, de asemenea, să investigheze încălcarea, deoarece persoana împuternicită de operator ar putea să nu cunoască toate faptele relevante legate de incident, de exemplu, dacă o copie sau o copie de rezervă a datelor cu caracter personal distrusă sau pierdută de către persoana împuternicită de operator încă mai este păstrată de către operator. Astfel poate fi stabilit faptul dacă operatorul va trebui să notifice sau nu.

45. RGPD nu prevede un termen explicit, în care persoana împuternicită de operator trebuie să alerteze operatorul, cu excepția faptului că trebuie să o facă „fără întârzieri nejustificate”. Prin urmare, CEPD recomandă ca persoana împuternicită de operator să notifice operatorul imediat, transmițând informații

[27] A se vedea Regulamentul nr. 1182/71 privind stabilirea regulilor, care se aplică termenelor, datelor și expirării termenelor, disponibil la: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31971R1182&from=EN
[28] A se vedea, de asemenea, Considerentul 79 din RGPD.

suplimentare despre încălcarea în etape, pe măsură ce află mai multe detalii. Aceasta este important pentru a ajuta operatorul să îndeplinească cerința de notificare a autorității de supraveghere în termen de 72 de ore.

46. După cum este explicat mai sus, contractul dintre operator și persoana împuternicită de operator ar trebui să stipuleze, în afară de alte prevederi din RGPD, modul în care cerințele prevăzute la articolul 33 alineatul (2) ar trebui îndeplinite. Acesta poate include cerințe de notificare în timp util de către persoana împuternicită de operator, care la rândul lor facilitează îndeplinirea obligațiilor operatorului de a notificarea autoritatea de supraveghere în termen de 72 de ore.

47. În cazul în care persoana împuternicită de operator prestează servicii mai multor operatori, care sunt toți afectați de același incident, persoana împuternicită de operator va trebui să comunice detaliile incidentului fiecărui operator.

48. O persoană împuternicită de operator poate efectua o notificare în numele operatorului, dacă operatorul i-a acordat împuternicirea corespunzătoare și aceasta este prevăzută de aranjamentele contractuale dintre operator și persoana împuternicită de operator. O astfel de notificare trebuie efectuată în conformitate cu articolele 33 și 34 din RGPD. Cu toate acestea, este important de menționat că de notificare juridic este responsabil operatorul.

B. Transmiterea informațiilor către autoritatea de supraveghere

1. Informațiile care trebuie transmise

49. În cazul în care un operator notifică o încălcare autorității de supraveghere, conform articolului 33 alineatul (3) din RGPD notificarea cel puțin:

„(a) descrie caracterul încălcării securității datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ al persoanelor vizate în cauză, precum și categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;
(b) *comunică numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;*
(c) *descrie consecințele probabile ale încălcării securității datelor cu caracter personal;*
(d) *descrie măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.”*

50. RGPD nu definește categoriile de persoane vizate sau înregistrările de date cu caracter personal. Cu toate acestea, CEPD sugerează că categoriile de persoane vizate se refere la diferite tipuri de persoane, ale căror date cu caracter personal au fost afectate de o încălcare: în dependență de descriptorii utilizați, acestea ar putea fi, printre altele, copii și alte grupuri vulnerabile, persoane cu dizabilități, angajați sau clienți. În mod similar, categoriile de înregistrări de date cu caracter personal se pot referi la diferitele tipuri de înregistrări, pe care le poate prelucra operatorul, cum ar fi date de sănătate, înregistrări educaționale, informații de asistență socială, date financiare, numere de conturi bancare, numere indicate în pașapoarte etc.

51. Considerentul 85 din RGPD prevede clar că unul din scopurile notificării este limitarea prejudiciului cauzat persoanelor fizice. Astfel, dacă tipurile de persoane vizate sau tipurile de date cu caracter personal indică un risc de cauzare a unor prejudicii speciale ca urmare a unei încălcări (de exemplu, furt de identitate, fraudă, pierdere financiară, amenințare a secretului profesional), este important ca în notificare să fie indicate aceste categorii. Astfel, se aplică cerința de a descrie consecințele probabile ale încălcării.

52. În cazul în care nu sunt disponibile informații precise (de exemplu, numărul exact de persoane vizate), aceasta nu ar trebui să constituie un obstacol pentru notificarea în timp util a încălcării. RGPD permite indicarea aproximativă a numărului de persoane afectate și a numărului de înregistrări de date cu caracter personal în cauză. Accentul ar trebui să fie pus pe abordarea efectelor negative ale încălcării, și nu pe indicarea cifrelor precise.

53. Astfel, atunci când este cert că a fost comisă o încălcare, însă amploarea acesteia nu este încă cunoscută, notificarea în etape (a se vedea mai jos) este o modalitate sigură de a îndeplini obligațiile de notificare.

54. Articolul 33 alineatul (3) din RGPD prevede că operatorul „cel puțin" trebuie să furnizeze aceste informații printr-o notificare, astfel încât, dacă este necesar, operatorul să poată decide să ofere detalii suplimentare. Pentru diferite tipuri de încălcări (de confidențialitate, integritate sau disponibilitate) ar putea fi necesară furnizarea informațiilor suplimentare pentru a explica pe deplin circumstanțele fiecărui caz.

Exemplu
Ca parte a notificării sale adresate autorității de supraveghere, un operator poate considera util să indice persoana împuternicită dacă ea este cauza principală a unei încălcări, în special dacă aceasta a cauzat un incident, care afectează înregistrările de date cu caracter personal ale multor altor operatori, care implică aceeași persoană împuternicită.

55. În orice caz, autoritatea de supraveghere poate solicita detalii suplimentare în cadrul investigației sale a unei încălcări.

2. Notificarea în etape

56. În dependență de tipul încălcării, poate fi necesară efectuarea unei investigații suplimentare de către operator pentru a stabili toate faptele relevante ale incidentului. Prin urmare, articolul 33 alineatul (4) din RGPD prevede:

„Atunci când și în măsura în care nu este posibil să se furnizeze informațiile în același timp, acestea pot fi furnizate în mai multe etape, fără întârzieri nejustificate."

57. Aceasta înseamnă că RGPD recunoaște că operatorii nu vor avea întotdeauna toate informațiile necesare despre o încălcare în termen de 72 de ore după ce au luat cunoștință despre aceasta, deoarece este posibil ca detaliile complete și cuprinzătoare ale incidentului să nu fie întotdeauna disponibile în acest termen inițial. Ca atare, se permite efectuarea unei notificări în etape. Este mai probabil ca notificarea să aibă loc în etape în cazul încălcărilor mai complexe, cum ar fi unele tipuri de incidente de securitate cibernetică în care, de exemplu, poate fi necesară o investigație criminalistică aprofundată pentru a stabili complet tipul încălcării și măsura în care au fost compromise datele cu caracter personal. Astfel, în multe cazuri, operatorul va trebui să efectueze mai multe investigații și să prezinte informații suplimentare ulterior. Aceasta se permite, cu condiția ca operatorul să indice motivele întârzierii, în conformitate cu articolul 33 alineatul (1) din RGPD. CEPD recomandă ca, atunci când operatorul notifică pentru prima dată autoritatea de supraveghere, acesta ar trebui să o informeze dacă operatorul nu deține încă toate informațiile necesare și să prezinte mai multe detalii ulterior. Autoritatea de supraveghere ar trebui să convină cum și când ar trebui furnizate informații suplimentare. Aceasta nu împiedică operatorul să transmită informații suplimentare la orice etapă ulterioară, dacă află detalii suplimentare relevante despre încălcare, care trebuie comunicate autorității de supraveghere.

58. Obiectivul cerinței de notificare este de a încuraja operatorii să acționeze cu promptitudine în cazul unei încălcări, să o limiteze și, dacă este posibil, să recupereze datele cu caracter personal compromise și să solicite consiliere relevantă de la autoritatea de supraveghere. Notificarea autorității de supraveghere

în primele 72 de ore poate permite operatorului să se asigure că deciziile privind notificarea sau nenotificarea persoanelor fizice sunt corecte.

59. Cu toate acestea, scopul notificării autorității de supraveghere nu este doar de a obține îndrumări cu privire la notificarea persoanelor afectate. În unele cazuri va fi evident că, din cauza tipului încălcării și a gravității riscului, operatorul va trebui să notifice persoanele afectate fără întârziere. De exemplu, dacă există o amenințare imediată de furt de identitate sau dacă categorii speciale de date cu caracter personal[29] sunt dezvăluite online, operatorul ar trebui să acționeze fără întârzieri nejustificate pentru a limita încălcarea și pentru a o comunica persoanelor în cauză (a se vedea secțiunea III). În circumstanțe excepționale, aceasta poate avea loc chiar înainte de notificarea autorității de supraveghere. În general, notificarea autorității de supraveghere poate să nu servească drept justificare a neinformării persoanei vizate despre încălcare atunci când este necesar.

