GRUPUL DE LUCRU „ARTICOLUL 29” PENTRU PROTECȚIA DATELOR

18/RO

WP250rev.01

Orientări privind notificarea încălcării securității datelor cu caracter personal în temeiul Regulamentului 2016/679

Adoptate la 3 octombrie 2017

Astfel cum au fost cel mai recent revizuite și adoptate la 6 februarie 2018

Acest grup de lucru a fost creat în temeiul articolului 29 din Directiva 95/46/CE. Grupul este un organism consultativ european independent care se ocupă cu protecția datelor și a vieții private. Sarcinile sale sunt prezentate la articolul 30 din Directiva 95/46/CE și la articolul 15 din Directiva 2002/58/CE.

Secretariatul este asigurat de Direcția C (Drepturi fundamentale și cetățenia Uniunii) a Comisiei Europene, Direcția Generală Justiție și Consumatori, B-1049 Bruxelles, Belgia, biroul MO-59 02/013.

Site: https://ec.europa.eu/info/law/law-topic/data-protection_ro

GRUPUL DE LUCRU PENTRU PROTECȚIA PERSOANELOR ÎN CEEA CE PRIVEȘTE PRELUCRAREA DATELOR CU CARACTER PERSONAL

instituit prin Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995,

având în vedere articolele 29 și 30,

având în vedere Regulamentul său de procedură,

ADOPTĂ PREZENTELE ORIENTĂRI:

CUPRINS

INTRODUCERE

Regulamentul general privind protecția datelor (RGPD) introduce cerința ca o încălcare a securității datelor cu caracter personal (denumită în continuare „încălcare") să fie notificată autorității naționale de supraveghere competente[1] (sau, în cazul unei încălcări la nivel transfrontalier, autorității principale) și, în anumite cazuri, ca persoanele ale căror date cu caracter personal au fost afectate de încălcare să fie informate cu privire la aceasta.

Obligații de notificare în cazuri de încălcări există în prezent pentru anumite organizații, cum ar fi furnizorii de servicii de comunicații electronice accesibile publicului [astfel cum se prevede în Directiva 2009/136/CE și Regulamentul (UE) nr. 611/2013][2]. De asemenea, unele state membre ale UE au prevăzut deja o obligație de notificare a încălcării în propria legislație la nivel național. Aceasta poate include obligația de a notifica încălcările care implică categorii de operatori în plus față de furnizorii de servicii de comunicații electronice accesibile publicului (de exemplu, în Germania și Italia) sau obligația de a raporta toate încălcările care implică date cu caracter personal (de exemplu, în Țările de Jos). Alte state membre pot avea coduri de bune practici relevante (de exemplu, Irlanda[3]). Deși o serie de autorități de protecție a datelor din UE încurajează în prezent operatorii să raporteze încălcările, Directiva 95/46/CE privind protecția datelor[4], care este înlocuită de Regulamentul general privind protecția datelor, nu conține o obligație specifică de notificare a încălcării, prin urmare o astfel de cerință va reprezenta o noutate pentru multe organizații. În prezent, RGPD prevede obligativitatea notificării pentru toate tipurile de operatori, cu excepția cazului în care o încălcare este puțin probabil să genereze un risc pentru drepturile și libertățile persoanelor[5]. De asemenea, persoanele împuternicite de operator îndeplinesc un rol important și trebuie să notifice orice încălcare operatorului lor[6].

Grupul de lucru „articolul 29" (GL29) consideră că noua cerință de notificare prezintă o serie de avantaje. La notificarea autorității de supraveghere, operatorii pot obține consiliere cu privire la necesitatea de informare a persoanelor afectate. Într-adevăr, autoritatea de supraveghere poate dispune ca operatorul să informeze persoanele respective cu privire la încălcare[7]. Comunicarea unei încălcări către persoanele afectate îi permite operatorului să furnizeze informații cu privire la riscurile generate ca urmare a încălcării și la măsurile pe care persoanele respective le pot lua pentru a se proteja de consecințele potențiale ale acesteia. Planul de răspuns la încălcări ar trebui să se concentreze pe protejarea persoanelor și a datelor lor cu caracter personal. În consecință, notificarea încălcării securității ar trebui considerată drept un instrument de îmbunătățire a conformității în ceea ce privește protecția datelor cu caracter personal. În același timp, ar trebui remarcat faptul că neraportarea unei

[1] A se vedea articolul 4 punctul 21 din RGPD.

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

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

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

[5] Drepturile consacrate în Carta drepturilor fundamentale a UE, disponibilă la adresa http://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:12012P/TXT

[6] A se vedea articolul 33 alineatul (2). Acesta este similar conceptual cu articolul 5 din Regulamentul (UE) nr. 611/2013, care prevede că un prestator care este contractat pentru a furniza o parte a unui serviciu de comunicații electronice (fără a avea o relație contractuală directă cu abonații) este obligat să informeze furnizorul contractant în cazul unei încălcări a securității datelor cu caracter personal.

[7] A se vedea articolul 34 alineatul (4) și articolul 58 alineatul (2) litera (e).

încălcări fie unei persoane fizice, fie unei autorități de supraveghere poate însemna că, în temeiul articolului 83, operatorul este pasibil de aplicarea unei eventuale sancțiuni.

Prin urmare, operatorii și persoanele împuternicite de operatori sunt încurajate să planifice din timp și să pună în aplicare procese pentru a fi în măsură să depisteze și să limiteze rapid o încălcare, să evalueze riscul pentru persoane[8] și ulterior să stabilească dacă este necesar să notifice autoritatea de supraveghere competentă, precum și să informeze persoanele vizate cu privire la încălcare atunci când este necesar. Notificarea autorității de supraveghere ar trebui să facă parte din planul de răspuns la incidente.

RGPD conține prevederi cu privire la momentul în care trebuie să fie notificată o încălcare și la entitatea căreia trebuie să îi fie notificată aceasta, precum și la informațiile care ar trebui furnizate ca parte a notificării. Informațiile necesare pentru notificare pot fi furnizate în mai multe etape, dar, în orice caz, operatorii ar trebui să ia măsuri cu privire la orice încălcare în timp util.

În Avizul său 03/2014 privind notificarea încălcării securității datelor cu caracter personal[9], GL29 a oferit orientări operatorilor pentru a-i sprijini în luarea deciziei de a informa sau nu persoanele vizate în cazul unei încălcări. Avizul a examinat obligația prestatorilor de servicii de comunicații electronice în temeiul Directivei 2002/58/CE și a oferit exemple din mai multe sectoare, în contextul RGPD aflat la momentul respectiv în stadiu de proiect, prezentând bune practici pentru toți operatorii.

Prezentele orientări explică cerințele obligatorii de notificare și comunicare în caz de încălcare a securității din RGPD și unele dintre măsurile pe care operatorii și persoanele împuternicite de operatori le pot lua pentru a îndeplini aceste noi obligații. De asemenea, orientările oferă exemple de diverse tipuri de încălcări, indicând cine ar trebui să fie notificat în diferite scenarii.

I. Notificarea încălcărilor securității datelor cu caracter personal în temeiul RGPD

A. Considerentele de securitate de bază

Una dintre cerințele din RGPD prevede că, prin utilizarea unor măsuri tehnice și organizatorice adecvate, datele cu caracter personal sunt prelucrate 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[10].

În consecință, RGPD impune atât operatorilor, cât și persoanelor împuternicite de operatori să pună în aplicare măsurile tehnice și organizatorice adecvate pentru a asigura un nivel de securitate adecvat riscului la care sunt expuse datele cu caracter personal care sunt prelucrate. Acestea ar trebui să ia în considerare stadiul actual al tehnicii, costurile de punere în aplicare și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscurile cu grade diferite de probabilitate și de gravitate pentru drepturile și libertățile persoanelor fizice[11]. De asemenea, RGPD prevede instituirea tuturor

[8] Acest lucru poate fi asigurat în temeiul cerinței de monitorizare și revizuire a unei evaluări a impactului asupra protecției datelor (EIPD), care este necesară pentru operațiunile de prelucrare a datelor susceptibile să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice [articolul 35 alineatele (1) și (11)].

[9] A se vedea Avizul 03/2014 privind notificarea încălcărilor securității datelor cu caracter personal http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[10] A se vedea articolul 5 alineatul (1) litera (f) și articolul 32.

[11] Articolul 32; a se vedea, de asemenea, considerentul 83

măsurilor organizatorice adecvate de protecție tehnologică în scopul de a se stabili imediat dacă s-a produs o încălcare, ceea ce determină în consecință dacă este activată obligația de notificare[12].

Prin urmare, un element esențial al oricărei politici de securitate a datelor este capacitatea, acolo unde este posibil, de a preveni o încălcare și, în cazul în care încălcarea survine cu toate acestea, de a reacționa la aceasta în timp util.

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

1. Definiție

Ca parte a oricărei încercări de a remedia o încălcare, operatorul ar trebui, în primul rând, să fie în măsură să recunoască o încălcare. RGPD definește „încălcarea securității datelor cu caracter personal" la articolul 4 alineatul (12):

> „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."

Ar trebui să fie foarte clar ce se înțelege prin „distrugerea" datelor cu caracter personal: în acest caz, datele nu mai există sau nu mai există într-o formă care să poată fi utilizată de operator. De asemenea, ar trebui să fie relativ clar ce se înțelege prin „deteriorare": acesta este cazul atunci când datele cu caracter personal au fost modificate, corupte sau nu mai sunt complete. În ceea ce privește „pierderea" datelor cu caracter personal, aceasta ar trebui să fie interpretată ca însemnând că datele pot continuă să existe, însă operatorul a pierdut controlul sau accesul la acestea sau acestea nu mai sunt în posesia sa. În cele din urmă, prelucrarea neautorizată sau ilegală poate include divulgarea datelor cu caracter personal către (sau accesarea de către) beneficiari care nu sunt autorizați să primească (sau să acceseze) datele sau orice altă formă de prelucrare care încalcă RGPD.

Exemplu

Un exemplu de pierdere a datelor cu caracter personal poate include cazul în care un dispozitiv care conține o copie a bazei de date a clienților unui operator de date a fost pierdut sau furat. Un alt exemplu de pierdere poate fi atunci când singura copie a unui set de date cu caracter personal a fost criptată printr-un program de ransomware sau a fost criptată de operator cu ajutorul unei chei care nu mai este în posesia sa.

Ceea ce trebuie să fie clar este că o încălcare este un tip de incident de securitate. Cu toate acestea, astfel cum se menționează la articolul 4 alineatul (12), RGPD se aplică numai în cazul în care există o încălcare a *datelor cu caracter personal*. Consecința unei astfel de încălcări este faptul că operatorul nu vor fi în măsură să asigure respectarea principiilor referitoare la prelucrarea datelor cu caracter personal, astfel cum este prevăzut la articolul 5 din RGPD. Aceasta evidențiază diferența dintre un incident de securitate și o încălcare a securității datelor cu caracter personal – în esență, deși toate încălcările securității datelor cu caracter personal sunt incidente de securitate, nu toate incidentele de securitate sunt în mod necesar încălcări ale securității datelor cu caracter personal[13].

[12] A se vedea considerentul 87.

[13] Trebuie remarcat faptul că un incident de securitate nu se limitează la modelele de amenințare în care o organizație este atacată dintr-o sursă externă, ci include incidente cauzate de prelucrarea internă care încalcă principiile de securitate.

Posibilele efecte negative ale unei încălcări asupra persoanelor sunt analizate în continuare.

2. Tipurile de încălcări ale securității datelor cu caracter personal

În Avizul său 03/2014 privind notificarea încălcărilor, GL29 a explicat că încălcările pot fi clasificate în funcție de următoarele trei principii bine cunoscute privind securitatea informațiilor[14]:

- „Încălcarea confidențialității" – în cazul în care are loc o divulgare neautorizată sau accidentală sau un acces neautorizat sau accidental la datele cu caracter personal.
- „Încălcarea integrității" – în cazul în care are loc o modificare neautorizată sau accidentală a datelor cu caracter personal.
- „Încălcarea disponibilității" – în cazul în care are loc o pierdere accidentală sau neautorizată a accesului[15] sau distrugerea datelor cu caracter personal.

De asemenea, trebuie remarcat faptul că, în funcție de circumstanțe, o încălcare se poate referi în același timp la confidențialitatea, integritatea și disponibilitatea datelor cu caracter personal, precum și la orice combinație a acestor elemente.

