GRUPUL DE LUCRU „ARTICOLUL 29” PRIVIND PROTECȚIA DATELOR

693/14/RO
WP 213

Avizul 03/2014 privind notificarea încălcărilor securității datelor cu caracter personal

Adoptat la Bruxelles, 25 martie 2014

Rezumat

În prezentul aviz, grupul de lucru „articolul 29” privind protecția datelor oferă orientări operatorilor pentru a-i sprijini să ia decizia de a informa sau nu persoanele vizate în cazul unei „încălcări a securității datelor cu caracter personal”. Deși prezentul aviz are în vedere obligația existentă a prestatorilor de servicii de comunicații electronice în temeiul Directivei 2002/58/CE, acesta oferă exemple din multiple sectoare, în contextul proiectului de regulament privind protecția datelor, și prezintă bune practici pentru toți operatorii.

În timp ce notificarea autorității competente este necesară pentru toate cazurile de încălcare a securității datelor în conformitate cu Directiva 2002/58/CE, prezentul aviz analizează cazurile de încălcare a securității datelor cu caracter personal care necesită notificarea persoanelor vizate și prezintă măsurile pe care operatorii ar fi putut să le adopte în cadrul punerii în aplicare a sistemului lor pentru a evita încălcarea securității datelor cu caracter personal sau, cel puțin, măsurile care ar fi putut să fie puse în aplicare de la început pentru a scuti operatorul de la notificarea persoanelor vizate.

De asemenea, avizul oferă răspunsuri la unele dintre principalele întrebări referitoare la cazurile de încălcare a securității datelor cu caracter personal și la punerea în aplicare a Directivei 2002/58/CE.

1. Introducere

„Încălcarea securității datelor cu caracter personal” este definită în Directiva 2002/58/CE la articolul 2 litera (i) ca fiind „încălcarea securității având ca rezultat distrugerea accidentală sau ilegală, pierderea, alterarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod în legătură cu furnizarea de servicii de comunicații electronice destinate publicului în cadrul Comunității”.

Directiva 2002/58/CE (și propunerea de regulament european privind protecția datelor) prevăd notificarea autorității naționale competente cu privire la încălcarea securității datelor cu caracter personal. În ceea ce privește notificarea, detaliile privind informațiile care trebuie furnizate sunt disponibile în anexa I la Regulamentul (UE) nr. 611/2013.

Atunci când încălcarea securității datelor cu caracter personal ar putea afecta negativ datele cu caracter personal sau viața privată a unei persoane vizate[1], operatorul de date informează, de asemenea, persoana vizată afectată de încălcare, fără întârzieri nejustificate[2].

Directiva 2002/58/CE, precum și Regulamentul (UE) nr. 611/2013 prevăd o scutire de la obligația de notificare a persoanelor vizate în cazul în care datele au devenit neinteligibile. Dacă furnizorul a demonstrat autorității competente, într-un mod pe care aceasta îl consideră satisfăcător, că a aplicat măsuri tehnologice adecvate de protecție pentru a se asigura că datele devin neinteligibile pentru persoanele care nu sunt autorizate să le acceseze[3] și că măsurile respective au fost aplicate datelor afectate de încălcarea securității, notificarea încălcării securității datelor cu caracter personal către persoana vizată nu este necesară[4].

Existența scutirii de la notificarea persoanelor vizate este motivată de faptul că, prin luarea de măsuri corespunzătoare, se pot reduce riscurile reziduale la adresa vieții private a persoanei vizate până la un nivel neglijabil. Încălcarea confidențialității datelor cu caracter personal care au fost criptate cu un algoritm de ultimă generație reprezintă tot o încălcare a securității datelor cu caracter personal și trebuie să fie notificată autorității. Cu toate acestea, în cazul în care confidențialitatea cheii de decriptare este intactă, datele sunt, în principiu, neinteligibile pentru persoanele neautorizate și, prin urmare, este puțin probabil ca încălcarea să afecteze în mod negativ persoana vizată; în consecință, nu este necesar ca aceasta să fie notificată persoanei vizate.

Cu toate acestea, chiar și atunci când datele sunt criptate, pierderea sau modificarea acestora poate avea efecte negative asupra persoanelor vizate în cazul în care operatorul de date nu are

[1] În prezentul aviz, utilizăm termenul de „persoană vizată” astfel cum este definit în Directiva 95/46/CE. În contextul Directivei 2002/58/CE, acesta corespunde termenului „abonat sau persoană individuală”.
[2] În conformitate cu Directiva 2002/58/CE și Regulamentul (UE) nr. 611/2013, autoritatea trebuie să fie notificată în termen de maxim 24 de ore de la detectarea încălcării securității datelor cu caracter personal, atunci când este posibil, cu posibilitatea de prelungire la 72 de ore în anumite cazuri. Notificarea abonatului sau a persoanei în cauză se face fără întârzieri nejustificate [în sensul articolului 2 alineatul (2) din Regulamentul (UE) nr. 611/2013] după detectarea încălcării securității datelor cu caracter personal. Notificarea persoanei vizate nu depinde de notificarea adresată autorității naționale competente.
[3] Directiva 2002/58/CE, articolul 4 alineatul (3); Regulamentul (UE) nr. 611/2013, articolul 4 alineatul (1); Regulamentul general privind protecția datelor, versiune consolidată neoficială după votul Comisiei pentru libertăți civile, justiție și afaceri interne, furnizată de către raportor, articolul 32 alineatul (3).
[4] Atragem atenția asupra faptului că, în cazul în care cheia de decriptare este compromisă ulterior, toate încălcările anterioare care nu au fost notificate pe baza confidențialității cheii trebuie să fie notificate.

copii de rezervă. În acest caz, notificarea persoanelor vizate ar trebui să rămână obligatorie, chiar dacă s-au luat măsuri de protecție prin criptare.