60. De asemenea, ar trebui să fie clar că, după o notificare inițială, un operator ar putea transmite autorității de supraveghere informații actualizate dacă în cadrul unei investigații ulterioare sunt identificate dovezi că incidentul de securitate a fost limitat și de fapt nu a avut loc nicio încălcare. Ulterior aceste informații ar putea fi adăugate la informațiile deja transmise autorității de supraveghere, iar incidentul ar putea fi înregistrat ca nefiind o încălcare. Nu se prevede nicio penalizare pentru raportarea unui incident care, în cele din urmă, se constată că nu constituie o încălcare.

Exemplu
Un operator informează autoritatea de supraveghere în termen de 72 de ore de la depistarea unei încălcări că a pierdut o cheie USB, care conține o copie a datelor cu caracter personal ale unor clienți ai săi. Ulterior se constată că cheia USB a fost lăsată într-un loc necorespunzător la sediul operatorului și este recuperată. Operatorul informează autoritatea de supraveghere și solicită modificarea notificării.

61. Trebuie remarcat faptul că o abordare treptată a notificării este deja un caz, față de care se aplică obligațiile prevăzute la Directiva 2002/58/CE, Regulamentul 611/2013 și alt incident auto-raportat.

3. Notificările întârziate

62. Articolul 33 alineatul (1) din RGPD precizează că, în cazul în care autoritatea de supraveghere nu este notificată în termen de 72 de ore, trebuie să fie prezentate motivele întârzierii. Această prevedere, precum și noțiunea de notificare în etape, recunoaște că un operator nu poate întotdeauna să notifice o încălcare în acest termen și că întârzierea notificării este admisibilă.

63. Un astfel de scenariu ar putea avea loc în cazul în care, de exemplu, un operator se confruntă cu mai multe încălcări similare ale confidențialității într-o perioadă scurtă de timp, care afectează în același mod un număr mare de persoane vizate. Un operator poate lua conștiință de o încălcare și, în timp ce își începe investigația și înainte de notificare, poate depista încălcări similare, care au cauze diferite. În dependență de circumstanțe, poate dura ceva timp până când operatorul va stabili amploarea încălcărilor și, în loc să notifice fiecare încălcare separat, operatorul notifică odată despre mai multe încălcări foarte similare, care ar avea diferite cauze. Din acest motiv notificarea autorității de supraveghere ar putea întârzia cu mai mult de 72 de ore după ce operatorul a luat cunoștință de aceste încălcări.

64. Strict vorbind, fiecare încălcare individuală este un incident, care poate fi raportat. Cu toate acestea, pentru a nu fi excesiv de împovărat, operatorul poate prezenta o notificare „în grup” a tuturor acestor încălcări, cu condiția ca acestea să se refere la același tip de date cu caracter personal, securitatea cărora este încălcată în același mod, într-un interval de timp relativ scurt. În cazul în care are loc o serie de

[29] A se vedea articolul 9 din RGPD.

încălcări a securității diferitelor tipuri de date cu caracter personal, comise în moduri diferite, notificarea ar trebui să fie efectuată în mod normal, fiecare încălcare fiind raportată în conformitate cu articolul 33.

65. În timp ce RGPD permite întârzierea notificării într-o anumită măsură, acest lucru nu ar trebui să fie văzut ca ceva, ce are loc în mod regulat. Trebuie subliniat faptul că notificările în grup pot fi făcute și pentru mai multe încălcări similare raportate în termen de 72 de ore.

C. Încălcările transfrontaliere și încălcările comise la entitățile din afara UE

1. Încălcările transfrontaliere

66. În cazul unei prelucrări transfrontaliere[30] a datelor cu caracter personal, o încălcare poate afecta persoanele vizate din mai mult de un stat membru. Articolul 33 alineatul (1) din RGPD precizează clar că, atunci când a avut loc o încălcare, operatorul trebuie să notifice autoritatea de supraveghere competentă în conformitate cu articolul 55 din RGPD[31]. Articolul 55 alineatul (1) din RGPD prevede următoarele:

> *„Fiecare autoritate de supraveghere are competența să îndeplinească sarcinile și să exercite competențele care îi sunt conferite în conformitate cu prezentul regulament pe teritoriul statului membru de care aparține."*

67. Cu toate acestea, articolul 56 alineatul (1) din RGPD stipulează:

> *„Fără a aduce atingere articolului 55, autoritatea de supraveghere a sediului principal sau a sediului unic al operatorului sau al persoanei împuternicite de operator este competentă să acționeze în calitate de autoritate de supraveghere principală pentru prelucrarea transfrontalieră efectuată de respectivul operator sau respectiva persoană împuternicită în cauză în conformitate cu procedura prevăzută la articolul 60."*

68. De asemenea, articolul 56 alineatul (6) din RGPD prevede:

> *„Autoritatea de supraveghere principală este singurul interlocutor al operatorului sau al persoanei împuternicite de operator în ceea ce privește prelucrarea transfrontalieră efectuată de respectivul operator sau de respectiva persoană împuternicită de operator."*

69. Aceasta înseamnă că ori de câte ori are loc o încălcare în contextul prelucrării transfrontaliere și trebuie notificată, operatorul va trebui să notifice autoritatea principală de supraveghere[32]. Prin urmare, atunci când își elaborează planul de răspuns la încălcări, operatorul trebuie să stabilească care este autoritatea de supraveghere principală, pe care va trebui să o notifice.[33] Astfel, operatorul va putea să răspundă prompt la o încălcare și să își îndeplinească obligațiile prevăzute la articolul 33. Ar trebui să fie clar că, în cazul unei încălcări care implică prelucrarea transfrontalieră, trebuie notificată autoritatea de supraveghere principală, care coincide neapărat cu locul unde se află persoanele vizate sau chiar cu locul unde a avut loc încălcarea. Atunci când notifică autoritatea principală, operatorul ar trebui să indice, după caz, dacă încălcarea implică entități din alte state membre și în ce state membre persoanele vizate ar putea fi afectate de încălcare. Dacă operatorul nu este sigur care este autoritatea de supraveghere principală, atunci ar trebui, cel puțin, să notifice autoritatea locală de supraveghere unde a avut loc încălcarea.

[30] A se vedea articolul 4 alineatul (23) din RGPD.
[31] A se vedea, de asemenea, Considerentul 122 din RGPD.
[32] A se vedea Orientările WP29 pentru identificarea autorității de supraveghere principale a unui operator sau a persoanei împuternicite de operator, disponibile la http://ec.europa.eu/newsroom/document.cfm?doc id=44102
[33] O listă cu datele de contact pentru toate autoritățile naționale europene de protecție a datelor poate fi găsită la: https://edpb.europa.eu/about-edpb/about-edpb/members en

2. Încălcări comise la entități din afara UE

70. Articolul 3 din RGPD se referă la domeniul de aplicare teritorial al RGPD, inclusiv atunci când acesta se aplică prelucrării datelor cu caracter personal de către un operator sau o persoană împuternicită de operator, care nu este stabilit/ă în UE. În special, articolul 3 alineatul (2) din RGPD precizează[34]:

„Prezentul regulament se aplică prelucrării datelor cu caracter personal ale unor persoane vizate care se află în Uniune de către un operator sau o persoană împuternicită de operator care nu este stabilit(ă) în Uniune, atunci când activitățile de prelucrare sunt legate de:
(a) oferirea de bunuri sau servicii unor astfel de persoane vizate în Uniune, indiferent dacă se solicită sau nu efectuarea unei plăți de către persoana vizată; sau
(b) monitorizarea comportamentului lor dacă acesta se manifestă în cadrul Uniunii."

71. Articolul 3 alineatul (3) din RGPD este, de asemenea, relevant și prevede[35]:

„Prezentul regulament se aplică prelucrării datelor cu caracter personal de către un operator care nu este stabilit în Uniune, ci într-un loc în care dreptul intern se aplică în temeiul dreptului internațional public."

72. În cazul în care față de un operator, care nu este stabilit în UE, se aplică prevederile articolului 3 alineatul (2) sau alineatul (3) din RGPD, și acesta se confruntă cu o încălcare, trebuie să îndeplinească obligațiile de notificare prevăzute la articolele 33 și 34 din RGPD. Articolul 27 din RGPD prevede ca un operator (și o persoană împuternicită de operator) să desemneze un reprezentant în UE, unde se aplică articolul 3 alineatul (2) din RGPD.

73. Cu toate acestea, simpla prezență a unui reprezentant într-un stat membru nu creează sistemul ghișeului unic[36]. Din acest motiv, încălcarea va trebui notificată fiecărei autorități de supraveghere, dacă persoanele vizate au reședința în statul lor membru. Responsabil pentru această (aceste) notificare (notificări) va fi operatorul[37].