În timp ce stabilirea faptului dacă a existat o încălcare referitoare la disponibilitate sau integritate este destul de clară, poate fi mai puțin evident dacă a existat o încălcare referitoare la disponibilitate. O încălcare va fi considerată întotdeauna o încălcare referitoare la disponibilitate dacă a existat o pierdere permanentă sau o distrugere a datelor cu caracter personal.

Exemplu

Exemple 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 mod securizat, atunci când cheia de decriptare a fost pierdută. În cazul în care operatorul nu poate restabili accesul la date, de exemplu dintr-o copie de rezervă, aceasta este considerată o pierdere permanentă a disponibilității.

O pierdere a disponibilității poate surveni, de asemenea, în cazul în care a existat o întrerupere semnificativă a serviciului normal al unei organizații, de exemplu se înregistrează o întrerupere a alimentării cu energie electrică sau un atac vizând blocarea accesului, ceea ce face ca datele cu caracter personal să devină indisponibile.

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 să fie notificată. Articolul 32 din RGPD privind „securitatea prelucrării" explică faptul că, atunci când se pun în aplicare măsuri tehnice și organizatorice pentru a asigura un nivel de securitate adecvat riscului, ar trebui să se ia 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".

[14] A se vedea Avizul 03/2014.

[15] Este bine stabilit faptul că „accesul" face parte în mod fundamental din noțiunea de „disponibilitate". A se vedea, de exemplu, NIST SP800-53rev4, care definește „disponibilitatea" după cum urmează: „Asigurarea accesului rapid și fiabil și utilizarea informațiilor", disponibil la adresa http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. CNSSI-4009 se referă, de asemenea, la: „Accesul prompt și fiabil al utilizatorilor autorizați la serviciile de date și de informații." A se vedea https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. ISO/IEC 27000:2016 definește, de asemenea, „disponibilitatea" ca fiind „calitatea de a fi accesibile și utilizabile la cerere de către o entitate autorizată": https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

Prin urmare, un incident de securitate care are ca rezultat o situație în care datele cu caracter personal devin indisponibile pentru o perioadă de timp constituie, de asemenea, un tip de încălcare, întrucât lipsa accesului la date poate avea un impact semnificativ asupra drepturilor și libertăților persoanelor fizice. Trebuie precizat clar că, în cazul în care datele cu caracter personal nu sunt disponibile din cauza efectuării unei întreținere planificate a sistemului, aceasta nu reprezintă o „încălcare a securității", astfel cum este definită la articolul 4 alineatul (12).

La fel ca în cazul pierderii sau distrugerii permanente a datelor cu caracter personal (sau al oricărui alt tip de încălcare), o încălcare care implică pierderea temporară a disponibilității trebuie documentată în conformitate cu articolul 33 alineatul (5). Aceasta sprijină operatorul să demonstreze responsabilitatea față de autoritatea de supraveghere, care poate solicita prezentarea înregistrărilor respective[16]. Cu toate acestea, în funcție de circumstanțele încălcării, acest fapt poate necesita sau nu notificarea autorității de supraveghere și informarea persoanelor afectate. Operatorul va trebui să evalueze probabilitatea și gravitatea impactului asupra drepturilor și libertăților persoanelor fizice ca urmare a lipsei de disponibilitate a datelor cu caracter personal. În conformitate cu articolul 33, operatorul trebuie să efectueze notificarea, cu excepția cazului în care este puțin probabil ca încălcarea să conducă la apariția unui risc pentru drepturile și libertățile persoanelor. Desigur, acest lucru va trebui evaluat de la caz la caz.

Exemple

În contextul unui spital, dacă date medicale critice despre pacienți nu sunt disponibile, chiar și temporar, acest lucru ar putea reprezenta un risc pentru drepturile și libertățile persoanelor; de exemplu, este posibil să fie anulate operații și să fie puse în pericol viețile oamenilor.

În schimb, în cazul în care sistemele unei companii media nu sunt disponibile timp de câteva ore (de exemplu, din cauza unei întreruperi a alimentării cu energie electrică), iar compania respectivă este împiedicată în consecință să trimită buletine informative abonaților săi, acest lucru este puțin probabil să prezinte un risc pentru drepturile și libertățile persoanelor.

Ar trebui remarcat faptul că, deși o pierdere a disponibilității sistemelor operatorului ar putea fi doar temporară și poate să nu aibă un impact asupra persoanelor, este important ca operatorul să ia în considerare toate consecințele posibile ale unei încălcări, întrucât este posibil ca notificarea să fie necesară în continuare din alte motive.

Exemplu

Infectarea prin ransomware [programe ostile (malicious software) care criptează datele operatorului până la plata răscumpărării] ar putea conduce la pierderea temporară a disponibilității, în cazul în care datele pot fi recuperate din copia de rezervă. Cu toate acestea, a avut loc totuși o intruziune în rețea și ar putea fi necesară notificarea în cazul în care incidentul este calificat drept încălcare a confidențialității (și anume, datele cu caracter personal sunt accesate de atacator), iar acest fapt reprezintă un risc pentru drepturile și libertățile persoanelor.

3. Posibilele consecințe ale încălcării securității datelor cu caracter personal

O încălcare poate avea o serie de efecte negative semnificative asupra persoanelor, ceea ce poate conduce la prejudicii fizice, materiale sau morale. RGPD explică faptul că acestea pot include pierderea controlului asupra datelor lor cu caracter personal, limitarea drepturilor persoanelor, discriminare, furt sau fraudă de identitate, pierdere financiară, inversarea neautorizată a pseudonimizării, compromiterea reputației și pierderea confidențialității datelor cu caracter personal

[16] A se vedea articolul 33 alineatul (5).

protejate prin secret profesional. De asemenea, acestea pot include orice alt dezavantaj semnificativ de natură economică sau socială adus persoanelor respective[17].

În consecință, RGPD impune operatorului să notifice o încălcare autorității de supraveghere competente, cu excepția cazului în care este puțin probabil ca aceasta să genereze un risc de apariție unor astfel de efecte negative. În cazul în care există un risc probabil ridicat de apariție a acestor efecte negative, RGPD impune operatorului să informeze persoanele afectate cu privire la încălcare în cel mai scurt timp posibil în mod rezonabil[18].

Importanța posibilității de a identifica o încălcare, de a evalua riscul pentru persoane și ulterior de a o notifica, dacă este necesar, este evidențiată 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.”

În secțiunea IV sunt examinate orientări suplimentare privind evaluarea riscului de apariție a unor efecte negative asupra persoanelor.

În cazul în care operatorii nu comunică autorității de supraveghere sau persoanelor vizate sau ambelor entități o încălcare a securității datelor, deși sunt îndeplinite cerințele articolului 33 și/sau ale articolului 34, autoritatea de supraveghere are opțiunea, pe baza unei analize a tuturor măsurilor corective aflate la dispoziția acesteia, de a lua în considerare impunerea amenzii administrative adecvate[19], fie pentru a însoți o măsură corectivă în temeiul articolului 58 alineatul (2), fie ca atare. Atunci când se optează pentru aplicarea unei amenzi administrative, valoarea acesteia poate fi de până la 10 000 000 EUR sau până la 2 % din cifra de afaceri mondială totală anuală a unei întreprinderi, în conformitate cu articolul 83 alineatul (4) litera (a) din RGPD. De asemenea, este important să se țină seama de faptul că, în unele cazuri, nerespectarea obligației de a notifica o încălcare ar putea semnala fie o lipsă a măsurilor de securitate existente, fie caracterul neadecvat al măsurilor de securitate existente. Orientările GL29 privind amenzile administrative prevăd că: „Apariția mai multor încălcări diferite comise împreună într-un anumit caz înseamnă că autoritatea de supraveghere poate să aplice amenzile administrative la un nivel care să fie eficace, proporțional și disuasiv în limita celei mai grave încălcări”. În acest caz, autoritatea de supraveghere va avea, de asemenea, posibilitatea de a aplica sancțiuni, pe de o parte, pentru nerespectarea obligației de a notifica sau a comunica încălcarea (articolele 33 și 34) și, pe de altă parte, pentru absența măsurilor de securitate (adecvate) (articolul 32), întrucât acestea reprezintă două încălcări distincte ale regulamentului.

[17] A se vedea, de asemenea, considerentele 85 și 75.

[18] A se vedea, de asemenea, considerentul 86.

[19] Pentru mai multe detalii, a se consulta Orientările GL29 privind aplicarea și stabilirea amenzilor administrative, document disponibil la următoarea adresă: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

II. **Articolul 33 – Notificarea autorității de supraveghere**

A. Când trebuie să se efectueze notificarea

1. Cerințele prevăzute la articolul 33

Articolul 33 alineatul (1) prevede că:

> „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 din partea autorității de supraveghere în cazul în care."

Considerentul 87 prevede că[20]:

> „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 „ia cunoștință" un operator de încălcare?

Astfel cum este detaliat mai sus, RGPD prevede că, în cazul în care are loc o încălcare, operatorul trebuie să notifice încălcarea 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. Aceasta poate ridica chestiunea momentului în care se poate considera că un operator „a luat cunoștință" de o încălcare. În opinia GL29, ar trebui considerat că un operator„a luat cunoștință" atunci când operatorul respectiv are un grad rezonabil de certitudine că s-a produs un incident de securitate care a condus la compromiterea datelor cu caracter personal.

Cu toate acestea, astfel cum s-a indicat anterior, RGPD impune operatorului să pună în aplicare toate măsurile de protecție tehnice și organizatorice adecvate pentru a stabili imediat dacă a avut loc o încălcare și pentru a informa imediat autoritatea de supraveghere și persoanele vizate. De asemenea, acesta precizează că efectuarea notificării fără întârzieri nejustificate ar trebui stabilită luând în considerare, în special, natura și gravitatea încălcării, precum și consecințele și efectele negative ale acesteia asupra persoanei vizate[21]. Aceasta impune operatorului obligația de a se asigura că va lua „cunoștință" de orice încălcare în timp util, astfel încât să poată lua măsurile corespunzătoare.

Momentul exact în care se poate considera că un operator „a luat cunoștință" de o anumită încălcare va depinde de circumstanțele încălcării specifice. În unele cazuri, va fi relativ clar încă 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 fie plasat pe acțiunea

[20] Considerentul 85 este, de asemenea, important în acest caz.

[21] A se vedea considerentul 87.

promptă de a investiga un incident pentru a determina dacă a avut loc într-adevăr o încălcare a securității datelor cu caracter personal și, în caz afirmativ, de a lua măsuri de remediere și de a o notifica dacă este necesar.

Exemple

1. În cazul pierderii unei chei USB cu date cu caracter personal necriptate, adesea nu este posibil să se verifice dacă persoane neautorizate au obținut acces la datele respective. Cu toate acestea, 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 s-a produs o încălcare a disponibilității; operatorul ar lua „cunoștință" de aceasta în momentul în care își dă seama că s-a pierdut cheia USB.

2. O parte terță informează un operator că a primit în mod accidental datele cu caracter personal ale unuia dintre clienții săi și oferă dovezi ale divulgării neautorizate. Întrucât operatorului i s-au prezentat dovezi clare privind o încălcare a confidențialității, nu există nicio îndoială că „a luat cunoștință" de aceasta.

3. Un operator depistează că a existat o posibilă intruziune în rețeaua sa. Operatorul își controlează sistemele pentru a stabili dacă datele cu caracter personal stocate în sistemul respectiv au fost compromise și confirmă acest lucru. Și în acest caz, întrucât operatorul are acum dovezi clare despre o încălcare, nu poate exista nicio îndoială că „a luat cunoștință" de aceasta.

4. Un infractor informatic intră în contact cu operatorul după ce a spart sistemul acestuia, pentru a cere o răscumpărare. În acest caz, după verificarea sistemului pentru a confirma că acesta a fost atacat, operatorul are dovezi clare că a avut loc o încălcare și nu există nicio îndoială că a luat cunoștință de aceasta.

După ce a fost informat prima dată despre o posibilă încălcare de către o persoană, o organizație media sau o altă sursă sau atunci când a depistat el însuși un incident de securitate, operatorul poate întreprinde o scurtă investigație pentru a stabili dacă o încălcare a avut loc sau nu de fapt. În această perioadă de investigație, operatorul nu poate fi considerat ca având „cunoștință" de încălcare. Cu toate acestea, se așteaptă 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.