Prin urmare, este important ca operatorii să adopte strategii proactive și să-și planifice activitatea în mod corespunzător. Articolul 17 din Directiva 95/46/CE, precum și articolul 4 alineatul (1) și articolul 4 alineatul (1a) din Directiva 2002/58/CE prevăd că operatorii trebuie să ia măsurile organizaționale și tehnologice adecvate pentru a „asigura un nivel de securitate corespunzător riscurilor" prezentate de prelucrare. În acest sens, este important să se dispună de un cadru adecvat de gestionare a riscurilor, care să conțină elementele minime pe care o astfel de abordare ar trebui să le aibă și care să furnizeze, de asemenea, un set de controale tehnice și organizatorice minime adecvate, pe care să le poată defini operatorul, cu un accent deosebit asupra controalelor care fac datele ininteligibile atunci când este necesar. În plus, întreprinderile ar trebui să stabilească, de asemenea, în avans, planuri adecvate pentru a soluționa cazurile de încălcare a securității datelor cu caracter personal, care să asigure că acestea răspund rapid și eficient la încălcarea securității datelor cu caracter personal.

În cazul în care articolul 17 fost respectat în mod corespunzător, și anume, înainte de instituirea prelucrării datelor, se poate considera că riscurile legate de încălcarea securității datelor cu caracter personal au fost analizate și reduse în prealabil. În astfel de cazuri, încălcarea securității datelor cu caracter personal poate avea loc mai rar și poate avea mai puține consecințe asupra persoanelor vizate. Având în vedere faptul că notificarea persoanelor vizate nu este necesară în cazul în care încălcarea nu afectează în mod negativ datele cu caracter personal sau viața privată a persoanelor vizate, sau în cazul în care au fost aplicate măsuri tehnologice adecvate de protecție a datelor afectate de încălcarea securității, cea mai bună modalitate de a evita obligația de a informa persoanele vizate este de a integra garanții adecvate privind protecția vieții private în proiectele în care se prelucrează date cu caracter personal.

Notificarea persoanelor vizate ar trebui să fie efectuată fără întârzieri nejustificate[5] și nu depinde de notificarea încălcării securității datelor cu caracter personal către autoritatea națională competentă. Operatorul de date ar trebui să aibă în vedere faptul că, deși acesta nu este un criteriu pentru luarea deciziei de a informa sau nu persoanele vizate, unul dintre principalele avantaje ale notificării este faptul că aceasta oferă persoanelor vizate informațiile necesare pentru a reduce efectele negative care rezultă din circumstanțele încălcării. În cazul în care operatorul are dubii cu privire la probabilitatea unor efecte negative asupra datelor cu caracter personal sau asupra vieții private a persoanelor vizate, acesta ar trebuie să procedeze cu prudență și să notifice persoanele în cauză. De asemenea, ar trebui să se țină seama de posibilitatea ca autoritățile competente să solicite notificarea persoanelor vizate după evaluarea aprofundată a notificării.

Prezentul aviz propune o **listă neexhaustivă de exemple de situații în care persoanele vizate ar trebui să fie notificate[6]**. Examinăm fiecare încălcare a securității datelor cu caracter personal utilizând trei criterii de securitate clasice: astfel, termenul „încălcarea

[5] În Directiva 2002/58/CE și în Regulamentul (UE) nr. 611/2013 se prevede că notificarea autorității trebuie efectuată în termen de maxim 24 de ore de la detectarea încălcării securității datelor cu caracter personal, în cazul în care este posibil, cu posibilitate de prelungire la 72 de ore în anumite cazuri. Notificarea abonatului sau a persoanei în cauză se face cât mai repede posibil după detectarea încălcării securității datelor cu caracter personal.

[6] Având în vedere faptul că propunerea de regulament privind protecția datelor prevede extinderea obligației de notificare la toate sectoarele și dat fiind că mai multe state membre au instituit deja o obligație legală de notificare, exemplele din prezentul aviz nu se limitează la sectorul comunicațiilor electronice.

disponibilității” corespunde distrugerii sau pierderii accidentale sau ilegale a datelor cu caracter personal, „încălcarea integrității” se referă la modificarea datelor cu caracter personal, iar „încălcarea confidențialității” se referă la divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal. În continuare, avizul oferă **orientări generale** cu privire la cazurile care nu necesită notificare. În cele din urmă, **se dezbat principalele aspecte** cu care operatorii se pot confrunta atunci când iau decizia de a notifica sau nu persoanele vizate.