74. În mod similar, dacă față de o persoană împuternicită de operator se aplică prevederile articolului 3 alineatul (2) din RGPD, aceasta va fi obligată să îndeplinească obligațiile persoanelor împuternicite de operator, deosebit de relevantă în acest caz fiind obligația de a notifica operatorului o încălcare în temeiul articolului 33 alineatul (2) din RGPD.

D. Condițiile, în care notificarea nu este necesară

75. Articolul 33 alineatul (1) din RGPD precizează că încălcarea, care „ este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice", nu trebuie notificată autorității de supraveghere. Un exemplu ar putea fi cazul în care datele cu caracter personal sunt deja public accesibile și o dezvăluire a unor astfel de date nu constituie un risc posibil pentru persoana fizică. În acest caz nu se aplică cerințele existente de notificare a încălcării aplicabile prestatorilor de servicii de comunicații electronice disponibile publicului prevăzute în Directiva 2009/136/CE, conform căreia toate încălcările relevante trebuie notificate autorității competente.

[34] A se vedea Considerentele 23 și 24 din RGPD.
[35] A se vedea Considerentul 25 din RGPD.
[36] A se vedea Orientările WP29 pentru identificarea autorității de supraveghere principale a unui operator sau a persoanei împuternicite de operator, disponibile la http://ec.europa.eu/newsroom/document.cfmPdoc id=44102
[37] În conformitate cu Orientările 3/2018 privind domeniul de aplicare teritorial al RGPD (articolul 3), disponibile la adresa https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version en, CEPD consideră că funcția unui reprezentant în Uniune nu este compatibilă cu rolul unui responsabil extern cu protecția datelor („RPD"), prin urmare operatorul are responsabilitatea de a notifica autoritatea de supraveghere în cazul unei încălcări a securității datelor cu caracter personal în conformitate cu articolul 27 alineatul (5) din RGPD. Totuși un reprezentant poate fi implicat în procesul de notificare, dacă aceasta a fost indicat în mod explicit în mandatul scris.

76. În Avizul 03/2014 privind notificarea încălcării[38], WP29 a explicat că o încălcare a confidențialității datelor cu caracter personal, care au fost criptate cu un algoritm de ultimă generație, constituie o încălcare a securității datelor cu caracter personal și trebuie notificată. Totuși, dacă confidențialitatea cheii este intactă, adică cheia nu a fost compromisă prin nicio încălcare a securității și a fost generată astfel încât să nu poată fi constatată prin mijloacele tehnice disponibile de către nicio persoană, care nu este autorizată să o acceseze, atunci în principiu datele sunt neinteligibile. Astfel, este puțin probabil ca încălcarea să afecteze în mod negativ persoanele fizice și, prin urmare, nu ar trebui notificată acestor persoane[39]. Cu toate acestea, chiar și în cazul în care datele sunt criptate, o pierdere sau o modificare poate avea consecințe negative pentru persoanele vizate, în cazul în care operatorul nu are copii de rezervă adecvate. Astfel, cazul ar trebui comunicat persoanelor vizate, chiar dacă datele au fost criptare în mod corespunzător.

77. WP29 a explicat, de asemenea, că acest caz ar fi similar cazului în care datele cu caracter personal, cum ar fi parolele, ar fi indexate prin hashing și salting în siguranță, valoarea indexată prin hashing ar fi calculată cu o funcție hash cu cheie criptografică de ultimă generație, cheia utilizată pentru hashing-ul datelor nu ar fi compromisă prin orice încălcare, iar cheia folosită pentru hashing-ul datelor ar fi generată astfel, încât să nu poată fi determinată prin mijloacele tehnologice disponibile de către nicio persoană, care nu este autorizată să le acceseze.

78. Astfel, în cazul în care datele cu caracter personal au devenit în mod esențial neinteligibile pentru părți neautorizate și datele sunt o copie sau există o copie de rezervă, o încălcare a confidențialității, care implică date cu caracter personal criptate în mod corespunzător, nu trebuie să fie notificată autorității de supraveghere. Motivul se explică prin faptul că este puțin probabil ca o astfel de încălcare să prezinte un risc pentru drepturile și libertățile persoanelor. Respectiv nici persoana fizică nu ar trebui să fie informată, deoarece probabil nu există un risc ridicat. Cu toate acestea, trebuie luat în considerare faptul că, deși notificarea poate să nu fie necesară inițial dacă nu există niciun risc posibil pentru drepturile și libertățile persoanelor, lucrurile se poate schimba în timp și riscul ar trebui reevaluat. De exemplu, dacă ulterior se constată că cheia a fost compromisă sau software-ul de criptare este vulnerabil, notificarea poate fi totuși necesară.

79. De asemenea, trebuie menționat faptul că, în cazul unei încălcări în care nu există copii de rezervă ale datelor cu caracter personal criptate, aceasta va constitui o încălcare a disponibilității, care ar putea prezenta riscuri pentru persoane fizice și, prin urmare, poate fi necesară o notificare. În mod similar, dacă are loc o încălcare, care implică pierderea datelor criptate, chiar dacă există o copie de rezervă a datelor cu caracter personal, aceasta poate fi totuși o încălcare, care trebuie notificată, în dependență de durata de timp necesară pentru restabilirea datelor din copia de rezervă respectivă și de impactul lipsei disponibilității asupra persoanelor fizice. După cum prevede articolul 32 alineatul (1) litera (c) din RGPD, un factor important de securitate este *„capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică”.*

Exemplu
O încălcare, care nu trebuie notificată autorității de supraveghere, ar constitui pierderea unui dispozitiv mobil criptat în siguranță, utilizat de operator și personalul acestuia. Dacă cheia de criptare rămână în posesia securizată a operatorului și aceasta nu este singura copie a datelor cu caracter personal, datele cu caracter personal nu ar fi accesibile unui atacator. Aceasta înseamnă că încălcarea este puțin probabil să genereze un risc pentru drepturile și libertățile persoanelor vizate în cauză. Dacă mai târziu devine evident că cheia de criptare a fost compromisă sau că software-ul sau algoritmul de criptare este vulnerabil, riscul pentru drepturile și libertățile persoanelor fizice se va schimba și, prin urmare, notificarea ar putea fi necesară.

[38] WP29, Avizul 03/2014 cu privire la notificarea privind încălcarea, http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2014/wp213 en.pdf
[39] A se vedea, de asemenea, articolul 4 alineatul (1) și (2) din Regulamentul 611/2013.

80. Cu toate acestea, articolul 33 din RGPD nu este respectat atunci când un operator nu notifică autoritatea de supraveghere, dacă datele nu au fost efectiv criptate în siguranță. Prin urmare, atunci când alege software-ul de criptare, operatorul trebuie să analizeze cu atenție calitatea și efectuarea corectă a criptării oferite, să înțeleagă ce nivel de protecție de fapt oferă și dacă acesta corespunde riscurilor prezentate. Operatorii ar trebui, de asemenea, să cunoască specificul modului în care funcționează produsul lor de criptare. De exemplu, un dispozitiv poate fi criptat dacă este oprit, dar nu în timp ce este în regim de așteptare. Unele produse, care folosesc criptarea, au „chei implicite" care trebuie modificate de fiecare client pentru a fi eficiente. Criptarea poate fi considerată în prezent adecvată de către experții în domeniul securității, dar poate deveni depășită în câțiva ani, ceea ce înseamnă că este dubios faptul dacă datele ar fi criptate suficient de produsul respectiv și ar oferi un nivel de protecție corespunzător.

III. ARTICOLUL 34 – INFORMAREA PERSOANEI VIZATE

A. Informarea persoanelor fizice

81. În anumite cazuri, în afară de notificarea autorității de supraveghere, operatorul este obligat să informeze și persoanele fizice afectate de o încălcare.
Articolul 34 alineatul (1) din RGPD prevede:

„ În cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare."

82. Operatorii ar trebui să reamintească faptul că notificarea autorității de supraveghere este obligatorie, cu excepția cazului în care este puțin probabil să existe un risc pentru drepturile și libertățile persoanelor cauzat de o încălcare. De asemenea, atunci când există probabilitatea unui risc ridicat pentru drepturile și libertățile persoanelor ca urmare a unei încălcări, persoanele trebuie, de asemenea, să fie informate. Prin urmare, pragul pentru comunicarea unei încălcări persoanelor fizice este mai mare, decât pentru notificarea autorităților de supraveghere și respectiv nu toate încălcările trebuie comunicate persoanelor fizice, protejându-le astfel de oboseala inutilă cauzată de notificare.

83. RGPD prevede că persoanele fizice ar trebui informare despre o încălcare „fără întârzieri nejustificate", adică cât mai curând posibil. Obiectivul principal al notificării persoanelor este de a oferi informații concrete despre măsurile, pe care trebuie să le ia pentru a se proteja[40]. După cum este menționat mai sus, în dependență de natura încălcării și de riscul prezentat, informarea la timp va ajuta persoanele să ia măsuri pentru a se proteja de orice consecințe negative ale încălcării.