Odată ce operatorul a luat cunoștință de aceasta, o încălcare notificabilă trebuie să fie notificată fără întârziere nejustificată și, dacă este posibil, în cel mult 72 de ore. În această perioadă, operatorul ar trebui să evalueze riscul potențial pentru persoane în scopul de a determina dacă a fost declanșată obligația de notificare, precum și acțiunea (acțiunile) necesară (necesare) pentru a remedia încălcarea. Cu toate acestea, un operator poate dispune deja de o evaluare inițială a riscului potențial care ar putea rezulta dintr-o încălcare, ca parte unei evaluări a impactului asupra protecției datelor (EIPD)[22] efectuate înainte de efectuarea operațiunii de prelucrare în cauză. Cu toate acestea, EIPD poate fi mai generalizată în comparație cu circumstanțele specifice ale oricărei încălcări efective și, în orice caz, va trebui efectuată o evaluare suplimentară ținând cont de aceste circumstanțe. Pentru mai multe detalii privind evaluarea riscului, consultați secțiunea IV.

În cele mai multe cazuri, aceste acțiuni preliminare ar trebui să fie finalizate imediat după alerta inițială (și anume, atunci când operatorul sau persoana împuternicită de operator suspectează că a avut

[22] A se consulta Orientările GL29 privind Evaluarea impactului asupra protecției datelor (EIPD) la adresa: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

loc un incident de securitate care poate implica date cu caracter personal.) – doar în cazuri excepționale ar trebui acestea să dureze mai mult.

Exemplu

O persoană informează operatorul că a primit, de la o entitate utilizând identitatea operatorului, un e-mail care conține date cu caracter personal referitoare la utilizarea (efectivă) de către aceasta a serviciului operatorului, ceea ce sugerează că securitatea operatorului a fost compromisă. Operatorul efectuează o scurtă investigație și identifică o intruziune în rețeaua sa și dovada accesului neautorizat la datele cu caracter personal. În acest moment, s-ar considera că operatorul are „cunoștință" de încălcare și este necesară notificarea autorității de supraveghere, cu excepția cazului în care este puțin probabil ca aceasta să prezinte un risc pentru drepturile și libertățile persoanelor. Operatorul va trebui să ia măsurile corective adecvate pentru remedierea nerespectării.

Prin urmare, operatorul ar trebui să dispună de procese interne pentru a depista și a remedia 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 analizatorii de registre, din care este posibil să se definească evenimente și alerte prin corelarea datelor din registre[23]. Este important ca, atunci când se depistează o încălcare, aceasta să fie raportată în sens ascendent către nivelul adecvat al conducerii, astfel încât încălcarea să poată fi remediată și, dacă este necesar, să fie notificată în conformitate cu articolul 33 și, după caz, cu articolul 34. Astfel de măsuri și mecanisme de raportare ar putea fi detaliate în planurile de răspuns la incidente și/sau mecanismele de guvernanță ale operatorului. Acestea vor sprijini operatorul să planifice în mod eficace și să determine cine are responsabilitatea operațională în cadrul organizației pentru gestionarea unei încălcări, precum și modul sau necesitatea de a modifica statutul unui incident, după caz.

Operatorul ar trebui să dispună, de asemenea, de mecanisme cu orice persoane împuternicite de operator pe care le utilizează, care la rândul lor au obligația de a notifica operatorul în cazul unei încălcări (a se vedea mai jos).

În timp ce este responsabilitatea operatorilor și a persoanelor împuternicite de operator să pună în aplicare măsuri adecvate pentru a preveni o încălcare, a reacționa la aceasta și a o remedia, există unele măsuri practice care ar trebui luate în toate cazurile.

- Informațiile referitoare la toate evenimentele legate de securitate ar trebui să fie direcționate către o persoană responsabilă sau către persoanele însărcinate cu remedierea incidentelor, stabilirea existenței unei încălcări și evaluarea riscului.
- Ulterior, trebuie evaluat riscul la adresa persoanelor ca urmare a unei încălcări (probabilitatea de a nu exista niciun risc, probabilitatea unui risc sau a unui risc ridicat), secțiunile relevante ale organizației fiind informate în acest sens.
- Dacă este necesar, ar trebui să se efectueze notificarea autorității de supraveghere și, eventual, informarea persoanelor afectate cu privire la încălcarea securității datelor.
- În același timp, operatorul ar trebui să acționeze pentru a limita și a remedia încălcarea.
- Documentarea încălcării ar trebui să aibă loc pe măsură ce aceasta evoluează.

Prin urmare, ar trebui să fie clar că operatorul are obligația de a acționa în legătură cu orice alertă inițială și de a stabili dacă într-adevăr s-a produs sau nu o încălcare. Această perioadă scurtă permite efectuarea unor investigații și oferă operatorul ocazia să obțină probe și alte detalii relevante. Cu toate

[23] Ar trebui remarcat faptul că datele din registre care facilitează audibilitatea, de exemplu stocarea, modificările sau ștergerea datelor pot fi calificate, de asemenea, drept date cu caracter personal referitoare la persoana care a inițiat operațiunea de prelucrare respectivă.

acestea, odată ce operatorul a stabilit cu un grad rezonabil de certitudine că a avut loc o încălcare, în cazul în care au fost îndeplinite condițiile prevăzute la articolul 33 alineatul (1), acesta trebuie să notifice încălcarea autorității de supraveghere fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult 72 de ore[24]. Dacă un operator nu acționează în timp util și devine evident că a avut loc o încălcare, atunci acest lucru poate fi considerat o nerespectare a obligației de notificare în conformitate cu articolul 33.

Articolul 32 clarifică faptul că operatorul și persoana împuternicită de acesta ar trebui să dispună de măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel adecvat de securitate a datelor cu caracter personal: capacitatea de a depista, a remedia și a raporta o încălcare în timp util ar trebui considerată o parte esențială a acestor măsuri.

3. Operatori asociați

Articolul 26 se referă la operatorii asociați și precizează că operatorii asociați stabilesc responsabilitățile fiecăruia pentru respectarea RGPD[25]. Aceasta va include stabilirea părții care va avea responsabilitatea pentru asigurarea respectării obligațiilor prevăzute la articolele 33 și 34. GL29 recomandă ca mecanismele contractuale dintre operatorii asociați să includă dispoziții care stabilesc operatorul care va prelua sarcina sau va fi responsabil pentru asigurarea respectării obligațiilor de notificare a încălcării prevăzute în RGPD.

4. Obligațiile persoanei împuternicite de operator

Operatorul își păstrează responsabilitatea generală pentru protecția datelor cu caracter personal, însă persoana împuternicită de operator are un rol important în a permite operatorului să își respecte obligațiile; acesta include notificarea încălcării. Într-adevăr, articolul 28 alineatul (3) precizează că prelucrarea de către o persoană împuternicită de un operator este reglementată de un contract sau de un alt act juridic. Articolul 28 alineatul (3) litera (f) prevede că în contract sau orice alt act juridic se stipulează că persoana împuternicită de operator „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”.

Articolul 33 alineatul (2) precizează că, în cazul în care un operatorul apelează la o persoană împuternicită de operator și aceasta constată o încălcare a securității datelor cu caracter personal pe care le prelucrează în numele operatorului, trebuie să înștiințeze operatorul „fără întârzieri nejustificate”. Ar trebui remarcat faptul că persoana împuternicită de operator nu trebuie să evalueze mai întâi probabilitatea unui risc care decurge dintr-o încălcare înainte de a o notifica operatorului; operatorul trebuie să facă această evaluare atunci când ia cunoștință de încălcare. Persoana împuternicită de operator trebuie să stabilească doar dacă a avut loc o încălcare și ulterior să o notifice operatorului. Operatorul se bazează pe persoana împuternicită de acesta pentru a-și atinge obiectivele; prin urmare, în principiu, ar trebui considerat că operatorul are „cunoștință” odată ce persoana împuternicită de acesta l-a informat despre încălcare. Obligația persoanei împuternicite de operator de a notifica operatorul său permite acestuia din urmă să remedieze încălcarea și să stabilească dacă este sau nu obligat să notifice încălcarea autorității de supraveghere în conformitate cu articolul 33 alineatul (1) și persoanelor afectate în conformitate cu articolul 34 alineatul (1). De asemenea, operatorul ar putea dori să investigheze încălcarea, întrucât persoana împuternicită de operator ar putea să nu fi în măsură să cunoască toate faptele relevante cu privire la aceasta, de exemplu dacă

[24] A se vedea Regulamentul nr. 1182/71 privind stabilirea regulilor care se aplică termenelor, datelor și expirării termenelor, disponibil la adresa: http://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:31971R1182&from=EN

[25] A se vedea, de asemenea, considerentul 79.

operatorul mai deține o copie sau o copie de rezervă a datelor cu caracter personal distruse sau pierdute de către persoana împuternicită de operator. Acest lucru poate afecta obligația ulterioară a operatorului de a efectua notificarea.

RGPD nu oferă un termen explicit în care persoana împuternicită de operator trebuie să alerteze operatorul, cu excepția faptului că operatorul trebuie să facă acest lucru „fără întârzieri nejustificate". Prin urmare, GL29 recomandă persoanei împuternicite de operator să transmită de îndată operatorului o notificare, furnizând informații suplimentare despre încălcare în etape, pe măsură ce devin disponibile mai multe detalii. Acest lucru este important pentru a ajuta operatorul să îndeplinească cerința de notificare a autorității de supraveghere în termen de 72 de ore.

Astfel cum s-a explicat mai sus, contractul dintre operator și persoana împuternicită de operator ar trebui să precizeze modul în care ar trebui îndeplinite cerințele formulate la articolul 33 alineatul (2), în plus față de alte dispoziții din RGPD. Aceasta poate include cerințe pentru notificarea timpurie de către persoana împuternicită de operator care, la rândul său, contribuie la îndeplinirea obligațiilor operatorului de a raporta autorității de supraveghere în termen de 72 de ore.

În cazul în care persoana împuternicită de operator oferă servicii mai multor operatori care sunt toți afectați de același incident, persoana împuternicită de operator va trebui să transmită fiecărui operator detalii despre incident.

O persoană împuternicită de operator ar putea efectua o notificare în numele operatorului, în cazul în care operatorul a acordat persoanei împuternicite de acesta autorizația corespunzătoare și aceasta face parte din mecanismele contractuale dintre operator și persoana împuternicită de operator. O astfel de notificare trebuie efectuată în conformitate cu articolele 33 și 34. Cu toate acestea, este important de reținut că responsabilitatea juridică de notificare revine în continuare operatorului.

B. Furnizarea de informații autorității de supraveghere

1. Informațiile care trebuie furnizate

Atunci când un operator notifică o încălcare autorității de supraveghere, articolul 33 alineatul (3) prevede că acesta ar trebui, cel puțin, să:

„(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) comunice 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."

RGPD nu definește categoriile de persoane vizate sau înregistrările de date cu caracter personal. Cu toate acestea, GL29 sugerează că aceste categorii de persoane vizate se referă la diferitele tipuri de persoane ale căror date cu caracter personal au fost afectate de o încălcare: în funcție de descriptorii utilizați, acestea ar putea include, printre altele, copiii și alte grupuri vulnerabile, persoanele cu dizabilități, angajații sau clienții. 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 datele medicale, foaia matricolă cu rezultatele educaționale, informații privind asistența socială, detalii financiare, numere de conturi bancare, numere de pașapoarte etc.

Considerentul 85 arată clar că unul dintre scopurile notificării este limitarea prejudiciilor aduse persoanelor. În consecință, dacă tipurile de persoane vizate sau tipurile de date cu caracter personal indică riscul anumitor prejudicii care apar ca urmare a unei încălcări (de exemplu, furt sau fraudă de identitate, pierdere financiară, amenințare la adresa secretului profesional), atunci este important ca notificarea să indice aceste categorii. Astfel aceasta este legată de cerința de a descrie consecințele posibile ale încălcării.

Chiar dacă nu sunt disponibile informații precise (de exemplu, numărul exact de persoane vizate afectate), aceasta nu ar trebui să constituie o barieră pentru notificarea în timp util a încălcării. RGPD permite aproximări în ceea ce privește numărul de persoane afectate și numărul de înregistrări de date cu caracter personal în cauză. Accentul ar trebui să fie plasat pe remedierea efectelor negative ale încălcării, mai degrabă decât pe furnizarea de cifre precise. Astfel, atunci când a devenit clar că s-a produs o încălcare într-un anumit caz, dar încă nu este cunoscută amploarea acesteia, o notificare în etape (a se vedea mai jos) este o modalitate sigură de a respecta obligațiile de notificare.