2. Încălcări care pot afecta negativ persoanele vizate

Încălcările ar trebui să fie notificate persoanelor vizate fără întârzieri nejustificate, în cazul în care este probabil ca acestea să aibă efecte negative asupra datelor cu caracter personal sau asupra vieții private. Prezenta secțiune enumeră exemple de încălcări care îndeplinesc aceste criterii. De asemenea, se prezintă exemple de măsuri tehnice care, dacă ar fi fost puse în aplicare înainte de incident, este posibil să fi permis evitarea notificării persoanelor vizate.

Cazul 1. *Patru laptopuri au fost furate dintr-un „institut de îngrijiri medicale pentru copii"; în acestea se aflau stocate date sensibile privind sănătatea și bunăstarea socială, precum și alte date cu caracter personal referitoare la 2 050 de copii.*

Această încălcare a securității datelor cu caracter personal afectează confidențialitatea, precum și (în cazul în care operatorul nu dispune de copii de rezervă ale datelor) disponibilitatea și integritatea datelor.

Eventualele consecințe și efecte negative ale încălcării confidențialității

- Primul impact este o încălcare a secretului medical: baza de date conține informații medicale intime privind copiii, care sunt accesibile persoanelor neautorizate.
- Publicarea datelor ar putea avea un impact asupra școlii și/sau asupra mediului familial al copiilor (de exemplu, date privind violența, boli pe termen lung, probleme mintale, dificultăți sociale sau financiare ale familiei etc.).
- Aceasta poate afecta emoțional copiii și părinții.
- Datele pot fi utilizate pentru a șantaja părinții și copiii (în funcție de vârsta acestora).
- Părinții unor copii grav bolnavi pot fi vizați de persoane dornice să profite de problemele acestora (de exemplu, șarlatani, secte etc.).

Eventualele consecințe și efecte negative ale încălcării disponibilității

- Aceasta poate perturba continuitatea tratamentului copiilor, determinând agravarea bolii sau o recidivă.
- Aceasta poate conduce la o otrăvire accidentală din cauza unor alergii la medicamente sau a unor interacțiuni ale medicamentelor, care pot cauza diferite probleme de sănătate sau deces.
- Aceasta poate conduce la întârzieri nejustificate în ceea ce privește rambursarea sau asistența financiară pentru persoanele vizate, care va avea un impact financiar asupra familiilor în cauză.

Eventuale consecințe și efecte negative ale încălcării integrității:

- Pierderea datelor ar putea afecta integritatea dosarelor medicale și ar putea perturba tratamentele copiilor. De exemplu, în cazul în care există doar o copie de rezervă veche a dosarelor medicale, toate modificările aduse datelor, care au fost înregistrate pe calculatoarele furate, se vor pierde, ceea ce conduce la compromiterea integrității datelor. Utilizarea datelor neactualizate din dosarul

medical poate perturba continuitatea tratamentelor copiilor, determinând agravarea bolii sau o recidivă.

Având în vedere efectele potențiale, în acest caz ar trebui să se efectueze notificarea, dar este, de asemenea, important să se ia în considerare vârsta și gradul de maturitate ale persoanelor vizate. În cazul de față, pe lângă notificarea copiilor înșiși, ar putea fi mai adecvat să se notifice un părinte sau tutore legal, care are deja un rol activ în îngrijirea medicală a copilului, atunci când notificarea este necesară sau este prevăzută de legislația aplicabilă.

În acest caz, părinții notificați vor fi în măsură să raporteze anomalii în continuitatea tratamentului, să verifice alergiile cunoscute de institut sau să solicite efectuarea de noi teste medicale pentru a se asigura că tratamentul primit de copiii lor este cel corect. De asemenea, aceștia pot alege să informeze direct și alte persoane cu privire la starea de sănătate a copiilor, cu scopul de a controla anumite efecte asupra mediului copiilor.

Exemplu de garanții corespunzătoare care ar fi putut reduce riscurile dacă ar fi fost puse în aplicare în prealabil:

- Încălcarea disponibilității și a integrității ar fi putut fi prevenită sau consecințele și efectele negative ar fi putut fi atenuate dacă ar fi existat copii de rezervă securizate și suficient de actualizate;
- Eventualele consecințe și efecte negative ale încălcării confidențialității ar fi putut fi atenuate prin protejarea datelor cu ajutorul unui produs de criptare adecvat, cu o cheie suficient de puternică și de confidențială.

În cazul în care garanțiile ar fi fost puse în aplicare și ar fi rămas securizate (și anume,, dacă cheia ar fi rămas confidențială și copia de rezervă ar fi continuat să fie disponibilă), notificarea persoanelor vizate nu ar fi fost obligatorie, în principiu. Acest lucru ar trebui demonstrat autorității competente, într-un mod pe care aceasta îl consideră satisfăcător.