84. Anexa B la prezentele Orientări conține o listă neexhaustivă de exemple de cazuri, în care o încălcare poate genera un risc ridicat pentru persoane fizice și respectiv cazuri în care un operator va trebui să informeze persoanele afectate despre o încălcare.

B. Informațiile care trebuie comunicate

85. În cazul notificării persoanelor fizice, articolul 34 alineatul (2) din RGPD prevede următoarele:

„În informarea transmisă persoanei vizate prevăzută la alineatul (1) din prezentul articol se include o descriere într-un limbaj clar și simplu a caracterului încălcării securității datelor cu caracter personal, precum și cel puțin informațiile și măsurile menționate la articolul 33 alineatul (3) literele (b), (c) și (d)."

86. Conform acestei prevederi, operatorul ar trebui să comunice cel puțin următoarele informații:

[40] A se vedea, de asemenea, Considerentul 86 din RGPD.

- o descriere a naturii încălcării;
- numele și datele de contact ale responsabilului cu protecția datelor sau ale altei persoane de contact;
- o descriere a consecințelor probabile ale încălcării; și
- o descriere a măsurilor luate sau propuse să fie luate de către operator pentru a aborda încălcarea, inclusiv, după caz, a măsurilor de atenuare a posibilelor efecte adverse ale acesteia.

87. Ca exemplu de măsuri luate pentru a aborda încălcarea și a atenua efectele negative posibile ale acesteia, operatorul ar putea afirma că, după ce a notificat încălcarea autorității de supraveghere relevante, operatorul a primit recomandări de gestionare a încălcării și reducere a impactului acesteia. Operatorul ar trebui, de asemenea, dacă este cazul, să ofere persoanelor fizice recomandări specifice cum să se protejeze de posibilele consecințe negative ale încălcării, cum ar fi resetarea parolelor în cazul în care datele de acces ale acestora au fost compromise. Un operator poate decide să transmită informații suplimentare în afară de cele necesare în cazul respectiv.

C. Contactarea persoanelor fizice

88. În principiu, încălcarea relevantă ar trebui comunicată direct persoanelor vizate afectate, cu excepția cazului în care ar fi necesar un efort disproporționat. Într-un astfel de caz, este necesară o comunicare publică sau o măsură similară, prin care persoanele vizate să fie informate într-un mod la fel de eficient (articolul 34 alineatul (3) litera (c) din RGPD).

89. Mesajele specifice ar trebui expediate în cazul informării persoanelor vizate despre o încălcare și nu ar trebui să fie trimise cu alte informații, cum ar fi actualizări regulate, buletine informative sau mesaje standard. Astfel este facilitată comunicarea încălcării în mod clar și transparent.

90. Exemple de metode de comunicare transparente includ mesageria directă (de exemplu, e-mail, SMS, mesaj direct), bannere proeminente pe site-uri web sau notificarea, comunicarea poștală și anunțuri publicitare importante în presa scrisă. O notificare doar printr-un comunicat de presă sau blog corporativ nu ar fi un mijloc eficient de comunicare a unei încălcări unei persoane fizice. CEPD recomandă operatorilor să aleagă un mijloc, care să maximizeze șansa de a comunica corect informațiile tuturor persoanelor afectate. În dependență de circumstanțe, aceasta poate însemna că operatorul folosește mai multe metode de comunicare și nu un singur canal de contact.

91. Operatorii ar putea avea nevoie, de asemenea, să asigure accesibilitatea comunicării în formate alternative corespunzătoare și în limbi relevante, pentru ca persoanele fizice să înțeleagă informațiile care le sunt comunicate. De exemplu, pentru a informa o persoană despre o încălcare, în general poate fi folosită limba folosită în cursul normal al activității anterioare. Cu toate acestea, în cazul în care încălcarea afectează persoane vizate, cu care operatorul nu a interacționat anterior, sau în special persoane care locuiesc într-un alt stat membru sau o altă țară din afara UE unde este stabilit operatorul, comunicarea în limba națională locală ar putea fi acceptabilă, luând în considerare resursa necesară. Este important ca persoanele vizate să înțeleagă natura încălcării și măsurile, pe care le pot întreprinde pentru a se proteja.

92. Operatorii au cele mai bine posibilități pentru a determina cel mai potrivit mijloc de informare a persoanelor fizice despre o încălcare, în special dacă acestea interacționează frecvent cu clienții lor. Totuși, este evident că un operator ar trebui să fie precaut ca să nu folosească un mijloc de comunicare compromis de încălcare, deoarece ar putea fi folosit și de atacatorii care utilizează identitatea operatorului.

93. În același timp, Considerentul 86 din RGPD explică că:

„Comunicările către persoanele vizate ar trebui efectuate în cel mai scurt timp posibil în mod rezonabil și în strânsă cooperare cu autoritatea de supraveghere, respectându-se orientările furnizate de aceasta sau

de alte autorități competente, cum ar fi autoritățile de aplicare a legii. De exemplu, necesitatea de a atenua un risc imediat de producere a unui prejudiciu ar presupune comunicarea cu promptitudine către persoanele vizate, în timp ce necesitatea de a implementa măsuri corespunzătoare împotriva încălcării în continuare a securității datelor cu caracter personal sau împotriva unor încălcări similare ale securității datelor cu caracter personal ar putea justifica un termen mai îndelungat pentru comunicare. ”

94. Prin urmare, operatorii ar putea dori să contacteze autoritatea de supraveghere nu doar pentru a solicita consiliere cu privire la informarea persoanelor vizate despre o încălcare în conformitate cu articolul 34, ci și cu privire la mesajele corespunzătoare, care trebuie trimise și la cea mai potrivită modalitate de a contacta persoanele fizice.

95. Este relevantă recomandarea dată în Considerentul 88 din RGPD, conform căruia notificarea unei încălcări ar trebui „să țină cont de interesele legitime ale autorităților de aplicare a legii în cazurile în care divulgarea timpurie ar putea îngreuna în mod inutil investigarea circumstanțelor în care a avut loc o încălcare a datelor cu caracter personal”. Aceasta poate însemna că, în anumite circumstanțe, dacă este justificat și conform recomandării autorităților de aplicare a legii, operatorul poate întârzia informarea persoanelor afectate despre încălcare până la momentul în care aceasta nu ar prejudicia investigația care are loc. Totuși , persoanele vizate ar trebui să fie informate imediat după încheierea investigației.

96. Ori de câte ori nu este posibil ca operatorul să informeze o persoană despre o încălcare, deoarece nu sunt stocate date suficiente pentru a contacta persoana respectivă, în aceste circumstanțe particulare operatorul ar trebui să informeze persoana respectivă de îndată ce este posibil (de exemplu atunci când o persoană își exercită dreptul de acces la datele cu caracter personal, conform articolului 15, și oferă operatorului informații suplimentare necesare pentru a o contacta).

D. Condițiile în care comunicarea nu este necesară

97. Articolul 34 alineatul (3) din RGPD prevede trei condiții în care, dacă sunt îndeplinite, persoanele fizice nu trebuie informate despre o încălcare. Acestea sunt:

- Operatorul a implementat măsuri tehnice și organizatorice adecvate pentru a proteja datele cu caracter personal înainte de încălcare, în special măsuri care fac datele personale neinteligibile pentru orice persoană, care nu este autorizată să le acceseze. Aceasta ar putea include, de exemplu, protejarea datelor cu caracter personal prin criptare de ultimă generație sau prin tokenizare.
- Imediat după producerea unei încălcări, operatorul a luat măsuri pentru ca riscul ridicat pentru drepturile și libertățile persoanelor să nu se materializeze. De exemplu, în dependență de circumstanțele cazului, operatorul poate să fi identificat imediat și să fi luat măsuri împotriva persoanei care a accesat datele cu caracter personal înainte de a putea face ceva cu acestea. De asemenea, trebuie acordată atenție cuvenită posibilelor consecințe ale oricărei încălcări a confidențialității, iarăși în dependență de tipul datelor în cauză.
- Ar fi necesar un efort disproporționat[41] de a contacta persoane fizice, posibil în cazul în care datele de contact au fost pierdute ca urmare a încălcării sau nu sunt cunoscute în primul rând. De exemplu, depozitul unui birou de statistică a fost inundat, iar documentele care conțin date cu caracter personal erau stocate doar pe suport de hârtie. Operatorul trebuie să facă o comunicare publică sau să ia o măsură similară, prin care persoanele fizice să fie informate într-un mod la fel de eficient. În cazul unui efort disproporționat, ar putea fi luate în considerare și aranjamente tehnice pentru a transmite la solicitare informații despre încălcare, care ar putea fi utile acestor persoane posibil afectate de încălcare, dacă operatorul nu le poate contacta în alt mod.