Articolul 33 alineatul (3) prevede că operatorul furnizează „cel puțin” aceste informații printr-o notificare, astfel încât un operator poate, dacă este necesar, să furnizeze detalii suplimentare. Diferitele tipuri de încălcări (confidențialitate, integritate sau disponibilitate) ar putea necesita furnizarea de informații suplimentare pentru a explica pe deplin circumstanțele fiecărui caz.

Exemplu

Ca parte a notificării adresate autorității de supraveghere, un operator poate considera că este util să menționeze numele persoanei împuternicite de operator, dacă aceasta se află la originea unei încălcări, în special dacă aceasta a condus la un incident care afectează înregistrările de date cu caracter personal ale multor altor operatori care utilizează aceeași persoană împuternicită de operator.

În orice caz, autoritatea de supraveghere poate solicita detalii suplimentare în cadrul investigației sale cu privire la o încălcare.

2. Notificarea în etape

În funcție de natura încălcării, poate fi necesară o investigație suplimentară efectuată de către operator pentru a stabili toate faptele relevante referitoare la incident. Prin urmare, articolul 33 alineatul (4) prevede că:

„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”.

Aceasta înseamnă că RGPD recunoaște că operatorii nu vor avea întotdeauna toate informațiile necesare cu privire la o încălcare în termen de 72 de ore de la luare la cunoștință a acesteia, întrucât detaliile complete și ample cu privire la incident nu pot fi disponibile întotdeauna în această perioadă inițială. Ca atare, RGPD permite o notificare în etape. Probabil că acest lucru va fi valabil, de asemenea, pentru încălcări mai complexe, cum ar fi anumite tipuri de incidente de securitate cibernetică atunci când, de exemplu, poate fi necesară o anchetă criminalistică detaliată pentru a stabili pe deplin natura încălcării și măsura în care au fost compromise datele cu caracter personal. În consecință, în multe cazuri, operatorul va trebui să efectueze mai multe investigații și să revină cu informații suplimentare la o dată ulterioară. Acest lucru este permis în cazul în care operatorul prezintă motive pentru întârziere, în conformitate cu articolul 33 alineatul (1). GL29 recomandă ca, atunci când operatorul notifică pentru prima dată autoritatea de supraveghere, acesta ar trebui să informeze, de asemenea, autoritatea de supraveghere în cazul în care nu dispune încă de toate informațiile necesare și va furniza mai multe detalii ulterior. Autoritatea de supraveghere ar trebui să convină asupra modului și momentului în care ar trebui furnizate informații suplimentare. Acest lucru nu împiedică operatorul să furnizeze informații suplimentare în orice altă etapă, în cazul în care i se

aduc la cunoștință detalii suplimentare relevante despre încălcare care trebuie furnizate autorității de supraveghere.

Obiectul cerinței de notificare este de a încuraja operatorii să acționeze cu promptitudine cu privire la o încălcare, să o limiteze și, dacă este posibil, să recupereze datele cu caracter personal compromise și să solicite avizul competent al autorității de supraveghere. Notificarea autorității de supraveghere în primele 72 de ore poate permite operatorului să se asigure că deciziile privind notificarea sau lipsa notificării persoanelor sunt corecte.

Cu toate acestea, scopul notificării autorității de supraveghere nu este numai de a obține îndrumări asupra necesității de a informa persoanele afectate. În anumite cazuri, va fi evident că, având în vedere natura încălcării și gravitatea riscului, operatorul va trebui să notifice persoanele afectate fără întârziere. De exemplu, dacă există o amenințare imediată de furt de identitate sau în cazul în care categoriile speciale de date cu caracter personal[26] sunt divulgate online, operatorul ar trebui să acționeze fără întârzieri nejustificate pentru a limita încălcarea și pentru a o comunica persoanelor vizate (a se vedea secțiunea III). În circumstanțe excepționale, acest lucru ar putea avea loc chiar înainte de notificarea autorității de supraveghere. La un nivel mai general, notificarea autorității de supraveghere nu poate servi drept justificare pentru necomunicarea încălcării către persoana vizată atunci când acest lucru este necesar.

De asemenea, ar trebui să fie clar că, după efectuarea unei notificări inițiale, un operator ar putea să transmită actualizări autorității de supraveghere în cazul în care într-o investigație ulterioară se descoperă dovezi că incidentul de securitate este limitat și că nu a avut loc de fapt nicio încălcare. Aceste informații ar putea fi adăugate ulterior informațiilor deja furnizate autorității de supraveghere, iar incidentul să fie înregistrat corespunzător ca nefiind o încălcare. Nu există nici o sancțiune pentru raportarea unui incident care în cele din urmă se dovedește a nu fi o încălcare.

Exemplu

Un operator notifică autorității de supraveghere în termen de 72 de ore de la detectarea unei încălcări că a pierdut o cheie USB care conține o copie a datelor cu caracter personal ale unora dintre clienții săi. Mai târziu, cheia USB este găsită, fiind îndosariată greșit în incinta operatorului și este recuperată. Operatorul furnizează informații actualizate autoritatea de supraveghere și solicită modificarea notificării.

Ar trebui remarcat faptul că o abordare pe etape a notificării se aplică deja în conformitate cu obligațiile existente din Directiva 2002/58/CE, Regulamentul 611/2013 și pentru alte incidente auto-raportate.

3. Notificări amânate

Articolul 33 alineatul (1) precizează că, în cazul în care notificarea către autoritatea de supraveghere nu se face în termen de 72 de ore, aceasta este însoțită de motive întârzierii. Această dispoziție, împreună cu noțiunea de notificare în etape, recunoaște că un operator nu poate fi întotdeauna în măsură să notifice o încălcare în termenul respectiv și că o notificare întârziată poate fi admisă.

Un astfel de scenariu ar putea avea loc în cazul în care, de exemplu, un operator suportă mai multe încălcări de confidențialitate similare într-o perioadă scurtă de timp, care afectează în același mod un număr mare de persoane vizate. Un operator ar putea lua cunoștință de o încălcare și, în timp ce începe investigația și înainte de notificare, poate depista alte încălcări similare, care au cauze diferite. În funcție de circumstanțe, este posibil ca operatorul să necesite ceva timp pentru a stabili amploarea

[26] A se vedea articolul 9.

încălcărilor și, mai degrabă decât să notifice fiecare încălcare în mod individual, operatorul pregătește în schimb o notificare semnificativă care reprezintă mai multe încălcări foarte asemănătoare, cu posibile cauze diferite. Acest lucru ar putea conduce la întârzierea notificării transmise autorității de supraveghere cu mai mult de 72 de ore după ce operatorul a luat cunoștință de încălcări.

Strict vorbind, fiecare încălcare individuală este un incident raportabil. Cu toate acestea, pentru a evita o sarcină excesivă, operatorul ar putea să prezinte o notificare „grupată" care să reprezinte toate încălcările în cauză, cu condiția să se refere la aceleași tipuri de date cu caracter personal afectate în același mod, într-un interval de timp relativ scurt. În cazul în care are loc o serie de încălcări care privesc diferite tipuri de date cu caracter personal, a căror securitate a fost încălcată în moduri diferite, notificarea ar trebui să se desfășoare în mod normal, fiecare încălcare fiind raportată în conformitate cu articolul 33.

În timp ce RGPD permite notificări întârziate într-o anumită măsură, acest lucru nu trebuie văzut ca o situație care are loc în mod regulat. Trebuie subliniat faptul că notificările grupate pot fi efectuate, de asemenea, pentru mai multe încălcări similare raportate în decurs de 72 de ore.

C. Încălcări la nivel transfrontalier și încălcări care au loc în unități din afara UE

1. Încălcări la nivel transfrontalier

În cazul în care există o prelucrare transfrontalieră[27] a datelor cu caracter personal, o încălcare poate afecta persoane vizate din mai multe state membre. Articolul 33 alineatul (1) precizează că, atunci când s-a produs o încălcare, operatorul ar trebui să notifice încălcarea autorității de supraveghere competente în conformitate cu articolul 55 din RGPD[28]. Articolul 55 alineatul (1) prevede că:

> „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."

Cu toate acestea, articolul 56 alineatul (1) prevede următoarele:

> „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."

În plus, articolul 56 alineatul (6) prevede că:

> „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".

Aceasta înseamnă că, ori de câte ori o încălcare are loc în contextul prelucrării transfrontaliere și este necesară notificarea, operatorul va trebui să notifice încălcarea autorității de supraveghere

[27] A se vedea articolul 4 alineatul (23).

[28] A se vedea, de asemenea, considerentul 122.

principale[29]. Prin urmare, atunci când își elaborează planul de răspuns la încălcări, un operator trebuie să evalueze care autoritate de supraveghere este autoritatea principală de supraveghere pe care va trebui să o notifice[30]. Acest lucru va permite operatorului să răspundă cu promptitudine la o încălcare și să își îndeplinească obligațiile care îi revin în temeiul articolului 33. Ar trebui să fie clar că, în cazul unei încălcări care implică prelucrarea transfrontalieră, notificarea trebuie transmisă autorității de supraveghere principale, care nu se află neapărat în locul unde sunt stabilite persoanele vizate afectate sau chiar în locul unde a avut loc încălcarea. Atunci când transmite o notificare autorității principale, operatorul ar trebui să indice, după caz, dacă încălcarea implică unități situate în alte state membre, precum și statele membre în care este posibil ca persoane vizate să fi fost afectate de încălcare. În cazul în care operatorul are îndoieli cu privire la identitatea autorității principale de supraveghere, acesta ar trebui să informeze, cel puțin, autoritatea de supraveghere de la nivel local acolo unde a avut loc încălcarea.

2. Încălcări care au loc în unități din afara UE

Articolul 3 se referă la domeniul teritorial de aplicare a 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 stabilită în UE. În special, articolul 3 alineatul (2) prevede[31]:

> „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."

Articolul 3 alineatul (3) este, de asemenea, relevant și prevede[32]:

> „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."

În cazul în care un operator care nu este stabilit în UE face obiectul dispozițiilor articolului 3 alineatul (2) sau alineatul (3) și se confruntă cu o încălcare, acesta este obligat, prin urmare, să respecte obligațiile de notificare prevăzute la articolele 33 și 34. Articolul 27 impune unui operator (și persoanei împuternicite de operator) să desemneze un reprezentant în UE, în cazul în care se aplică articolul 3 alineatul (2). În astfel de cazuri, GL29 recomandă ca notificarea să fie făcută autorității de supraveghere din statul membru în care este stabilit reprezentantul în UE al operatorului[33].

---

[29] A se vedea Orientările GL29 pentru identificarea autorității de supraveghere principale a operatorului sau a persoanei împuternicite de către operator, disponibile la adresa http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

[30] O listă a detaliilor de contact pentru toate autoritățile naționale pentru protecția datelor din Europa se găsește la adresa: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

[31] A se vedea, de asemenea, considerentele 23 și 24.

[32] A se vedea, de asemenea, considerentul 25

[33] A se vedea considerentul 80 și articolul 27.

În mod similar, în cazul în care o persoană împuternicită de operator face obiectul dispozițiilor articolului 3 alineatul (2), aceasta se află sub incidența obligațiilor asumate de persoanele împuternicite de operator, din care cea care prezintă o importanță deosebită în cazul de față este obligația de a notifica o încălcare operatorului în conformitate cu articolul 33 alineatul (2).

D. Condiții în care nu este necesară notificarea

Articolul 33 alineatul (1) precizează că încălcările care nu sunt „susceptibile să genereze un risc pentru drepturile și libertățile persoanelor fizice" nu necesită notificarea autorității de supraveghere. Un exemplu ar putea fi cazul în care datele cu caracter personal sunt deja disponibile în mod public și o divulgare a acestor date nu constituie un risc probabil pentru persoana vizată. Acest lucru este în contrast cu cerințele existente privind notificarea încălcării pentru furnizorii de servicii de comunicații electronice disponibile publicului în Directiva 2009/136/CE, care precizează că toate încălcările relevante trebuie notificate autorității competente.