Cazul 2. *Datele cu caracter personal privind clienții unui broker de asigurări de viață au fost accesate de persoane neautorizate prin exploatarea vulnerabilității unei aplicații web. Persoanele vizate erau identificate cu numele și adresa, datele cuprinzând, de asemenea, chestionare medicale completate. 700 de persoane vizate au fost afectate.*

Eventuale consecințe și efecte negative ale încălcării confidențialității

- Datele publicate pe internet de către atacator pot afecta abilitatea persoanelor vizate de a găsi un loc de muncă (de exemplu, răspunsuri privind probleme de sănătate, graviditate etc.).
- Aceasta ar putea avea un impact asupra mediului profesional și/sau familial al persoanelor vizate.
- Ar putea exista, de asemenea, un impact emoțional, în cazul în care persoanele vizate își ascund afecțiunea diagnosticată.
- Aceasta poate conduce la fraudă de identitate.
- Datele (de exemplu, faptul de a fi client al unei anumite societăți sau de a plăti pentru anumite servicii) pot fi utilizate pentru phishing.

Întrucât situația este susceptibilă a afecta în mod negativ persoana vizată, aceasta ar trebui să fie comunicată persoanei vizate.

Exemplu de garanții corespunzătoare care ar fi putut reduce riscurile dacă ar fi fost puse în aplicare în prealabil:

- O monitorizare continuă a aspectelor vulnerabile potențiale ale tehnologiilor utilizate, inclusiv dar fără a se limita la verificarea periodică a vulnerabilității site-ului internet și actualizarea software-ului (inclusiv software-ul de securitate), ar fi putut să prevină încălcarea sau să limiteze impactul acesteia.

  Deși vulnerabilitățile de tip „atacuri în ziua zero" în materie de securitate nu pot fi evitate ușor, adoptarea de politici adecvate și eficiente privind prevenirea proactivă a exploatării vulnerabilităților în materie de securitate, inclusiv revizuirea codului, poate reduce marja de risc până la un nivel acceptabil. De asemenea, o bună politică de gestionare a incidentelor în materie de securitate poate, la rândul său, să reducă consecințele unei încălcări prin limitarea efectelor sale negative în ceea ce privește durata și domeniul de aplicare.

- La fel precum în cazul precedent, eventualele consecințe și efecte negative ale încălcării confidențialității ar fi putut să fie atenuate prin protejarea datelor referitoare la clienți cu ajutorul unui produs de criptare adecvat, cu chei confidențiale suficient de puternice. Această metodă poate fi deosebit de eficientă pentru a proteja datele împotriva furtului discului sau a unor circumstanțe similare.

- În sfârșit, societatea de asigurări ar fi putut să utilizeze diferite tehnologii care sporesc confidențialitatea pentru a minimiza cantitatea de date înregistrate și/sau posibilitatea de identificare a persoanei vizate. De exemplu, societatea ar fi putut să transmită prin poștă un număr de identificare atribuit în mod aleatoriu pentru a permite clienților săi să completeze online chestionarul medical. Acest lucru poate evita includerea de întrebări referitoare la nume, adresă, data nașterii sau numărul de telefon în chestionarul online.

Cazul 3. *Un angajat al unui furnizor de servicii de internet a transmis unui terț numele de utilizator și parola unui cont cu drepturi globale de acces la baza de date a clienților. Utilizând contul respectiv, terțul poate avea acces la toate informațiile despre clienți, fără nicio restricție. Baza de date include numele, adresa, adresa de e-mail, numerele de telefon, datele de acces și alte date de identificare (nume de utilizator, parole criptate prin funcția hash, numărul de identificare a clientului), precum și date privind plățile (numărul de cont, detalii privind cărțile de credit etc.). Deși datele privind plățile au fost criptate cu un algoritm de ultimă generație, contul de administrator compromis avea autorizație de acces la acestea, prin urmare, terțul a putut, de asemenea, să le acceseze. Societatea are peste 100 000 de clienți.*

Eventuale consecințe și efecte negative ale încălcării confidențialității

- Utilizarea abuzivă a datelor privind plățile (în special detaliile privind cardurile de credit) ar avea un impact financiar asupra clienților.

- Întrucât parolele au fost criptate numai prin funcția hash, terțul poate deduce cu ușurință textul corespunzător. Accesul la contul oricărui client ar fi posibil chiar și după închiderea contului a cărei securitate a fost încălcată.
- Terțul ar putea folosi cu ușurință adresa de e-mail și parola unora dintre persoanele vizate pentru a accesa conturi ale altor servicii online, având în vedere faptul că multe persoane folosesc aceeași parolă pentru o gamă variată de servicii online.

Eventuale consecințe și efecte negative ale încălcării integrității:

- Terțul a avut acces integral la baza de date și a avut posibilitatea să modifice, să șteargă sau să adauge date în conturi.
    - Dacă furnizorul de servicii de internet oferea, de asemenea, un serviciu de e-mail sau de găzduire de pagini internet, terțul ar fi avut posibilitatea să acceseze, să modifice sau să șteargă conținutul respectiv, să modifice setările DNS sau să închidă contul persoanei vizate.

Deși datele financiare au fost criptate, terțul a avut acces la datele decriptate prin interfața de utilizator și, prin urmare, scutirea de la notificare nu se aplică.