[41] A se vedea Orientările WP29 privind transparența, care vor aborda subiectul efortului disproporționat, disponibile la adresa http://ec.europa.eu/newsroom/just/document.cfm?doc id=48850

98. În conformitate cu principiul răspunderii, operatorii ar trebui să poată demonstra autorității de supraveghere că îndeplinesc una sau mai multe dintre aceste condiții[42]. Trebuie avut în vedere faptul că, deși notificarea poate să nu fie necesară inițial, dacă nu există niciun risc pentru drepturile și libertățile persoanelor fizice, lucrurile se pot schimba în timp și riscul ar trebui reevaluat.

99. În cazul în care un operator decide să nu informeze persoana despre o încălcare, articolul 34 alineatul (4) din RGPD explică că autoritatea de supraveghere îi poate solicita să o informeze, dacă consideră că încălcarea ar putea genera un risc ridicat pentru persoane. Alternativ, ar putea considera că au fost îndeplinite condițiile prevăzute la articolul 34 alineatul (3) din RGPD și nu este necesară informarea persoanelor fizice. În cazul în care autoritatea de supraveghere stabilește că decizia de a nu notifica persoanele vizate nu este întemeiată, aceasta ar putea aplica competențele disponibile și sancțiunile prevăzute.

IV. EVALUAREA RISCULUI ȘI A RISCULUI RIDICAT

A. Riscul ca declanșator al notificării

100. Deși RGPD introduce obligația de a notifica o încălcare, această cerință de notificare nu se aplică în toate circumstanțele:

- Notificarea autorității de supraveghere competente este necesară, cu excepția cazului în care este puțin probabil ca o încălcare să genereze un risc pentru drepturile și libertățile persoanelor.
- Informarea unei persoane fizice despre încălcare este necesară doar atunci, când este probabil să genereze un risc ridicat pentru drepturile și libertățile sale.

101. Aceasta înseamnă că imediat după ce a luat cunoștință de o încălcare, este foarte important ca operatorul nu doar să încerce să limiteze incidentul, ci și să evalueze și riscul care ar putea apărea. Există două motive importante: în primul rând, cunoașterea probabilității și a gravității posibile a impactului asupra persoanei fizice va ajuta operatorul să ia măsuri eficiente pentru a limita și a soluționa încălcarea; în al doilea rând, îl va ajuta să stabilească dacă autoritatea de supraveghere și persoanele fizice în cauză trebuie informate.

102. După cum s-a explicat mai sus, notificarea unei încălcări este necesară, cu excepția cazului în care este puțin probabil să genereze un risc pentru drepturile și libertățile persoanelor, iar factorul-cheie, în cazul căruia trebuie informate persoanele vizate, există atunci când este probabil să apară un risc *ridicat* pentru drepturile și libertățile persoanelor. Acest risc există atunci când încălcarea poate cauza prejudicii fizice, materiale sau morale pentru persoanele, securitatea datelor cărora a fost încălcată. Exemple de astfel de prejudicii sunt discriminarea, furtul de identitate sau frauda, pierderea financiară și deteriorarea imaginii. Atunci când încălcarea implică date cu caracter personal, care dezvăluie originea rasială sau etnică, opinia politică, religia sau convingeri filozofice sau apartenența la un sindicat sau include date genetice, date privind sănătatea sau date privind viața sexuală sau antecedente penale și infracțiuni sau măsuri de securitate aferente, producerea unui astfel de prejudiciu ar trebui considerată ca fiind posibilă[43].

[42] A se vedea articolul 5 alineatul (2) din RGPD.
[43] A se vedea Considerentul 75 și Considerentul 85 din RGPD.

B. Factorii, care trebuie luați în considerare la evaluarea riscului

103. Considerentele 75 și 76 din RGPD sugerează că, în general, atunci când se evaluează riscul, ar trebui să se ia în considerare atât probabilitatea, cât și gravitatea riscului pentru drepturile și libertățile persoanelor vizate. De asemenea, se precizează că riscul ar trebui evaluat pe baza unei evaluări obiective.

104. Trebuie menționat faptul că evaluarea riscului pentru drepturile și libertățile persoanelor ca urmare a unei încălcări are un accent diferit față de o EIPD în care se evaluează riscul[44]. EIPD ia în considerare atât riscurile prelucrării planificate a datelor, cât și riscurile unei încălcări. Atunci când este examinată o încălcare posibilă, se analizează, în termeni generali, probabilitatea comiterii acesteia și prejudiciul care ar putea afecta persoana vizată; cu alte cuvinte, este o evaluare a unui eveniment ipotetic. În cazul unei încălcări reale, evenimentul a avut deja loc și, prin urmare, accentul se pune integral pe riscul generat de impactul încălcării asupra persoanelor fizice.

Exemplu
O EIPD sugerează că utilizarea propusă a unui anumit produs software de securitate pentru a proteja datele cu caracter personal este o măsură adecvată pentru asigurarea unui nivel de securitate corespunzător riscului, pe care l-ar prezenta prelucrarea pentru persoanele fizice în alt mod. Cu toate acestea, dacă o vulnerabilitate devine ulterior cunoscută, aceasta ar schimba gradul de potrivire a software-ului pentru limitarea riscului pentru datele cu caracter personal protejate și, prin urmare, ar trebui reevaluat în cadrul unei EIPD în curs de desfășurare. Ulterior cineva profită de vulnerabilitatea produsului și comite o încălcare. Operatorul ar trebui să evalueze circumstanțele încălcării, datele afectate și nivelul potențial al impactului asupra persoanelor, precum și cât de probabil se va materializa acest risc.

105. Astfel, în cazul evaluării riscului pentru persoane fizice ca urmare a unei încălcări, operatorul ar trebui să ia în considerare circumstanțele specifice ale încălcării, inclusiv gravitatea impactului potențial și probabilitatea ca acesta să se producă. Prin urmare, CEPD recomandă ca în timpul evaluării să ia în considerare următoarele criterii[45]:

- **Tipul încălcării**

106. Tipul încălcării, care a avut loc, poate influența asupra nivelului riscului pentru persoanele fizice. De exemplu, o încălcare a confidențialității, prin care informațiile medicale au fost dezvăluite unor părți neautorizate, poate avea diferite consecințe pentru o persoană fizică afectată de încălcare, din cauza căreia datele sale medicale au fost pierdute și nu mai sunt disponibile.

- **Natura, sensibilitatea și volumul datelor cu caracter personal**

107. Desigur, atunci când se evaluează riscul, un factor cheie este tipul și sensibilitatea datelor cu caracter personal, care au fost compromise de încălcare. De obicei, cu cât datele sunt mai sensibile, cu atât riscul de prejudiciere va fi mai mare pentru persoanele afectate, dar ar trebui luate în considerare și alte date cu caracter personal ale persoanei vizate, care pot fi deja disponibile. De exemplu, dezvăluirea numelui și adresei unei persoane în circumstanțe obișnuite este puțin probabil să cauzeze prejudicii substanțiale. Cu toate acestea, dacă numele și adresa unui părinte adoptiv sunt dezvăluite unui părinte biologic, consecințele ar putea fi foarte grave atât pentru părintele adoptiv, cât și pentru copil.

108. Încălcările, care implică date de sănătate, acte de identitate sau date financiare, cum ar fi datele cărții de credit, pot provoca prejudicii singure, dar dacă sunt utilizate împreună, ar putea fi folosite pentru furtul

[44] A se vedea Orientările WP privind EIPD-urile aici: http://ec.europa.eu/newsroom/document.cfmPdoc id=44137
[45] Articolul 3.2 din Regulamentul 611/2013 oferă îndrumări factorilor, care ar trebui luați în considerare în legătură cu notificarea încălcărilor în sectorul serviciilor comunicațiilor electronice, care pot fi utile în contextul notificării conform RGPD. A se vedea http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF

de identitate. O combinație de date cu caracter personal, de obicei, este mai sensibilă, decât o parte a acestora.

109. Unele tipuri de date cu caracter personal pot părea la început relativ inofensive, însă ceea ce ar putea dezvălui aceste date despre persoana afectată ar trebui luat în considerare cu atenție. O listă de clienți, care acceptă livrări regulate, poate să nu fie deosebit de sensibilă, dar aceleași date despre clienții care au solicitat suspendarea livrărilor lor pe perioada vacanței ar fi informații utile pentru infractori.

110. În mod similar, un volum nesemnificativ de date cu caracter personal extrem de sensibile poate avea un impact mare asupra unei persoane, iar o gamă largă de date poate dezvălui o gamă mai mare de informații despre persoana respectivă. De asemenea, o încălcare care afectează volume mari de date cu caracter personal despre multe persoane vizate poate afecta un număr corespunzător de mare de persoane.