În Avizul său 03/2014 privind notificarea încălcării[34], GL29 a explicat că încălcarea confidențialității datelor cu caracter personal care au fost criptate utilizând un algoritm de ultimă generație este în continuare o încălcare a datelor cu caracter personal și trebuie notificată. Cu toate acestea, în cazul în care confidențialitatea cheii este intactă – și anume, cheia nu a fost compromisă în nicio încălcare a securității și a fost generată astfel încât să nu poată fi identificată prin mijloace tehnice disponibile de către nicio persoană care nu este autorizată să o acceseze – datele sunt în principiu neinteligibile. Astfel, este puțin probabil ca încălcarea să afecteze persoanele și, prin urmare, nu ar impune informarea persoanelor respective[35]. Cu toate acestea, chiar dacă 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. În acest caz, ar fi necesară informarea persoanelor vizate, chiar dacă datele în sine făceau obiectul unor măsuri de criptare adecvate.

De asemenea, GL29 a explicat că o situație similară ar fi cea în care date cu caracter personal, cum ar fi parolele, au fost criptate și securizate utilizând o valoare aleatorie („salt"), valoarea algoritmului de criptare (hash) a fost calculată cu o funcție hash de ultimă generație cu cheie criptografică, cheia utilizată pentru a cripta datele nu a fost compromisă în nicio încălcare și cheia utilizată pentru a cripta datele au fost generată astfel încât să nu poată fi identificată prin mijloace tehnologice disponibile de nicio persoană care nu este autorizată să o acceseze.

În consecință, dacă datele cu caracter personal au fost făcute în esență neinteligibile pentru părțile neautorizate și există o copie sau o copie de rezervă, în cazul unei încălcări a confidențialității care implică date cu caracter personal criptate în mod corespunzător ar putea să nu fie necesară notificarea autorității de supraveghere. Aceasta se datorează faptului că este puțin probabil ca o astfel de încălcare să reprezinte un risc pentru drepturile și libertățile persoanelor. Bineînțeles, acest lucru înseamnă că nici persoana nu va trebui să fie informată, întrucât probabil nu există un risc ridicat. Cu toate acestea, ar trebui să se țină seama de faptul că, deși inițial nu este necesară notificarea în cazul în care probabil nu există un riscuri pentru drepturile și libertățile persoanelor, acest lucru se poate schimba în timp, iar riscul ar trebui reevaluat. De exemplu, în cazul în care se constată ulterior că a fost compromisă cheia sau este expusă o vulnerabilitate în software-ul de criptare, este posibil ca notificarea să fie în continuare necesară.

În plus, ar trebui remarcat faptul că, dacă există o încălcare într-un caz în care nu există copii de rezervă ale datelor cu caracter personal criptate, atunci va exista o încălcare a disponibilității, care ar

[34] GL29, Avizul 03/2014 privind notificarea încălcării, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[35] A se vedea, de asemenea, articolul 4 alineatele (1) și (2) din Regulamentul (UE) nr. 611/2013.

putea prezenta riscuri pentru persoane și, prin urmare, poate necesita notificare. În mod similar, în cazul în care are loc o încălcare care implică pierderea datelor criptate, chiar dacă există o copie de rezervă a datelor cu caracter personal, aceasta ar putea fi totuși o încălcare raportabilă, în funcție de perioada de timp necesară pentru recuperarea datelor din copia de rezervă și de efectul lipsei de disponibilitate asupra persoanelor. Astfel cum prevede articolul 32 alineatul (1) litera (c), 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 ar necesita notificarea autorității de supraveghere ar fi pierderea unui dispozitiv mobil criptat securizat, utilizat de operator și personalul său. În cazul în care cheia de criptare rămâne 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 este puțin probabil ca încălcarea să genereze un risc pentru drepturile și libertățile persoanelor vizate în cauză. Dacă ulterior devine evident că a fost compromisă cheia de criptare sau că software-ul sau algoritmul de criptare este vulnerabil, atunci riscul pentru drepturile și libertățile persoanelor fizice se va schimba și, prin urmare, notificarea poate deveni necesară.

Cu toate acestea, va constitui o nerespectare a articolului 33 dacă un operator nu notifică autoritatea de supraveghere într-o situație în care datele nu au fost criptate securizat. Prin urmare, atunci când selectează software de criptare, operatorii ar trebui să evalueze cu atenție calitatea și aplicarea corectă a criptării oferite, pentru a înțelege ce nivel de protecție oferă de fapt și dacă acesta este adecvat riscurilor prezentate. De asemenea, operatorii ar trebui să fie familiarizați cu specificul funcționării produsului lor de criptare. De exemplu, un dispozitiv poate fi criptat odată ce este oprit, dar nu în timp ce se află în modul „standby". Unele produse care utilizează criptarea au „chei prestabilite" care trebuie să fie modificate de către fiecare client pentru a fi eficace. De asemenea, criptarea poate fi considerată adecvată în prezent de către experți din domeniul securității, dar poate deveni depășită în câțiva ani, ceea ce înseamnă că este discutabil dacă datele ar fi suficient de criptate de produsul respectiv și ar oferi un nivel adecvat de protecție.

III. **Articolul 34 – Informarea persoanei vizate**

A. Informarea persoanelor

În anumite cazuri, pe lângă notificarea autorității de supraveghere, operatorul este obligat, de asemenea, să informeze persoanele afectate cu privire la o încălcare.

Articolul 34 alineatul (1) prevede următoarele:

„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."

Operatorii ar trebui să țină cont de 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 ca urmare a unei încălcări. În plus, în cazul în care există un risc ridicat pentru drepturile și libertățile persoanelor ca urmare a unei încălcări, persoanele vizate trebuie, de asemenea, să fie informate. Prin urmare, pragul pentru informarea persoanelor cu privire la o încălcare este mai ridicat decât pentru notificarea autorităților de supraveghere și nu este necesar ca persoanele să fie informate cu privire la toate încălcările, protejându-le astfel de excesul de înștiințări.

RGPD afirmă că informarea persoanelor cu privire la încălcare trebuie făcută „fără întârzieri nejustificate”, ceea ce înseamnă cât mai curând posibil. Obiectivul principal al notificării persoanelor este furnizarea de informații specifice despre măsurile pe care acestea ar trebui să le ia pentru a se proteja[36]. Astfel cum s-a menționat mai sus, în funcție de natura încălcării și de riscul prezentat, informarea în timp util va ajuta persoanele să ia măsuri pentru a se proteja de eventualele consecințe negative ale încălcării.

Anexa B la prezentele orientări oferă o listă neexhaustivă de exemple de cazuri în care o încălcare ar putea conduce la un risc ridicat pentru persoane și, în consecință, de cazuri în care un operator va trebui să notifice o încălcare celor afectați.

B. Informațiile care trebuie furnizate

La notificarea persoanelor, articolul 34 alineatul (2) prevede că:

> „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).”

În conformitate cu această dispoziție, operatorul trebuie să furnizeze cel puțin următoarele informații:

- o descriere a naturii încălcării;
- numele și datele de contact ale responsabilului cu protecția datelor sau ale altui punct de contact;
- o descriere a consecințelor probabile ale încălcării; și
- o descriere a măsurilor luate sau propuse a fi luate de către operator pentru a remedia încălcarea, inclusiv, după caz, a măsurilor de atenuare a eventualelor sale efecte adverse.

Ca exemplu de măsuri luate pentru a remedia încălcarea și pentru a atenua posibilele efecte negative ale acesteia, operatorul ar putea preciza că, în urma notificării încălcării către autoritatea de supraveghere competentă, operatorul a primit consiliere privind gestionarea încălcării și diminuarea impactului acesteia. De asemenea, operatorul ar trebui să ofere, după caz, consiliere specifică persoanelor pentru a se proteja de posibilele consecințe negative ale încălcării, cum ar fi resetarea parolelor în cazul în care identificatorii lor de acces au fost compromiși. Un operator poate alege, de asemenea, să furnizeze informații în plus față de ceea ce este solicitat în acest caz.

C. Contactarea persoanelor

În principiu, încălcarea relevantă ar trebui să fie comunicată direct persoanelor vizate, cu excepția cazului în care acest lucru ar implica un efort disproporționat. Într-un astfel de caz, trebuie să existe în schimb o comunicare publică sau o măsură similară prin care persoanele vizate să fie informate într-un mod la fel de eficace [articolul 34 alineatul (3) litera (c)].

Atunci când persoanele vizate sunt informate cu privire la o încălcare, ar trebui utilizate mesaje dedicate și acestea nu ar trebui trimise cu alte informații, cum ar fi actualizări regulate, buletine informative sau mesaje standard. Aceasta contribuie la claritatea și transparența comunicării încălcării.

Exemple de metode de comunicare transparente includ mesajele directe (de exemplu, e-mail, SMS, mesaj direct), bannere de site-uri proeminente sau notificări, comunicări poștale și anunțuri proeminente în presa scrisă. O notificare limitată doar la un comunicat de presă sau un blog corporativ

[36] A se vedea, de asemenea, considerentul 86.

nu ar fi un mijloc eficace de informare a unei persoane cu privire la o încălcare. GL29 recomandă operatorilor să aleagă un mijloc care maximizează șansa de a informa în mod corespunzător toate persoanele afectate. În funcție de circumstanțe, acest lucru poate însemna că operatorul utilizează mai multe metode de informare, spre deosebire de utilizarea unui singur canal de contact.

De asemenea, operatorii trebuie eventual să se asigure că comunicarea este accesibilă în formate alternative adecvate și limbi relevante, pentru a garanta că persoanele sunt în măsură să înțeleagă informațiile care le sunt furnizate. De exemplu, la informarea unei persoane cu privire la o încălcare, limbajul utilizat în timpul desfășurării activității obișnuite cu destinatarul va fi, în general, adecvat. Cu toate acestea, în cazul în care încălcarea afectează persoane vizate cu care operatorul nu a interacționat anterior sau, în special, care locuiesc într-un alt stat membru sau în altă țară terță decât cea în care este stabilit operatorul, comunicarea în limba națională locală ar putea fi acceptabilă, ținând seama de resursele necesare. Cheia este de a ajuta persoanele vizate să înțeleagă natura încălcării și măsurile pe care acestea le pot lua pentru a se proteja.

Operatorii sunt cei mai în măsură să determine cel mai potrivit canal de contact pentru a informa persoanele cu privire la o încălcare, mai ales dacă aceștia interacționează frecvent cu clienții lor. Cu toate acestea, în mod evident un operator ar trebui să fie precaut în a utiliza un canal de contact compromis de încălcare, întrucât acest canal ar putea fi utilizat, de asemenea, de către atacatorii care uzurpează identitatea operatorului.

În același timp, considerentul 86 explică faptul 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.”

Prin urmare, operatorii ar putea dori să contacteze și să consulte autoritatea de supraveghere pentru a solicita consiliere nu numai cu privire la informarea persoanelor vizate despre o încălcare în conformitate cu articolul 34, ci și despre mesajele corespunzătoare care trebuie trimise și cele mai potrivite modalități de contactare a persoanelor.

Legată de acest aspect este recomandarea de la considerentul 88 conform căreia 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, acolo unde este justificat și pe baza recomandărilor autorităților de aplicare a legii, operatorul poate să amâne informarea persoanelor afectate cu privire la încălcare până când acest lucru nu va aduce atingere unor astfel de investigații. Cu toate acestea, persoanele vizate ar trebui totuși să fie informate imediat după această perioadă.

Ori de câte ori nu este posibil ca operatorul să informeze o persoană cu privire la o încălcare deoarece nu există date suficiente pentru a contacta persoana, în situația respectivă operatorul ar trebui să informeze persoana cât mai curând posibil (de exemplu, atunci când persoana își exercită dreptul de acces la datele cu caracter personal în temeiul articolului 15 și îi oferă operatorului informațiile suplimentare necesare pentru a o contacta).

D. Condiții în care nu este necesară informarea

Articolul 34 alineatul (3) prevede trei condiții care, dacă sunt îndeplinite, nu necesită notificarea persoanelor în cazul unei încălcări. Acestea sunt:

- Operatorul a aplicat măsuri tehnice și organizatorice adecvate pentru a proteja datele cu caracter personal înainte de încălcare, în special măsurile prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane 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 o încălcare, operatorul a luat măsuri pentru a se asigura că riscul ridicat pentru drepturile și libertățile persoanelor nu mai este probabil să se materializeze. De exemplu, în funcție de circumstanțele cazului, operatorul poate să fi identificat imediat și să fi luat măsuri împotriva persoanei care a accesat datele cu caracter personal, înainte ca acestea să poată face ceva cu acestea. Trebuie să se țină seama în continuare de posibilele consecințe ale oricărei încălcări a confidențialității, de asemenea în funcție de natura datelor în cauză.
- Aceasta ar implica eforturi disproporționate[37] de contactare a persoanelor, poate chiar în cazul în care datele lor de contact au fost pierdute ca urmare a încălcării sau nu sunt cunoscute de la început. De exemplu, arhiva unui birou de statistică a fost inundată, iar documentele care conțin date cu caracter personal au fost stocate numai pe suport de hârtie. În schimb, operatorul trebuie să facă o comunicare publică sau să ia o măsură similară, prin care persoanele sunt informate într-un mod la fel de eficace. În cazul eforturilor disproporționate, ar putea fi avute în vedere, de asemenea, modalitățile tehnice pentru a pune la dispoziție la cerere informații cu privire la încălcare, care ar putea fi utile pentru persoanele care pot afectate de o încălcare, dar care nu pot fi contactate în alt mod de către operator.