În cazul în care fișierele-jurnal securizate sunt fiabile (și anume, nu au fost compromise) și se poate observa din acestea că din contul respectiv nu s-a accesat baza de date a clienților, notificarea persoanei vizate nu ar trebui să fie obligatorie.

În caz contrar, situația ar trebui să fie notificată clienților afectați și scutirea nu se aplică, întrucât încălcarea securității ar putea afecta în mod negativ persoana vizată.

Atunci când parolele sunt compromise, operatorul de date ar trebui să oblige persoanele vizate să își creeze în mod securizat o parolă nouă, asigurându-se că toate noile parolele sunt introduse de utilizatori legitimi și nu de părți terțe care au obținut datele de autentificare. În practică, aceasta poate corespunde procedurii securizate de reînnoire a unei parole pierdute și ar trebui să includă informații cu privire la motivul pentru reînnoirea parolei. Notificarea către utilizator ar trebui să includă, de asemenea, recomandarea de a nu utiliza parola folosită anterior sau o parolă similară și de a modifica parola compromisă în toate conturile în care este folosită parola respectivă.

Exemplu de garanții corespunzătoare care ar fi putut reduce riscurile dacă ar fi fost puse în aplicare în prealabil:

- Fiecare persoană trebuie să aibă propriul cont și accesul la datele cu caracter personal ar trebui să fie autorizat exclusiv prin aplicarea principiului necesității de a cunoaște și a principiului privilegiilor minime. Aceasta se aplică, de asemenea, furnizorilor, personalului de întreținere al societăților terțe și altor persoane care au nevoie de acces la baza de date în mod temporar: acestea nu ar trebui să aibă acces decât la funcționalitatea și la datele care le sunt necesare pentru a îndeplini sarcinile care le sunt atribuite, într-un timp nu mai lung decât este strict necesar. Utilizarea conturilor cu „acces global” la baza de date ar trebui să fie limitată și ar trebui să se pună în aplicare metode pentru urmărirea și limitarea utilizării acestui tip de conturi. Prin instituirea unor astfel de garanții, încălcarea ar fi putut să fie prevenită sau impactul acesteia ar fi putut să fie atenuat.
- În cazul în care parolele ar fi fost stocate în condiții de securitate (de exemplu, criptate prin utilizarea funcțiilor „salt” și „hash”), efectele negative secundare

asupra persoanelor vizate ar fi scăzut considerabil. Cu toate acestea, persoanele care aleg parole cu un nivel scăzut de securitate pot fi supuse riscurilor, în special în cazul în care folosesc aceleași date de acces și pentru alte servicii online. Riscurile ar fi putut să fie reduse dacă s-ar fi sugerat utilizatorilor să aleagă parole cu un nivel mai înalt de securitate.

Cazul 4. *Un plic care conținea chitanțe eliberate pentru plăți cu carte de credit a fost aruncat din greșeală într-un coș de gunoi în loc să fie distrus în mod securizat. Coșul de gunoi a fost răsturnat într-un coș mare lăsat în afara clădirii în vederea colectării deșeurilor. O persoană a luat plicul din cel de-al doilea coș și a distribuit apoi chitanțele eliberate pentru plățile cu carte de credit într-un cartier de locuințe din apropiere. Datele includeau detaliile complete ale cărții de credit*[7] *și numele titularului cărții de credit. În unele cazuri, semnătura titularului cărții de credit era, de asemenea, disponibilă. 800 de persoane vizate au fost afectate.*

Eventuale consecințe și efecte negative ale încălcării confidențialității

- Încălcarea ar putea avea un impact financiar asupra persoanelor vizate, în cazul în care datele cărților de credit ale acestora sunt încă valabile și sunt utilizate în mod abuziv[8].

Întrucât situația este susceptibilă a afecta în mod negativ persoana vizată, aceasta ar trebui să fie adusă la cunoștința persoanelor vizate în cauză. În acest caz, dacă nu există alte evidențe, poate părea dificil să se notifice fiecare persoană vizată în parte, întrucât nu se poate ști ce chitanțe specifice eliberate pentru plăți cu carte de credit erau în plic. Magazinul ar trebuie să avertizeze instituția de prelucrare a plăților cu carte de credit, astfel încât aceasta să poată monitoriza eventualele tranzacțiile frauduloase. O altă orientare practică propusă în Regulamentul (UE) nr. 611/2013[9] prevede că, atunci când prestatorul, „în ciuda faptului că a depus eforturi rezonabile, nu poate identifica, în intervalul de timp menționat la alineatul (3), toate persoanele care riscă să fie afectate negativ de încălcarea securității datelor cu caracter personal, prestatorul poate notifica persoanele respective, în acest interval de timp, prin anunțuri în mass-media regională sau națională de mare anvergură din statul membru în cauză". Prin urmare, în cazul unui magazin cu o gamă de clienți care este, în cea mai mare parte, locală, o notificare într-un ziar regional poate fi considerată suficientă. De asemenea, informarea companiilor care emit cărți de credit în legătură cu încălcarea ar putea contribui la protejarea clienților acestora.