- **Ușurința identificării persoanelor**

111. Un factor important care trebuie luat în considerare este cât de ușor va fi unei părți, care are acces la date cu caracter personal compromise, să identifice anumite persoane sau să potrivească datele cu alte informații pentru a identifica persoane. În dependență de circumstanțe, identificarea ar putea fi posibilă direct din datele cu caracter personal, securitatea cărora a fost încălcată, fără nicio cercetare specială necesară pentru a descoperi identitatea persoanei, sau poate fi extrem de dificil de potrivit datele cu caracter personal cu o anumită persoană, dar totuși posibil în anumite condiții. Identificarea poate fi direct sau indirect posibilă din datele, securitatea cărora a fost încălcată, dar poate depinde și de contextul specific al încălcării și de disponibilitatea publică a detaliilor personale aferente. Acest lucru poate fi mai relevant pentru încălcările de confidențialitate și disponibilitate.

112. După cum este menționat mai sus, datele cu caracter personal protejate de un nivel de criptare corespunzător vor fi neinteligibile pentru persoanele neautorizate fără cheia de decriptare. De asemenea, pseudonimizarea efectuată în mod corespunzător (definită la articolul 4 alineatul (5) din RGPD ca *„prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile”*) poate reduce probabilitatea ca persoanele fizice să fie identificate în cazul unei încălcări. Cu toate acestea, nu se poate considera că tehnicile de pseudonimizare singure pot face datele neinteligibile.

- **Gravitatea consecințelor pentru persoane fizice**

113. În dependență de tipul datelor cu caracter personal implicate într-o încălcare, de exemplu, categorii speciale de date, prejudiciul potențial asupra persoanelor fizice poate fi deosebit de grav, în special atunci când încălcarea ar putea duce la furt de identitate sau fraudă, vătămare corporală, suferință psihologică, umilire sau deteriorare a imaginii. Dacă încălcarea se referă la date cu caracter personal despre persoane vulnerabile, acestea ar putea fi expuse unui risc mai mare de vătămare.

114. Dacă operatorul este conștient de faptul că datele cu caracter personal sunt în mâinile unor persoane, ale căror intenții sunt necunoscute sau posibil rău intenționate, acest fapt poate influența asupra nivelului de risc potențial. Poate exista o încălcare a confidențialității, prin care datele cu caracter personal sunt dezvăluite unei părți terțe, care este definită la articolul 4 alineatul (10), sau altui destinatar din greșeală. Aceasta se poate întâmpla, de exemplu, atunci când datele cu caracter personal sunt expediate accidental unui departament greșit al unei organizații sau unui prestator contractat în mod obișnuit. Operatorul poate solicita destinatarului fie să returneze, fie să distrugă în siguranță datele pe care le-a primit. În

ambele cazuri, având în vedere că operatorul are o relație continuă cu destinatarul și poate fi la curent cu procedurile, istoricul și alte detalii relevante ale acestuia, destinatarul poate fi considerat „fiabil”. Cu alte cuvinte, operatorul poate avea un nivel de asigurare față de destinatar, astfel încât să se poată aștepta în mod rezonabil că partea respectivă nu va citi sau accesa datele trimise din eroare și va respecta indicațiile sale de a le returna. Chiar dacă datele au fost accesate, operatorul ar putea avea încredere în destinatar că nu va face nimic cu ele și că le va returna operatorului imediat și va coopera pentru a le recupera. În astfel de cazuri, acest lucru poate fi luat în considerare în procesul de evaluare a riscurilor efectuată de operator în urma încălcării – faptul că destinatarul este de încredere poate reduce gravitatea consecințelor încălcării, dar nu înseamnă că nu a avut loc o încălcare. Totuși, aceasta la rândul său poate elimina probabilitatea apariției unui risc pentru persoane, nemaifiind astfel necesară notificarea autorității de supraveghere sau a persoanelor afectate. Totul depinde de caz. Cu toate acestea, operatorul trebuie să păstreze informațiile privind încălcarea ca parte a obligației generale de a păstra evidența încălcărilor (a se vedea secțiunea V, mai jos).

115. Ar trebui să se ia în considerare, de asemenea, permanența consecințelor pentru persoanele fizice, în cazul în care impactul poate fi considerat mai mare dacă efectele sunt pe termen lung.

- **Caracteristicile speciale ale persoanei fizice**

116. O încălcare poate afecta datele cu caracter personal referitoare la copii sau alte persoane vulnerabile, care pot fi expuse unui risc mai mare de pericol. Pot exista și alți factori despre persoana fizică, care pot afecta nivelul impactului încălcării asupra acestora.

- **Caracteristicile speciale ale operatorului de date**

117. Tipul și rolul operatorului și activităților acestuia pot afecta nivelul de risc pentru persoane generat de o încălcare. De exemplu, o instituție medicală va procesa categorii speciale de date cu caracter personal, ceea ce înseamnă că există o amenințare mai mare pentru persoane, dacă securitatea datelor lor cu caracter personal va fi încălcată, în comparație cu o listă de corespondență a unui ziar.

- **Numărul de persoane afectate**

118. O încălcare poate afecta doar una sau câteva persoane sau câteva mii, dacă nu mai multe. În general, cu cât mai mare este numărul de persoane afectate, cu atât mai mare poate fi impactul unei încălcări. Cu toate acestea, o încălcare poate avea un impact grav chiar și asupra unei persoane, în dependență de tipul datelor cu caracter personal și de contextul în care acestea au fost compromise. Din nou, este important să luăm în considerare probabilitatea și gravitatea impactului asupra persoanelor afectate.

- **Aspecte generale**

119. Prin urmare, atunci când evaluează riscul care ar putea fi generat de o încălcare, operatorul ar trebui să ia în considerare gravitatea impactului potențial asupra drepturilor și libertăților persoanelor și probabilitatea apariției acestuia. În mod clar, dacă consecințele unei încălcări sunt mai grave, riscul este mai mare și dacă probabilitatea comiterii încălcării este mai mare, riscul, de asemenea, este mai mare. Dacă aveți îndoieli, operatorul ar trebui să fie mai precaut și să notifice. În Anexa B sunt prezentate câteva exemple utile de diferite tipuri de încălcări, care implică riscuri sau riscuri ridicate pentru persoane fizice.

120. Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) a elaborat recomandări pentru o metodologie de evaluare a gravității unei încălcări, pe care operatorii și persoanele împuternicite de

operatori le pot considera utile atunci când își elaborează planul de răspuns pentru gestionarea încălcării.[46]

V. RESPONSABILITATEA ȘI PĂSTRAREA EVIDENȚELOR

A. Documentarea încălcărilor

121. Indiferent dacă o încălcare trebuie sau nu notificată autorității de supraveghere, operatorul trebuie să păstreze documentația cu privire la toate încălcările, după cum este explicat în articolul 33 alineatul (5) din RGPD:
„Operatorul păstrează documente referitoare la toate cazurile de încălcare a securității datelor cu caracter personal, care cuprind o descriere a situației de fapt în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor acesteia și a măsurilor de remediere întreprinse. Această documentație permite autorității de supraveghere să verifice conformitatea cu prezentul articol."

122. Acest lucru este legat de principiul răspunderii prevăzut la articolul 5 alineatul (2) din RGPD. Scopul înregistrării încălcărilor, care nu trebuie notificate, precum și a încălcărilor notificabile, se referă și la obligațiile operatorului în temeiul articolului 24 din RGPD, iar autoritatea de supraveghere poate solicita să vadă aceste înregistrări. Astfel, operatorii sunt încurajați să aibă un registru intern al încălcărilor, indiferent dacă sunt obligați să notifice sau nu[47].

123. Deși operatorul trebuie să determine ce metodă și ce structură să folosească atunci când documentează o încălcare, în ceea ce privește informațiile care pot fi înregistrate, există elemente cheie care ar trebui incluse în toate cazurile. După cum prevede articolul 33 alineatul (5) din RGPD, operatorul trebuie să înregistreze detalii privind încălcarea, care ar trebui să includă cauzele acesteia, ce a avut loc și datele cu caracter personal afectate. Ar trebui să includă, de asemenea, efectele și consecințele încălcării, precum și măsurile de remediere luate de operator.

124. RGPD nu specifică o perioadă de păstrare a unei astfel de documentații. În cazul în care astfel de înregistrări conțin date cu caracter personal, operatorul va avea sarcina de a determina perioada corespunzătoare de păstrare în conformitate cu principiile referitoare la prelucrarea datelor cu caracter personal[48] și de a îndeplini cerințele unei baze legale privind prelucrarea[49]. Va trebui să păstreze documentația în conformitate cu articolul 33 alineatul (5) din RGPD, în măsura în care poate fi solicitat să prezinte autorității de supraveghere dovezi de conformitate cu articolul respectiv sau, în general, cu principiul răspunderii. În mod clar, dacă înregistrările în sine nu conțin date cu caracter personal, atunci principiul limitării păstrării[50] prevăzut de RGPD nu se aplică.

125. Pe lângă aceasta, CEPD recomandă operatorului să își documenteze, de asemenea, motivele deciziilor luate ca răspuns la o încălcare. În special, dacă o încălcare nu este notificată, ar trebui documentată justificarea acestei decizii. Aceasta ar trebui să includă motivele pentru care operatorul consideră că încălcarea este puțin probabil să genereze un risc pentru drepturile și libertățile persoanelor[51]. În mod alternativ, dacă operatorul consideră că orice condiție prevăzută la articolul 34 alineatul (3) din RGPD este îndeplinită, ar trebui să poată prezenta dovezi corespunzătoare.