În conformitate cu principiul responsabilității, operatorii ar trebui să poată demonstra autorității de supraveghere că îndeplinesc una sau mai multe dintre aceste condiții [38]. Ar trebui să se țină cont de faptul că, deși inițial poate să nu fie necesară notificarea în cazul în care nu există riscuri pentru drepturile și libertățile persoanelor fizice, acest lucru se poate schimba în timp și riscul ar trebui reevaluat.

În cazul în care un operator decide să nu comunice o încălcare persoanei, articolul 34 alineatul (4) explică faptul că autoritatea de supraveghere poate solicita acest lucru dacă consideră că încălcarea este susceptibilă să genereze un risc ridicat pentru persoane. În mod alternativ, aceasta poate considera că au fost îndeplinite condițiile de la articolul 34 alineatul (3), caz în care nu este necesară notificarea persoanelor. În cazul în care autoritatea de supraveghere stabilește că decizia de a nu notifica persoanele vizate nu este întemeiată, aceasta poate lua în considerare posibilitatea utilizării competențelor și a sancțiunilor aflate la dispoziția sa.

[37] A se consulta Orientările GL29 privind transparența, care examinează problema efortului disproporționat, document disponibil la adresa http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

[38] A se vedea articolul 5 alineatul (2).

IV. Evaluarea riscului și riscul ridicat

A. Riscul ca element declanșator al notificării

Deși RGPD introduce obligația de notificare a unei încălcări, nu este o cerință ca notificarea să fie efectuată în toate cazurile:

- notificarea autorității de supraveghere competente este obligatorie, cu excepția cazului în care este puțin probabil ca o încălcare să genereze un risc pentru drepturile și libertățile persoanelor.
- Informarea unei persoane cu privire la o încălcare este declanșată numai atunci când este posibil ca încălcarea să genereze un risc ridicat pentru drepturile și libertățile acesteia.

Aceasta înseamnă că, imediat după ce operatorul a luat cunoștință de o încălcare, este extrem de important că acesta ar trebui nu numai să urmărească limitarea incidentului, ci și să evalueze riscul care ar putea decurge din acesta. Există două motive importante pentru aceasta: în primul rând, cunoașterea probabilității și a gravității potențiale a impactului asupra persoanei va sprijini operatorul să ia măsuri eficace pentru a limita și a remedia încălcarea; în al doilea rând, aceasta îl va ajuta să stabilească dacă este necesară notificarea autorității de supraveghere și, dacă este necesar, a persoanelor în cauză.

Astfel cum s-a explicat mai sus, este necesară notificarea unei încălcări, cu excepția cazului în care este puțin probabil ca aceasta să genereze un risc pentru drepturile și libertățile persoanelor, iar elementul principal de declanșare care impune informarea persoanelor vizate cu privire la o încălcare este posibilitatea ca aceasta să genereze un risc *ridicat* la adresa drepturilor și libertăților persoanelor. Acest risc există atunci când încălcarea poate conduce la prejudicii de natură fizică, materială sau morală pentru persoanele ale căror date au fost afectate. Exemple de astfel de prejudicii includ discriminarea, furtul sau frauda de identitate, pierderea financiară și compromiterea reputației. Atunci când încălcarea implică date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, religia sau convingerile filozofice sau apartenența la sindicate sau includ date genetice, date privind sănătatea sau date privind viața sexuală sau condamnări penale și infracțiuni sau măsuri de securitate conexe, ar trebui să se considere că este posibil să se producă prejudicii[39].

B. Factori de luat în considerare la evaluarea riscului

Considerentele 75 și 76 din RGPD sugerează că, în general, la evaluarea riscului ar trebui luată 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.

Ar trebui remarcat faptul că evaluarea riscului pentru drepturile și libertățile persoanelor ca urmare a unei încălcări are un accent diferit față de riscul luat în considerare în cadrul unei EIPD[40]. Evaluarea impactului asupra protecției datelor ia în considerare atât riscurile prelucrării datelor conform planificării, cât și riscurile în cazul unei încălcări. Atunci când se analizează o eventuală încălcare, se examinează, în termeni generali, probabilitatea ca aceasta să se producă și prejudiciile care ar putea fi aduse persoanei vizate; cu alte cuvinte, aceasta este o evaluare a unui eveniment ipotetic. În cazul unei încălcări reale, evenimentul a avut deja loc și, prin urmare, accentul este plasat exclusiv pe riscul aferent impactului încălcării asupra persoanelor.

---

[39] A se vedea considerentul 75 și considerentul 85.

[40] A se consulta Orientările GL29 privind Evaluarea impactului asupra protecției datelor (EIPD) la adresa: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

Exemplu

O evaluare a impactului asupra protecției datelor sugerează că utilizarea propusă a unui anumit produs software de securitate pentru a proteja datele cu caracter personal este o măsură adecvată pentru a asigura un nivel de securitate adecvat riscului pe care prelucrarea ar putea să o reprezinte pentru persoană. Cu toate acestea, dacă o vulnerabilitate devine cunoscută ulterior, aceasta ar schimba caracterul adecvat al software-ului pentru a limita riscul pentru datele cu caracter personal protejate și, prin urmare, riscul va trebui reevaluat ca parte a unei evaluări a impactului asupra protecției datelor în curs.

O vulnerabilitate a produsului este exploatată ulterior și are loc o încălcare. Operatorul ar trebui să evalueze circumstanțele specifice ale încălcării, datele afectate și nivelul potențial de impact asupra persoanelor, precum și probabilitatea ca acest risc să se materializeze.

Prin urmare, atunci când se evaluează riscul pentru persoane ca urmare a unei încălcări, operatorul ar trebui să ia în considerare circumstanțele specifice ale încălcării, inclusiv gravitatea impactului potențial și probabilitatea apariției acestuia. În consecință, GL29 recomandă că evaluarea ar trebui să țină seama de următoarele criterii[41]:

- Tipul de încălcare

Tipul de încălcare care a avut loc poate afecta nivelul de risc la care sunt expuse persoanele. De exemplu, o încălcare a confidențialității prin care au fost divulgate informații medicale unor părți neautorizate poate avea un set diferit de consecințe pentru o persoană în comparație cu o încălcare în care datele medicale ale unei persoane au fost pierdute și nu mai sunt disponibile.

- Natura, sensibilitatea și volumul datelor cu caracter personal

Desigur, atunci când se evaluează riscul, un factor-cheie îl reprezintă tipul și sensibilitatea datelor cu caracter personal compromise de încălcare. De regulă, cu cât sunt mai sensibile datele, cu atât va fi mai mare riscul de prejudicii pentru persoanele afectate, dar ar trebui să se ia în considerare și alte date cu caracter personal despre persoana vizată care pot fi deja disponibile. De exemplu, în circumstanțe obișnuite, este puțin probabil ca divulgarea numelui și a adresei unei persoane să aduce prejudicii substanțiale. Cu toate acestea, dacă numele și adresa unui părinte adoptiv sunt divulgate unui părinte biologic, consecințele ar putea fi foarte grave, atât pentru părintele adoptiv, cât și pentru copil.

Încălcările care implică date privind sănătatea, documente de identitate sau date financiare, cum ar fi detaliile cărții de credit, pot provoca prejudicii ca atare, dar dacă sunt utilizate împreună pot fi folosite pentru furtul de identitate. O combinație de date cu caracter personal este în mod obișnuit mai sensibilă decât un singur element de date cu caracter personal.

Unele tipuri de date cu caracter personal pot părea la început relativ inofensive, totuși ar trebui luat în considerare cu atenție ceea ce ar putea dezvălui datele respective despre persoana afectată. O listă a clienților care acceptă livrări regulate este posibil să nu fie deosebit de sensibilă, dar aceleași date

[41] Articolul 3.2 din Regulamentul 611/2013 oferă orientări cu privire la factorii care ar trebui luați în considerare în legătură cu notificarea încălcărilor în sectorul serviciilor de comunicații electronice, care ar putea fi utile în contextul notificării în temeiul RGPD. A se vedea http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:ro:PDF

despre clienții care au solicitat oprirea livrărilor în timpul vacanței ar constitui informații utile pentru infractori.

În mod similar, o cantitate mică de date cu caracter personal extrem de sensibile poate avea un impact ridicat asupra unei persoane, iar un număr mare de detalii poate dezvălui o gamă mai largă de informații despre persoana respectivă. De asemenea, o încălcare care afectează volume mari de date cu caracter personal privind numeroase persoane vizate poate avea un efect asupra unui număr mare corespunzător de persoane.

- Ușurința identificării persoanelor

Un factor important care trebuie luat în considerare este cât de ușor va fi pentru o parte care are acces la date cu caracter personal compromise să identifice anumite persoane sau să coreleze datele cu alte informații pentru a identifica persoane. În funcție de circumstanțe, identificarea ar putea fi posibilă direct din datele cu caracter personal a căror securitate a fost încălcată, fără a fi necesare cercetări speciale pentru a descoperi identitatea persoanei, sau ar putea fi extrem de dificilă corelarea datelor cu caracter personal cu o anumită persoană, dar aceasta ar putea fi totuși posibilă în anumite condiții. Identificarea poate fi posibilă direct sau indirect din datele a căror securitate a fost încălcată, dar poate depinde, de asemenea, de contextul specific al încălcării și de disponibilitatea publică a detaliilor cu caracter personal aferente. Acest lucru poate fi mai relevant pentru încălcarea confidențialității și a disponibilității.

Astfel cum s-a menționat mai sus, datele cu caracter personal protejate printr-un nivel corespunzător de criptare vor fi neinteligibile persoanelor neautorizate fără cheia de decriptare. În plus, pseudonimizarea pusă în aplicare în mod adecvat [definită la articolul 4 alineatul (5) 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, de asemenea, să reducă posibilitatea ca persoanele să fie identificate în cazul unei încălcări. Cu toate acestea, nu se poate considera că tehnicile de pseudonimizare fac datele neinteligibile.

- Gravitatea consecințelor pentru persoane.

În funcție de natura datelor cu caracter personal implicate într-o încălcare, de exemplu categorii speciale de date, potențialele prejudicii care ar putea rezulta la adresa persoanelor pot fi deosebit de grave, în special în cazul în care încălcarea poate conduce la furt sau fraudă de identitate, stres psihologic, umilire sau compromiterea reputației. În cazul în care încălcarea se referă la date cu caracter personal referitoare la persoane vulnerabile, acestea ar putea fi expuse unui risc mai mare de apariție a unui prejudiciu.

Dacă operatorul este conștient de faptul că datele cu caracter personal se află în mâinile unor persoane ale căror intenții sunt necunoscute sau care eventual sunt rău intenționate, acest fapt poate influența nivelul riscului potențial. Este posibil să existe o încălcare a confidențialității, prin care datele cu caracter personal sunt divulgate unei părți terțe, astfel cum este definită la articolul 4 alineatul (10), sau altui destinatar în mod eronat. Acest lucru se poate întâmpla, de exemplu, în cazul în care datele cu caracter personal sunt trimise în mod accidental departamentului greșit al unei organizații sau unei organizații de furnizori utilizate 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 permanentă cu aceștia și poate cunoaște procedurile, istoricul și alte detalii relevante ale acestora, destinatarul poate fi considerat „de încredere”. Cu alte cuvinte, operatorul poate avea un nivel de asigurare cu destinatarul, astfel încât să se poată aștepta în mod rezonabil ca partea terță respectivă să nu citească sau să acceseze datele trimise în mod eronat și să se conformeze instrucțiunilor sale pentru a le returna. Chiar dacă datele au fost accesate, operatorul ar putea în continuare să aibă încredere că destinatarul nu ia nicio altă măsură în legătură cu acestea, returnează

cu promptitudine datele operatorului și cooperează în vederea recuperării acestora. În astfel de cazuri, acest aspect poate fi luat în considerare în evaluarea riscului pe care o efectuează operatorul în urma încălcării – faptul că destinatarul este de încredere poate eradica gravitatea consecințelor încălcării, dar nu înseamnă că nu a avut loc o încălcare. Acest fapt însă, la rândul său, poate să elimine posibilitatea unui risc pentru persoane, astfel încât să nu mai fie necesară notificarea autorității de supraveghere sau a persoanelor afectate. Aceasta va depinde, de asemenea, de la caz la caz. Cu toate acestea, operatorul trebuie în continuare să păstreze informațiile referitoare la încălcare, ca parte a obligației generale de a ține evidența încălcărilor (a se vedea secțiunea V de mai jos).