În cazul în care operatorul ar fi recuperat plicul dintr-unul din coșurile de gunoi și acesta ar fi rămas nedeschis, este improbabil ca situația să afecteze utilizatorii; prin urmare, nu ar fi necesar ca persoanele vizate să fie informate în legătură cu încălcarea.

[7] Deși cea mai bună practică este trunchierea datelor cărții de credit cu care se efectuează plata pe chitanța imprimată eliberată clientului, aceasta nu este o funcție disponibilă la toate terminalele din punctele de vânzare (POS) și datele cărții de credit pot fi imprimate integral pe copiile chitanțelor comerciantului.
[8] Având în vedere faptul că există încă modalități de utilizare a detaliilor cărților de credit fără cod CVV (sau echivalente), trebuie să fie notificate inclusiv încălcările care nu includ CVV.
[9] Deși regulamentul nu este aplicabil în acest context.

Exemplu de garanţii corespunzătoare care ar fi putut reduce riscurile dacă ar fi fost puse în aplicare în prealabil:

- Informarea angajaților cu privire la consecințele potențiale ale unor astfel de încălcări și utilizarea unui dispozitiv de distrugere a documentelor de birou corespunzător[10] sau a unui serviciu de distrugere a arhivei pentru a distruge chitanțele eliberate pentru plata cu carte de credit (și orice alte documentele care conțin date cu caracter personal) înainte de a le arunca ar reduce considerabil riscul producerii unei astfel de încălcări.
- Utilizarea terminalelor din punctele de vânzare (POS) care nu includ detaliile complete ale cărții de credit.

Cazul 5. *Laptopul criptat al unui consilier financiar a fost furat din portbagajul unui autoturism. Au fost afectate toate detaliile evaluărilor financiare – de exemplu, datele privind ipotecile, salariile, cererile de împrumut ale unui număr de 1 000 de persoane vizate. Cheia de criptare și fraza de securitate nu sunt compromise, însă nu există nicio copie de rezervă.*

Eventuale consecinţe şi efecte negative ale încălcării confidenţialităţii

- În funcție de natura exactă a datelor a căror securitate a fost încălcată, utilizarea abuzivă a datelor poate avea efecte diferite asupra persoanelor vizate. Cu toate acestea, întrucât laptopul dispunea de criptare integrală a discului (de ultimă generație) activată cu o frază de securitate puternică care nu a fost compromisă, nu a avut loc nicio divulgare neautorizată a datelor.

Eventuale consecințe și efecte negative:

- Lipsa datelor face necesar ca persoanele vizate să ofere informațiile necesare din nou. Acest lucru implică un efect negativ redus din partea persoanelor vizate sub formă de acțiuni care necesită timp și implică disconfort.
- În unele cazuri, acest lucru poate provoca, de asemenea, nerespectarea termenelor limită de depunere sau de înaintare a cererilor, ceea ce poate avea diferite efecte secundare asupra persoanelor vizate, în funcție de context: amenzi, pierderea veniturilor sau a beneficiilor anticipate, pierderea unor oportunități, rezilierea unui contract de vânzare-cumpărare etc.

Întrucât datele au fost pierdute și efectele încălcării disponibilității nu au fost diminuate, încălcarea securității datelor cu caracter personal poate afecta în mod negativ persoana vizată. Prin urmare, încălcarea ar trebui să fie adusă la cunoștința persoanelor vizate în cauză. În timp ce notificarea va explica faptul că informațiile vor trebui să fie furnizate din nou consilierului financiar, aceasta ar trebui, de asemenea, să informeze persoanele vizate în legătură cu diferitele consecințe și efecte negative potențiale cu care acestea ar putea să se confrunte din cauza încălcării.

[10] De exemplu, un dispozitiv de distrugere a documentelor de clasa 2 la nivelul P-4 sau mai mult în clasificarea DIN 66399 pentru documente din hârtie.

Exemplu de garanții corespunzătoare care ar fi putut reduce riscurile dacă ar fi fost puse în aplicare în prealabil:

- O soluție de rezervă eficientă și sigură ar fi permis restabilirea datelor. Dacă ar fi fost disponibilă o copie de rezervă actualizată a datelor, nu ar fi avut loc încălcarea disponibilității și notificarea nu ar fi fost necesară.

Cazul 6. *Un operator de rețea de telefonie mobilă oferă posibilitatea creării unui cont online la care abonații se pot conecta și unde pot consulta facturile recente și activitatea desfășurată în cadrul contului. S-a descoperit accesul ilegal al unui site web la baza de date care stochează parolele. Partea terță a accesat datele de autentificare a utilizatorilor (numele de utilizator și parolele criptate prin funcția „MD5-hash", însă fără funcția „salt").*

Eventuale consecințe și efecte negative ale încălcării confidențialității:

- Partea terță poate să deducă parola și, prin urmare, să acceseze contul oricărui client deoarece dispune, de asemenea, de numele de utilizator ale acestora.
- Dat fiind că numeroase persoane folosesc același nume de utilizator și aceeași parolă pentru mai multe conturi online, este probabil ca partea terță să aibă acces la alte conturi ale unora dintre persoanele vizate în cauză, inclusiv conturi de e-mail, în unele cazuri.