---

[46] ENISA, Recomandări pentru o metodologie de evaluare a gravității încălcărilor datelor cu caracter personal, https://www.enisa.europa.eu/publications/dbn-severity

[47] Operatorul poate decide să documenteze încălcările ca parte a evidenței sale privind activitățile de prelucrare, care este menținută în conformitate cu articolul 30 din RGPD. Nu este necesar un registru separat, cu condiția ca informațiile relevante încălcării să fie clar identificabile ca atare și să poată fi extrase la solicitare..

[48] A se vedea articolul 5 din RGPD.

[49] A se vedea articolul 6 și, de asemenea, articolul 9 din RGPD

[50] A se vedea articolul 5 alineatul (1) litera (e) din RGPD.

[51] A se vedea Considerentul 85 din RGPD.

126. În cazul în care operatorul notifică o încălcare autorității de supraveghere, dar cu întârziere, operatorul trebuie să poată prezenta motivele acestei întârzieri; documentația aferentă ar putea demonstra faptul că întârzierea notificării este justificată și nu excesivă.

127. În cazul în care operatorul informează despre o încălcare persoanele afectate, ar trebui să fie transparent cu privire la încălcare și să informeze despre aceasta într-un mod eficient și în timp util. Astfel, păstrând dovezile unei astfel de informări, operatorul ar putea demonstra mai ușor responsabilitatea și conformitatea sa.

128. Pentru a facilita conformitatea cu articolele 33 și 34 din RGPD, ar fi avantajos atât pentru operatori, cât și pentru persoanele împuternicite de operatori să aibă în vigoare o procedură de notificare documentată, care să stabilească procesul care trebuie efectuat în cazul depistării unei încălcări, inclusiv modul de limitare, gestionare și recuperare a incidentului, precum și procedura de evaluare a riscului și de notificare a încălcării. În acest sens, pentru a demonstra conformitatea cu RGPD ar putea fi, de asemenea, util să se demonstreze că angajații au fost informați despre existența unor astfel de proceduri și mecanisme și că știu cum să reacționeze la încălcări.

129. Trebuie remarcat faptul că în cazul nedocumentării în mod corespunzător a unei încălcări, autoritatea de supraveghere ar putea să își exercite competențele în temeiul articolului 58 din RGPD și/sau să aplice o amendă administrativă în conformitate cu articolul 83 din RGPD.

B. Rolul responsabilului cu protecția datelor

130. Ca o bună practică, un operator sau o persoană împuternicită de operator poate avea un responsabil cu protecția datelor (RPD)[52], fie în conformitate cu articolul 37 din RGPD, fie în mod voluntar. Articolul 39 din RGPD prevede o serie de sarcini obligatorii pentru RPD, dar nu împiedică alocarea sarcinilor suplimentare de către operator, în caz de necesitate.

131. Deosebit de relevant pentru notificarea încălcării este faptul, că sarcinile obligatorii ale RPD includ, printre altele, acordarea consilierii și informațiilor privind protecția datelor operatorului sau persoanei împuternicite de operator, monitorizarea conformității cu RGPD și consilierea în legătură cu EIPD. De asemenea, RPD trebuie să coopereze cu autoritatea de supraveghere și să acționeze ca persoană de contact pentru autoritatea de supraveghere și persoanele vizate. De asemenea, trebuie remarcat faptul că, în cazul notificării unei încălcări autorității de supraveghere, conform articolului 33 alineatul (3) litera (b) din RGPD operatorul trebuie să indice numele și datele de contact ale RPD sau altei persoane de contact.

132. În ceea ce privește documentarea încălcărilor, operatorul sau persoana împuternicită de operator ar putea dori să obțină avizul RPD-ului său cu privire la structura, crearea și administrarea acestei documentații. RPD ar putea avea, de asemenea, sarcina de a menține astfel de înregistrări.

133. Acești factori înseamnă că RPD ar trebui să joace un rol cheie în sprijinirea prevenirii sau pregătirii pentru o încălcare acordând consiliere și monitorizând conformitatea, precum și în timpul unei încălcări (adică în cazul notificării autorității de supraveghere) și în procesul oricărei investigații ulterioare a autorității de supraveghere. În acest context, CEPD recomandă ca RPD să fie informat imediat cu privire la existența unei încălcări și să fie implicat pe tot parcursul procesului de gestionare și notificare a încălcării.

[52] A se vedea Orientările WP privind RPD-urile aici: http://ec.europa.eu/newsroom/just/item-detail.cfmPitem id=50083

VI. OBLIGAȚII DE NOTIFICARE ÎN TEMEIUL ALTOR ACTE LEGALE

134. În afară și separat de notificarea și informarea despre încălcări în temeiul RGPD, operatorii ar trebui, de asemenea, să cunoască orice cerință de a notifica incidentele de securitate în temeiul altei legislații conexe, care li se poate aplica și dacă conform acesteia ar fi obligați să notifice, în același timp, autoritatea de supraveghere despre o încălcare a securității datelor cu caracter personal. Astfel de cerințe pot varia de la un stat membru la altul, dar exemplele de cerințe de notificare prevăzute în alte acte legale și modul în care acestea interacționează cu RGPD includ următoarele:

- *Regulamentul (UE) 910/2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă (Regulamentul eIDAS)*[53].

135. Articolul 19 alineatul (2) din Regulamentul eIDAS obligă prestatorii de servicii de încredere să își notifice organul de supraveghere cu privire la o încălcare a securității sau o pierdere a integrității, care are un impact semnificativ asupra serviciului de încredere prestat sau asupra datelor cu caracter personal păstrate la aceștia. Dacă este cazul, adică atunci când o astfel de încălcare sau pierdere constituie și o încălcare a securității datelor cu caracter personal în conformitate cu RGPD, prestatorul de servicii de încredere ar trebui să notifice și autoritatea de supraveghere.

- *Directiva (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (Directiva NIS)*[54].

136. Articolele 14 și 16 din Directiva NIS obligă operatorii de servicii esențiale și prestatorii serviciilor digitale să notifice incidentele de securitate autorității lor competente. După cum se recunoaște în Considerentul 63 din NIS[55], incidentele de securitate pot deseori include compromiterea datelor cu caracter personal. În timp ce NIS obligă autoritățile competente și autoritățile de supraveghere să coopereze și să facă schimb de informații în acest context, dacă astfel de incidente sunt sau devin încălcări ale securității datelor cu caracter personal în temeiul RGPD, acești operatori și/sau prestatori ar fi obligați să notifice autoritatea de supraveghere separat de cerințele de notificare a incidentelor prevăzute de NIS.

Exemplu
Un prestator de servicii cloud, care notifică o încălcare în temeiul Directivei NIS, ar trebui, de asemenea, să notifice un operator, dacă aceasta include o încălcare a securității datelor cu caracter personal. În mod similar, în cazul unei încălcări un prestator de servicii de încredere care notifică în temeiul eIDAS poate fi obligat, de asemenea, să notifice autoritatea relevantă de protecție a datelor.

- *Directiva 2009/136/CE (Directiva privind drepturile cetățenilor) și Regulamentul 611/2013 (Regulamentul privind notificarea încălcării).*

137. Prestatorii de servicii de comunicații electronice accesibile publicului în contextul Directivei 2002/58/CE[56] trebuie să notifice încălcările autorităților naționale competente.

138. Operatorii ar trebui să cunoască, de asemenea, orice obligații de notificare suplimentară legale, medicale sau profesionale în cadrul altor regimuri aplicabile.

---

[53] A se vedea http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

[54] A se vedea http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

[55] Considerentul 63: *„Datele cu caracter personal în multe cazuri sunt compromise ca urmare a unor incidente. În acest context, autoritățile competente și autoritățile de protecție a datelor ar trebui să coopereze și să facă schimb de informații cu privire la toate chestiunile relevante pentru a aborda orice încălcare a securității datelor cu caracter personal care rezultă din incidente."*

[56] La 10 ianuarie 2017, Comisia Europeană a propus un Regulament privind confidențialitatea și comunicațiile electronice care va înlocui Directiva 2009/136/CE și va elimina cerințele de notificare. Cu toate acestea, până la aprobarea acestei propuneri de către Parlamentul European, cerința de notificare existentă rămâne în vigoare, a se vedea https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electroniccommunications

VII. ANEXĂ

A. Diagrama care prezintă cerințele de notificare

<table>
<tr><td>Operatorul depistează/este informat despre un incident de securitate și stabilește dacă a avut loc o încălcare a securității datelor cu caracter personal.</td><td></td><td>Operatorul „a luat cunoștință” de o încălcare a securității datelor cu caracter personal și evaluează riscul pentru persoane fizice.</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Încălcarea poate genera un risc pentru drepturile ? și libertățile persoanelor fizice ?</td><td>Nu</td><td>Nu sunt cerințe de notificare a autorității de supraveghere sau a persoanelor fizice.</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Da</td><td></td><td rowspan="2">Notificați autoritatea de supraveghere competentă.