Ar trebui să se ia în considerare, de asemenea, persistența consecințelor asupra persoanelor, caz în care impactul poate fi considerat mai mare dacă efectele sunt pe termen lung.

- Caracteristici speciale ale persoanei

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 în urma acesteia. Pot exista și alți factori referitori la persoană care ar putea afecta nivelul impactului încălcării asupra acestora.

- Caracteristici speciale ale operatorului de date

Natura și rolul operatorului și activitățile acestuia pot afecta nivelul riscului pentru persoane ca urmare a unei încălcări. De exemplu, o organizație medicală va prelucra categorii speciale de date cu caracter personal, ceea ce înseamnă că există o amenințare mai mare la adresa persoanelor în cazul în care este încălcată securitatea datelor lor cu caracter personal, în comparație cu o listă de abonați a unui ziar.

- Numărul persoanelor afectate

O încălcare poate afecta doar una sau mai multe persoane sau câteva mii, dacă nu chiar mult mai multe. În general, cu cât este mai mare numărul persoanelor afectate, cu atât poate fi mai mare impactul unei încălcări. Cu toate acestea, o încălcare poate avea un impact grav asupra unei singure persoane, în funcție de natura datelor cu caracter personal și de contextul în care acestea au fost compromise. De asemenea, cheia este de a lua în considerare probabilitatea și gravitatea impactului asupra celor afectați.

- Puncte generale

Prin urmare, atunci când evaluează riscul care ar putea fi generat de o încălcare, operatorul ar trebui să ia în considerare o combinație a gravității impactului potențial asupra drepturilor și libertăților persoanelor și a probabilității apariției acestuia. În mod evident, în cazul în care consecințele unei încălcări sunt mai grave, riscul este mai mare și, în mod similar, în cazul în care probabilitatea apariției acestora este mai mare, riscul este, de asemenea, sporit. În cazul în care există dubii, operatorul ar trebui să fie mai degrabă precaut și să efectueze notificarea. Anexa B oferă câteva exemple utile de diferite tipuri de încălcări care implică risc sau un risc ridicat pentru persoane.

Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA) a elaborat recomandări pentru o metodologie de evaluare a gravității unei încălcări, pe care operatorii și persoanele împuternicite de operator ar putea să o considere utilă atunci când elaborează planul de răspuns pentru gestionarea încălcărilor[42].

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

V. **Responsabilitatea și păstrarea evidenței**

A. Documentarea încălcărilor

Indiferent dacă o încălcare este necesar sau nu să fie notificată autorității de supraveghere, operatorul trebuie să păstreze documentația privind toate încălcările, astfel cum se explică la articolul 33 alineatul (5):

> „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."

Acest aspect este legat de principiul responsabilității din RGPD, prevăzut la articolul 5 alineatul (2). Scopul înregistrării încălcărilor care nu trebuie notificate, precum și a încălcărilor care trebuie notificate este legat, de asemenea, de obligațiile operatorului în temeiul articolului 24, iar autoritatea de supraveghere poate solicita prezentarea acestor înregistrări. Prin urmare, operatorii sunt încurajați să întocmească un registru intern al încălcărilor, indiferent dacă au sau nu obligația să le notifice[43].

Deși este de competența operatorului să stabilească metoda și structura pe care să le utilizeze la documentarea unei încălcări, în ceea ce privește informațiile care pot fi înregistrate există elemente-cheie care ar trebui incluse în toate cazurile. În conformitate cu articolul 33 alineatul (5), operatorul trebuie să înregistreze detalii privind încălcarea care ar trebui să includă cauzele acesteia, ceea ce s-a întâmplat și datele cu caracter personal afectate. De asemenea, ar trebui să se includă efectele și consecințele încălcării, împreună cu măsurile de remediere luate de operator.

RGPD nu specifică o perioadă de păstrare pentru această documentație. În cazul în care astfel de înregistrări conțin date cu caracter personal, va reveni operatorului să stabilească perioada de păstrare corespunzătoare în conformitate cu principiile privind prelucrarea datelor cu caracter personal[44] și să respecte o bază legală pentru prelucrare[45]. Operatorul va trebui să păstreze documentația în conformitate cu articolul 33 alineatul (5), în măsura în care i se poate solicita să furnizeze autorității de supraveghere dovezi privind conformitatea cu articolul respectiv sau cu principiul responsabilității în sens mai general. În mod clar, dacă înregistrările în sine nu conțin date cu caracter personal, atunci principiul limitării legate de stocare[46] din RGPD nu se aplică.

Pe lângă aceste detalii, GL29 recomandă operatorului să își documenteze, de asemenea, raționamentul pentru deciziile luate ca răspuns la o încălcare. În special, în cazul în care o încălcare nu este notificată, ar trebui documentată justificarea pentru decizia respectivă. Aceasta ar trebui să includă motivele pentru care operatorul consideră că încălcarea este puțin probabil să genereze un risc pentru drepturile și libertățile persoanelor[47]. În mod alternativ, în cazul în care operatorul consideră că sunt

[43] Operatorul poate alege să documenteze încălcările ca parte a registrului activităților de prelucrare care este menținut în conformitate cu articolul 30. Nu este necesar un registru separat, cu condiția ca informațiile relevante pentru încălcare să fie clar identificabile ca atare și să poată fi extrase la cerere.

[44] A se vedea articolul 5.

[45] A se vedea articolul 6 și, de asemenea, articolul 9.

[46] A se vedea articolul 5 alineatul (1) litera (e).

[47] A se vedea considerentul 85.

îndeplinite oricare dintre condițiile prevăzute la articolul 34 alineatul (3), acesta ar trebui să fie în măsură să furnizeze dovezi corespunzătoare în acest sens.

În cazul în care operatorul notifică o încălcare autorității de supraveghere, dar notificarea este întârziată, operatorul trebuie să fie în măsură să motiveze această întârziere; Documentația legată de aceasta ar putea contribui la demonstrarea faptului că întârzierea în raportare este justificată și nu excesivă.

În cazul în care operatorul comunică o încălcare persoanelor afectate, acesta ar trebui să fie transparent în privința încălcării și să comunice în mod eficace și în timp util. În consecință, aceasta ar sprijini operatorul să își demonstreze responsabilitatea și conformitatea prin păstrarea dovezilor unei astfel de comunicări.

Pentru a facilita respectarea articolelor 33 și 34, ar fi avantajos atât pentru operatori, cât și pentru persoanele împuternicite de operator să aibă o procedură de notificare documentată, care să stabilească procesul de urmat după ce a fost depistată o încălcare, inclusiv modul de limitare, gestionare și remediere a situației în urma unui incident, precum și evaluarea riscurilor și notificarea încălcării. În acest sens, pentru a demonstra conformitatea cu RGPD, ar putea fi util, de asemenea, să se demonstreze că angajații au fost informați despre existența unor astfel de proceduri și mecanisme și că aceștia știu cum să reacționeze la încălcări.

Ar trebui remarcat faptul că lipsa documentării corespunzătoare a unei încălcări poate conduce la exercitarea de către autoritatea de supraveghere a competențelor sale în temeiul articolului 58 și la impunerea unei amenzi administrative în conformitate cu articolul 83.

B. Rolul responsabilului cu protecția datelor

Un operator sau o persoană împuternicită de operator poate avea un responsabil cu protecția datelor (RPD)[48], fie conform dispozițiilor articolului 37, fie în mod voluntar, ca o chestiune de bună practică. Articolul 39 din RGPD stabilește o serie de sarcini obligatorii pentru RPD, dar nu împiedică repartizarea unor sarcini suplimentare de către operator, dacă este cazul.

De o importanță deosebită pentru notificarea încălcării, sarcinile obligatorii ale RPD includ, printre alte sarcini, furnizarea de consiliere și de informații privind protecția datelor pentru operator sau persoana împuternicită de operator, monitorizarea conformității cu RGPD și furnizarea de consultanță în legătură cu evaluările impactului asupra protecției datelor. De asemenea, RPD trebuie să coopereze cu autoritatea de supraveghere și să acționeze ca punct de contact pentru autoritatea de supraveghere și pentru persoanele vizate. În plus, ar trebui remarcat faptul că, la notificarea încălcării către autoritatea de supraveghere, articolul 33 alineatul (3) litera (b) impune operatorului să furnizeze numele și datele de contact ale responsabilului său cu protecția datelor sau ale unui alt punct de contact.

În ceea ce privește documentarea încălcărilor, operatorul sau persoana împuternicită de operator ar putea dori să obțină avizul RPD cu privire la structura, configurarea și administrarea acestei documentații. De asemenea, RPD ar putea fi însărcinat cu menținerea acestei evidențe.

Acești factori înseamnă că RPD ar trebui să joace un rol-cheie în asistarea prevenirii încălcării sau a pregătirii pentru o încălcare prin furnizarea de consultanță și monitorizarea conformității, precum și în timpul unei încălcări (și anume, la notificarea autorității de supraveghere) și în timpul oricărei investigații ulterioare efectuate de autoritatea de supraveghere. Având în vedere acestea, GL29 recomandă ca RPD să fie informat cu promptitudine cu privire la existența unei încălcări și să fie implicat în procesul de gestionare și de notificare a încălcărilor.

[48] A se consulta Orientările GL29 privind responsabilii cu protecția datelor (RPD) la adresa: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

VI. Obligații de notificare în temeiul altor instrumente juridice

În plus față de notificarea și comunicarea încălcărilor în temeiul RGPD, operatorii ar trebui să aibă cunoștință, de asemenea, de orice cerință de notificare a incidentelor de securitate în conformitate cu alte reglementări conexe care le pot fi aplicabile și dacă acestea le-ar putea impune, de asemenea, să informeze autoritatea cu privire la o încălcare a securității datelor cu caracter personal în același timp. Astfel de cerințe pot varia între statele membre, dar exemplele privind cerințe de notificare prevăzute în alte instrumente juridice și modul în care acestea sunt interconectate cu RGPD includ următoarele:

- Regulamentul (UE) nr. 910/2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă (Regulamentul eIDAS)[49].

Articolul 19 alineatul (2) din Regulamentul eIDAS obligă prestatorii de servicii de încredere să notifice organismului lor de supraveghere o încălcare a securității sau pierdere a integrității care are un impact semnificativ asupra serviciului de încredere prestat sau asupra datelor cu caracter personal păstrate de acesta. După caz, și anume atunci când o astfel de încălcare sau pierdere este deopotrivă o încălcare a securității datelor cu caracter personal în temeiul RGPD, prestatorul de servicii de încredere trebuie, de asemenea, să o notifice autorității 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)[50].

Articolele 14 și 16 din Directiva NIS impun operatorilor de servicii esențiale și furnizorilor de servicii digitale să notifice incidentele de securitate autorității lor competente. Astfel cum este recunoscut în considerentul 63 din Directiva NIS[51], incidentele de securitate pot include adesea o compromitere a datelor cu caracter personal. Deși Directiva NIS impune autorităților competente și autorităților de supraveghere să coopereze și să facă schimb de informații în acest context, nu este mai puțin adevărat că, atunci când astfel de incidente sunt sau pot deveni încălcări ale securității datelor cu caracter personal în temeiul RGPD, operatorii și/sau furnizorii respectivi ar fi obligați să notifice incidentul autorității de supraveghere în mod separat de cerințele de notificare a incidentelor din Directiva NIS.