Deoarece parolele au fost criptate utilizând numai funcția „hash", acestea nu pot fi considerate neinteligibile în sensul articolului 4 alineatul (2) din Regulamentul (UE) nr. 611/2013 al Comisiei[11]. Astfel, scutirea de la notificarea persoanelor vizate nu se aplică.

Întrucât situația este susceptibilă a afecta în mod negativ persoana vizată și scutirea nu se aplică, încălcarea trebuie să fie comunicată clienților afectați, împreună cu o recomandare clară pentru utilizator de a-și modifica parola în toate conturile care au aceeași parolă compromisă. În orice caz, toți utilizatorii ar trebuie să fie obligați să își modifice parola — utilizând o metodă sigură — atunci când încearcă să aibă acces la serviciu.

Exemplu de garanții corespunzătoare care ar fi putut reduce riscurile dacă ar fi fost puse în aplicare în prealabil:

- Dacă parolele ar fi fost stocate în siguranță (criptate prin funcțiile „hash" și „salt" printr-o funcție „hash" de ultimă generație și o cheie sau un element „salt"), efectele negative asupra persoanelor vizate s-ar fi redus considerabil. Cu toate

[11] Articolul 4 alineatul (2) prevede următoarele:

Datele sunt considerate neinteligibile dacă:

(a) au fost criptate în mod sigur cu un algoritm standardizat, iar cheia folosită pentru decriptarea datelor nu a fost compromisă prin nicio încălcare a securității și a fost generată în așa fel încât să nu poată fi identificată prin mijloacele tehnologice disponibile de nicio persoană care nu este autorizată să o acceseze; sau

(b) au fost înlocuite cu valoarea algoritmului de criptare (hash) calculată cu o funcție hash standardizată cu cheie criptografică, cheia folosită pentru criptarea (hashing-ul) datelor nu a fost compromisă prin nicio încălcare a securității și a fost generată în așa fel încât să nu poată fi identificată prin mijloacele tehnologice disponibile de nicio persoană care nu este autorizată să o acceseze.

acestea, persoanele cu un nivel scăzut de securitate a parolei se pot afla în continuare în situații de risc, în special în cazul în care acestea utilizează aceleași date de acces și pentru alte servicii online.

Cazul 7. *Un furnizor de servicii de internet oferă abonaților posibilitatea de a consulta detaliile contului lor, istoricul utilizării internetului, inclusiv lărgimea benzii și domeniile vizitate frecvent. Din cauza unei erori de codificare a site-ului, identificatorii de acces ai utilizatorului nu sunt validați și datele sunt accesibile prin alterarea valorii de identificare a abonatului prezentată în parametrii URL-ului. Detaliile conturilor tuturor clienților pot fi accesate prin identificarea ciclurilor de coduri de identificare consecutive ale abonaților.*

Eventuale consecințe și efecte negative ale încălcării confidențialității:

- Datele pot fi utilizate pentru „spamming"-ul persoanelor vizate prin e-mail sau telefon.
- Datele pot oferi un profil al abonatului și pot divulga detalii privind comportamentul acestuia, putând expune informații sensibile. Aceasta ar putea avea un impact asupra mediului profesional sau familial al persoanelor vizate.

Încălcarea este susceptibilă să aibă consecințe negative asupra persoanei vizate, prin urmare, aceasta ar trebui să fie adusă la cunoștința clienților.

Exemplu de garanții corespunzătoare care ar fi putut reduce riscurile dacă ar fi fost puse în aplicare în prealabil:

- Monitorizarea posibilelor aspecte vulnerabile ale tehnologiilor utilizate, astfel cum s-a explicat în cazul 2, precum și testele efectuate pe o platformă de preproducție înainte de implementare și revizuirea codului ar fi permis să se evite încălcarea.

3. Scenarii posibile în care notificarea persoanelor vizate nu este necesară

În timp ce evaluarea consecințelor unei încălcări a securității datelor cu caracter personal trebuie să se realizeze de la caz la caz, pentru a lua în considerare în mod adecvat toate elementele în evaluarea posibilelor efecte negative asupra persoanelor vizate, ca orientare generală și în completarea scutirilor descrise în secțiunea anterioară, operatorul poate, de asemenea, să considere că notificarea persoanelor vizate nu este necesară în anumite cazuri specifice.

Astfel de situații pot include:

- O încălcare a securității datelor cu caracter personal care se referă doar la confidențialitate, în cazul în care datele au fost criptate în mod sigur cu un algoritm de ultimă generație, cheia pentru decriptarea datelor nu a fost compromisă prin nicio încălcare a securității și a fost generată astfel încât să nu poată fi identificată prin

mijloacele tehnologice disponibile de nicio persoană care nu este autorizată să o acceseze. Într-adevăr, aceste măsuri garantează că datele devin neinteligibile pentru persoanele care nu sunt autorizate să le acceseze.