În cazul în care încălcarea afectează persoane fizice din mai multe state membre, iar operatorul are sediu în SEE, notificați autoritatea principală de supraveghere.

Dacă încălcarea afectează persoane fizice din mai multe state membre, iar operatorul nu are sedii în SEE, dar față de acesta se aplică RGPD în temeiul articolului 3 alineatul (2), notificați fiecare autoritate de supraveghere din statul membru, în care își au reședința persoanele vizate.</td></tr>
<tr><td>Încălcarea poate genera un risc ridicat pentru drepturile ? și libertățile persoanelor fizice ?</td><td></td></tr>
<tr><td>Da Nu</td><td></td><td>Nu sunt cerințe de notificare a persoanelor fizice.</td></tr>
<tr><td></td><td>Notificați persoanele afectate și, dacă este necesar, transmiteți informații pe etape despre măsurile pe care le pot lua pentru a se proteja de consecințele încălcării.</td><td></td></tr>
<tr><td></td><td>Toate încălcările care pot fi înregistrate în temeiul articolului 33 alineatul (5). Încălcarea ar trebui să fie documentată și înregistrată de operator.</td><td></td></tr>
</table>

B. Exemple de încălcări ale securității datelor cu caracter personal și cine trebuie notificat

Următoarele exemple neexhaustive vor ajuta operatorii să determine, dacă trebuie să notifice în diferite scenarii de încălcare a securității datelor cu caracter personal. Aceste exemple pot ajuta, de asemenea, la diferențierea între risc și riscul ridicat pentru drepturile și libertățile persoanelor fizice.

Exemplu	Notificați autoritatea de supraveghere	Notificați persoana vizată	Note/recomandări
Un operator a stocat o copie de rezervă a unei arhive de date personale criptate pe o cheie USB. Cheia a fost furată în timpul unei spargeri.	Nu.	Nu.	Atât timp cât datele sunt criptate cu un algoritm de ultimă generație, există copii de rezervă ale datelor, cheia unică nu este compromisă și datele pot fi restabilite în timp util, aceasta poate să nu fie o încălcare care trebuie notificată. Cu toate acestea, dacă ulterior datele sunt compromise, încălcarea trebuie notificată.
Un operator menține un serviciu online. Ca urmare a unui atac cibernetic asupra serviciului respectiv, datele cu caracter personal ale persoanelor fizice sunt exfiltrate. Operatorul are clienți într-un singur stat membru.	Da, notificați autorității de supraveghere dacă există incidentul ar putea avea consecințe asupra persoanelor fizice.	Da, informați persoanele fizice în dependență de tipul datelor cu caracter personal afectate și dacă gravitatea consecințelor probabile pentru persoanele fizice este mare.	
Are loc scurtă întrerupere a curentului, care durează câteva minute la centrul de apeluri al unui operator, din cauza căreia clienții nu pot suna operatorul și accesa înregistrările lor.	Nu.	Nu.	Aceasta nu este o încălcare, care poate fi notificată, dar totuși este un incident care poate fi înregistrat în conformitate cu articolul 33 alineatul (5). Operatorul trebuie să păstreze înregistrări corespunzătoare.
Un operator este victima unui atac ransomware, care are ca rezultat criptarea tuturor datelor. Copii de rezervă nu sunt și datele nu pot fi restabilite. În urma	Da, notificați incidentul autorității de supraveghere, dacă ar putea există consecințe asupra persoanelor fizice, deoarece constituie o	Da, informați persoanele fizice în dependență de tipul datelor cu caracter personal afectate și de impactul posibil al	Dacă ar exista o copie de rezervă disponibilă și datele ar putea fi restabilite în timp util, acest caz nu ar trebui să fie notificat autorității de supraveghere sau persoanelor fizice, deoarece

investigației, devine clar că singura funcționalitate a ransomware-ului a fost criptarea datelor și că în sistem nu exista un alt malware.	pierdere a disponibilității.	lipsei de disponibilitate a datelor, precum și de alte consecințe posibile.	nu ar exista o pierdere permanentă a disponibilității sau confidențialității. Cu toate acestea, dacă autoritatea de supraveghere a luat cunoștință de incident prin alte mijloace, aceasta poate efectua o investigație pentru a evalua conformitatea cu cerințele mai ample de securitate prevăzute la articolul 32.
O persoană sună la centrul de apeluri al unei bănci pentru a informa despre o încălcare a securității datelor. Persoana a primit un extras lunar pentru altcineva. Operatorul efectuează o scurtă investigație (adică timp de 24 de ore) și stabilește cu o încredere rezonabilă că a avut loc o încălcare a securității datelor cu caracter personal și dacă are o defecțiune sistemică care poate însemna că alte persoane sunt sau ar putea fi afectate.	Da.	Doar persoanele afectate sunt anunțate dacă există risc ridicat și este clar că altele nu sunt afectate.	În cazul în care, în urma investigației ulterioare, se constată că sunt afectate mai multe persoane, autorității de supraveghere trebuie să-i fie transmise informații actuale, iar operatorul notifică suplimentar alte persoane fizice dacă există un risc ridicat pentru acestea.
Un operator operează un marketplace online și are clienți în mai multe state membre. Marketplace-ul este ținta unui atac cibernetic, în urma căruia atacatorul publică online numele de utilizator, parolele și istoricul achizițiilor.	Da, informați autoritatea principală de supraveghere dacă implică procesarea transfrontalieră.	Da, deoarece ar putea genera un risc ridicat.	Operatorul ar trebui să ia măsuri, de exemplu prin forțarea resetărilor parolelor conturilor afectate, precum și alte măsuri pentru atenuarea riscului. Operatorul ar trebui să ia în considerare și orice alte obligații de notificare, de exemplu conform Directivei NIS ca prestator de servicii digitale.
O companie de găzduire a site-urilor web, care acționează ca persoană împuternicită de operator, identifică o	În calitate de persoană împuternicită de operator, compania de găzduire a site-ului	Dacă este probabil că nu există riscuri ridicate pentru persoane fizice,	Compania de găzduire a site-urilor web (persoana împuternicită de operator) trebuie să ia în considerare orice alte obligații de

eroare în codul care controlează autorizarea utilizatorului. Efectul erorii înseamnă că orice utilizator poate accesa datele contului oricărui alt utilizator	web trebuie să își notifice clienții afectați (operatorii) fără întârzieri nejustificate. Presupunând că compania de găzduire a site-ului web a efectuat propria investigație, operatorii afectați ar trebui să aibă încredere în mod rezonabil în faptul dacă fiecare a suferit de încălcare și, prin urmare, este probabil să fie considerat că „au luat cunoștință” odată ce au fost notificați de către compania de găzduire (persoana împuternicită de operator). Apoi operatorul trebuie să notifice autoritatea de supraveghere.	acestea nu trebuie să fie notificate.	notificare (de exemplu, în conformitate cu Directiva NIS ca prestator de servicii digitale). Dacă nu există dovezi că de această vulnerabilitate a profitat oricare dintre operatorii săi, este posibil să nu fi avut loc o încălcare notificabilă, dar este posibil să poată fi înregistrată sau să constituie un caz de nerespectare în temeiul articolului 32.
Fișele medicale de la un spital nu sunt accesibile timp de 30 de ore din cauza unui atac cibernetic.	Da, spitalul este obligat să informeze că poate apărea un risc ridicat pentru bunăstarea și confidențialitatea datelor pacientului.	Da, informați persoanele fizice afectate.	
Datele cu caracter personal ale unui număr mare de studenți sunt trimise din greșeală către o listă de corespondență greșită cu peste 1000 de destinatari.	Da, notificați cazul autorității de supraveghere.	Da, informați persoanele fizice în dependență de domeniul și tipul datelor cu caracter personal afectate și de gravitatea posibilelor consecințe.	
Un e-mail de marketing direct este trimis destinatarilor în câmpurile „către:” sau „cc:”, fapt prin care	Da, notificarea autorității de supraveghere poate fi obligatorie, dacă un număr mare de	Da, informați persoanele fizice în dependență de domeniul și tipul datelor cu caracter	Este posibil ca notificarea să nu fie necesară, dacă nu sunt dezvăluite date sensibile și dacă este dezvăluit doar un

fiecare destinatar poate vedea adresa de e-mail a altor destinatari.	persoane fizice sunt afectate, dacă sunt dezvăluite date sensibile (de exemplu, o listă de corespondență a unui psihoterapeut) sau dacă alți factori prezintă riscuri mari (de exemplu, e-mailul conține parolele inițiale).	personal implicate și de gravitatea posibilelor consecințe.	număr mic de adrese de e-mail.