Exemplu

Un furnizor de servicii de tip cloud care notifică o încălcare în temeiul Directivei NIS poate avea, de asemenea, obligația să notifice un operator dacă încălcarea include o încălcare a securității datelor cu caracter personal. În mod similar, un furnizor de servicii de încredere care notifică în temeiul eIDAS poate avea, de asemenea, obligația să informeze autoritatea relevantă pentru protecția datelor în cazul unei încălcări.

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

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

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

51 Considerentul 63: *„În multe cazuri, datele cu caracter personal sunt compromise în urma 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 aspectele relevante pentru abordarea oricăror cazuri de încălcare a securității datelor cu caracter personal în urma unor incidente.”*

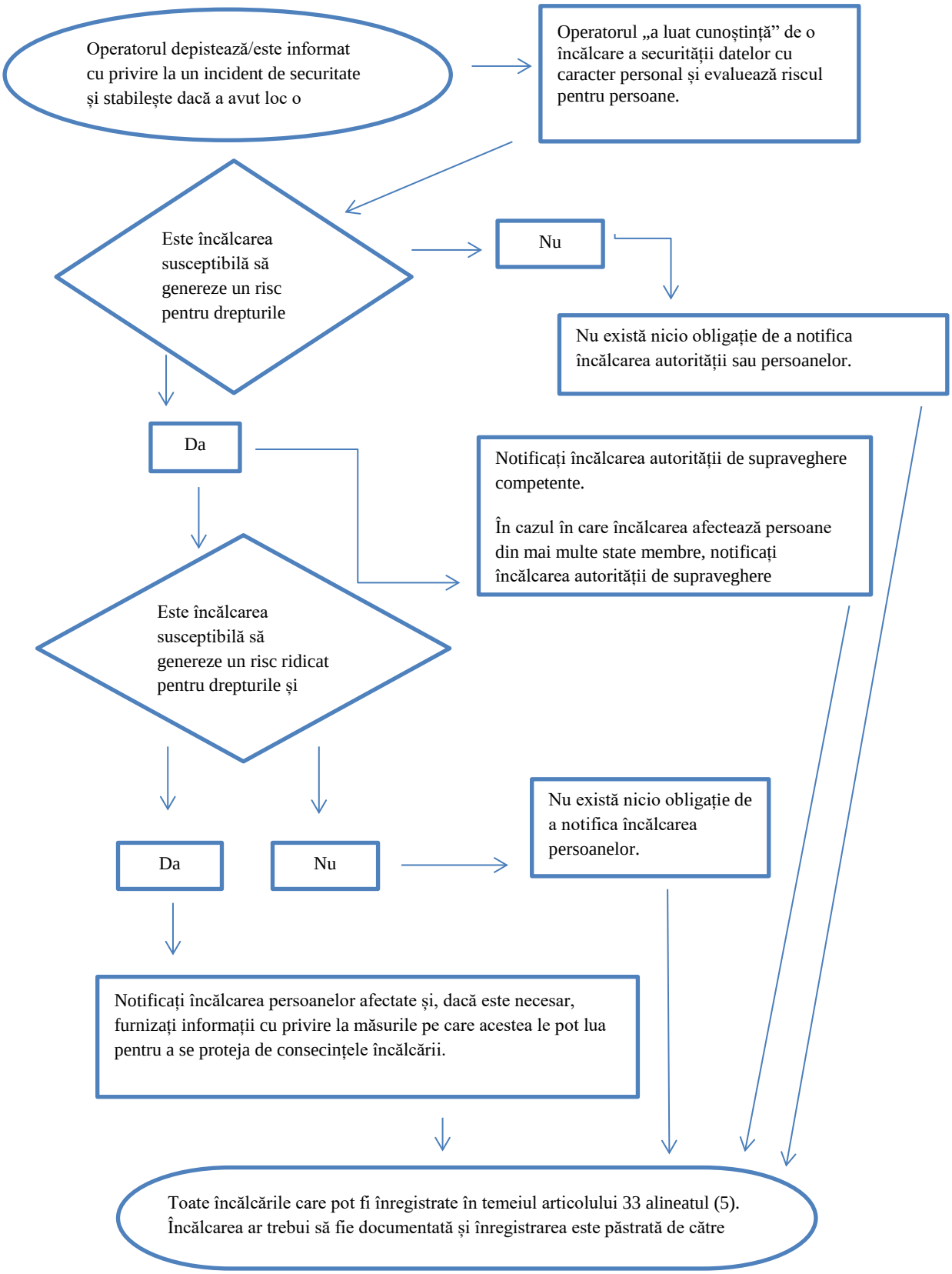
Furnizorii de servicii de comunicații electronice accesibile publicului în contextul Directivei 2002/58/CE[52] trebuie să notifice încălcările autorităților naționale competente.

Operatorii ar trebui, de asemenea, să aibă cunoștință de orice obligații suplimentare de notificare de natură juridică, medicală sau profesională în temeiul altor regimuri aplicabile.

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

VII. **Anexă**

A. Diagramă care prezintă cerințele de notificare



B. Exemple de încălcări ale securității datelor cu caracter personal și cine trebuie să le notifice

Următoarele exemple neexhaustive vor sprijini operatorii în a stabili dacă trebuie să notifice încălcarea în diferite scenarii de încălcare a securității datelor cu caracter personal. Aceste exemple pot contribui, de asemenea, la a face distincția între risc și risc ridicat la adresa drepturilor și libertăților persoanelor.

Exemplu	**Notificarea autorității de supraveghere?**	**Notificarea persoanei vizate?**	**Note/recomandări**
i. Un operator păstrează o copie de rezervă a unei arhive de date cu caracter personal criptate pe o cheie USB. Cheia este furată în timpul unei spargeri.	Nu.	Nu.	Atât timp cât datele sunt criptate utilizând un algoritm de ultimă generație, există copii de rezervă ale datelor, cheia unică nu este compromisă, iar datele pot fi recuperate în timp util, aceasta ar putea să nu fie o încălcare de raportat. Cu toate acestea, dacă datele sunt compromise ulterior, este necesară notificarea.
ii. Un operator menține un serviciu online. Ca urmare a unui atac informatic asupra serviciului respectiv, datele cu caracter personal ale persoanelor sunt exfiltrate. Operatorul are clienți într-un singur stat membru.	Da, raportați autorității de supraveghere dacă există consecințe probabile pentru persoane.	Da, raportați persoanelor în funcție de natura datelor cu caracter personal afectate și în cazul în care consecințele probabile pentru persoanele fizice sunt deosebit de grave.	
iii. O scurtă întrerupere a alimentării cu energie electrică, care durează câteva minute, la un centru de apeluri al operatorului, ceea ce înseamnă că clienții nu pot contacta telefonic operatorul și accesa înregistrările lor.	Nu.	Nu.	Aceasta nu este o încălcare care trebuie să fie notificată, dar este totuși un incident care poate fi înregistrat în temeiul articolului 33 alineatul (5). Înregistrările corespunzătoare ar trebui să fie păstrate de operator.

iv. Un operator suferă un atac cibernetic, care conduce la criptarea tuturor datelor. Nu sunt disponibile copii de rezervă și datele nu pot fi recuperate. În cadrul investigației, devine clar că singura funcționalitate a programului de ransomware a fost de a cripta datele și că în sistem nu este prezent niciun alt program de malware.	Da, raportați autorității de supraveghere dacă există consecințe posibile pentru persoane, întrucât aceasta constituie o pierdere a disponibilității.	Da, raportați persoanelor, în funcție de natura datelor cu caracter personal afectate și de efectul posibil al lipsei de disponibilitate a datelor, precum și de alte consecințe posibile.	Dacă era disponibilă o copie de rezervă și datele puteau fi recuperate în timp util, nu ar fi fost necesar ca incidentul să fie raportat autorității de supraveghere sau persoanelor deoarece nu ar fi existat o pierdere permanentă a disponibilității sau a confidențialității. Cu toate acestea, în cazul în care autoritatea de supraveghere a luat cunoștință de incident prin alte mijloace, aceasta poate lua în considerare o investigație pentru a evalua respectarea cerințelor mai ample de securitate prevăzute la articolul 32.
v. O persoană contactează telefonic centrul de apeluri al unei bănci pentru a raporta o încălcare a securității datelor. Persoana a primit o declarație lunară pentru altcineva. Operatorul efectuează o investigație scurtă (și anume, finalizată în decurs de 24 de ore) și stabilește cu o certitudine rezonabilă că a avut loc o încălcare a securității datelor cu caracter personal și dacă aceasta implică o eroare sistemică care poate însemna că alte persoane sunt sau ar putea fi afectate.	Da.	Numai persoanele afectate sunt notificate dacă există un risc ridicat și este clar că nu au fost afectate alte persoane.	În cazul în care, după o examinare ulterioară, se stabilește faptul că sunt afectate mai multe persoane, trebuie să se transmită o actualizare autorității de supraveghere, iar operatorul ia măsurile suplimentare de notificare a altor persoane dacă există un risc ridicat pentru acestea.

vi. Un operator administrează o piață online și are clienți în mai multe state membre. Piața suferă un atac cibernetic si numele utilizatorilor, parolele si istoricul achizițiilor sunt publicate online de către atacator.	Da, raportați autorității de supraveghere principale dacă este implicată prelucrarea transfrontalieră.	Da, ar putea conduce la un risc ridicat.	Operatorul ar trebui să ia măsuri, de exemplu prin forțarea resetării parolelor conturilor afectate, precum și prin alte măsuri pentru diminuarea riscului. Operatorul ar trebui să ia în considerare, de asemenea, orice alte obligații de notificare, de exemplu în conformitate cu Directiva INS, în calitate de furnizor de servicii digitale.
vii. O societate care găzduiește site-uri web și care acționează în calitate de persoană împuternicită de operatorul de date identifică o eroare în codul care controlează autorizația utilizatorului. Efectul erorii înseamnă că orice utilizator poate accesa detaliile contului oricărui alt utilizator.	În calitate de persoană împuternicită de operator, societatea care găzduiește site-uri web trebuie să notifice clienții afectați (operatorii) fără întârzieri nejustificate. Presupunând că societatea care găzduiește site-uri web a derulat propria investigație, operatorii afectați ar trebui să aibă încredere în mod rezonabil în notificarea dacă fiecare dintre aceștia a suferit o încălcare și, prin urmare, fiecare poate fi considerat ca având „cunoștință” odată ce au fost notificați de către societatea care găzduiește site-uri web (persoana împuternicită de operator). Operatorul trebuie să notifice ulterior autoritatea de supraveghere.	Dacă nu există probabil un risc ridicat pentru persoanele, acestea nu este necesar să fie notificate.	Societatea care găzduiește site-ul web (persoana împuternicită de operator) trebuie să ia în considerare orice alte obligații de notificare (de exemplu, în conformitate cu Directiva NIS, în calitate de furnizor de servicii digitale). Dacă nu există nicio dovadă privind exploatarea acestei vulnerabilități la oricare dintre operatorii săi, este posibil să nu fi survenit o încălcare care trebuie notificată, dar este posibil ca aceasta să trebuiască înregistrată sau să fie o chestiune de nerespectare în temeiul articolului 32.

viii. Dosarele medicale dintr-un spital nu sunt disponibile pentru perioada de 30 de ore din cauza unui atac cibernetic.	Da, spitalul este obligat să notifice, întrucât poare apărea un risc ridicat pentru bunăstarea și confidențialitatea pacientului.	Da, raportați persoanelor afectate.	
ix. Datele cu caracter personal ale unui număr mare de studenți sunt trimise în mod eronat către lista de corespondență greșită cu peste 1 000 de destinatari.	Da, raportați autorității de supraveghere.	Da, raportați persoanelor în funcție de domeniul de aplicare și de tipul datelor cu caracter personal implicate și de gravitatea posibilelor consecințe.	
x. Un e-mail de marketing direct este trimis destinatarilor în câmpurile „către:” sau „cc:” permițând astfel fiecărui destinatar să vadă adresa de e-mail a altor destinatari.	Da, notificarea autorității de supraveghere poate fi obligatorie dacă este afectat un număr mare de persoane, dacă sunt dezvăluite date sensibile (de exemplu, lista de corespondență a unui psihoterapeut) sau dacă alți factori prezintă riscuri ridicate (de exemplu, e-mailul conține parolele inițiale).	Da, raportați persoanelor în funcție de domeniul de aplicare și de tipul datelor cu caracter personal implicate și de gravitatea posibilelor consecințe.	Este posibil ca notificarea să nu fie necesară dacă nu se dezvăluie date sensibile și dacă se dezvăluie doar un număr minor de adrese de e-mail.