- Datele, de exemplu parolele, au fost criptate în mod securizat prin funcțiile „hash" și „salt". Valoarea algoritmului de criptare („hash") a fost calculată cu o funcție „hash" de ultimă generație cu cheie criptografică, iar cheia folosită pentru criptarea („hashing-ul") datelor nu a fost compromisă prin nicio încălcare a securității și a fost generată astfel încât să nu poată fi identificată prin mijloacele tehnologice disponibile de nicio persoană care nu este autorizată să o acceseze.

4. Întrebări frecvente și răspunsuri

Când nu este obligatorie notificarea persoanelor vizate?

- Atunci când încălcarea securității nu constituie o încălcare a securității datelor cu caracter personal (a se vedea întrebarea următoare).
- Ori de câte ori nu este probabil ca încălcarea securității datelor cu caracter personal să afecteze negativ datele cu caracter personal sau viața privată a persoanei vizate, în conformitate cu rezultatele unei evaluării a gravității, cu aprobarea autorității competente.
- În cazul în care prestatorul a demonstrat autorității competente, într-un mod pe care aceasta îl consideră satisfăcător, că a pus în aplicare măsuri tehnologice adecvate de protecție și că măsurile respective au fost aplicate datelor afectate de încălcarea securității. De exemplu, în cazul în care o încălcare a securității datelor cu caracter personal (în ceea ce privește doar confidențialitatea) nu se referă decât la datele criptate cu un algoritm de ultimă generație sau la datele criptate prin „salt"/„hash" cu ajutorul unei funcții „hash" de ultimă generație și în cazul în care toate cheile și elementele „salt" de securitate relevante nu au fost compromise.
- Notificarea încălcărilor securității datelor, astfel cum este descrisă în prezentul aviz, constituie o bună practică pentru toți operatorii de date, inclusiv în cazul în care notificarea nu este obligatorie.

În ce situație o încălcare a securității devine o încălcare a securității datelor cu caracter personal?

O încălcare a securității constituie o încălcare a securității datelor cu caracter personal atunci când sunt vizate date cu caracter personal, astfel cum sunt definite la articolul 2 litera (a) din Directiva 95/46/CE: *„date cu caracter personal" înseamnă orice informație cu referitoare la o persoană fizică identificată sau identificabilă (persoana vizată); o persoană identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un număr de identificare sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, psihice, economice, culturale sau sociale.*

Avizul 4/2007 precizează că este vorba despre date referitoare la o persoană: „O persoană poate fi identificată direct prin nume sau indirect printr-un număr de telefon, un număr de înmatriculare al autovehiculului, un număr de securitate socială, număr de pașaport sau printr-o combinație de criterii semnificative care îi permite să fie recunoscut prin restrângerea grupului căruia îi aparține (vârsta, ocupația, locul de reședință etc.)". Orientări suplimentare privind acest aspect sunt disponibile în avizul 4/2007.

Ar trebui să se țină seama de efectele secundare probabile?

Da, încălcarea securității datelor ar trebui să fie comunicată persoanelor vizate în cazul în care este probabil ca încălcarea să afecteze negativ datele cu caracter personal sau viața privată a persoanelor vizate.
Astfel, ar trebui să fie luate în considerare toate eventualele consecințe și efecte negative asupra persoanelor vizate.

> ***Exemplul 1:*** *Site-ul internet al unei societăți de spectacole muzicale este atacat de hackeri și baza de date a utilizatorilor este furată și publicată pe internet. Datele cu caracter personal care au devenit publice sunt numele/prenumele, preferințele muzicale, precum și numele de utilizator și parolele utilizatorilor înregistrați pe site-ul internet al societății. 9 000 de utilizatori au fost afectați.*

În cazul acestei încălcări, efectul negativ direct asupra persoanelor vizate ar putea să pară destul de limitat în majoritatea cazurilor (de exemplu, compromiterea securității informațiilor privind preferințele muzicale) și poate conduce la întrebarea dacă ar trebuie să fie sau nu informate persoanele vizate. Cu toate acestea, întrucât parolele au fost compromise, acestea vor trebui să fie reînnoite de către operatorul de date. În acest proces, operatorul va trebui să informeze utilizatorii cu privire la motivele pentru care sunt reînnoite parolele. De asemenea, întrucât mulți utilizatori folosesc aceeași parolă pentru diferite conturi[12], este probabil, de asemenea, ca încălcarea să implice, ca efect negativ secundar, o încălcare a confidențialității altor conturi. Persoana vizată va avea posibilitatea de a reduce la minim astfel de efecte secundare prin schimbarea parolelor tuturor celorlalte conturi. Prin urmare, notificarea ar trebui să conțină, de asemenea, informații privind efectele negative probabile referitoare la alte conturi și ar trebui să includă, în consecință, o recomandare de a utiliza parole diferite pe diferite site-uri și de a reînnoi parolele oricăror conturi accesate cu ajutorul parolei compromise.

> ***Exemplul 2:*** *Un al doilea exemplu poate fi situația în care o probă într-o cauză penală privind o persoană a fost trimisă pe un CD unui avocat prin poștă, cu confirmare de primire, însă CD-ul este pierdut la poștă.*

Încălcarea directă este o încălcare a disponibilității. Situația poate avea un impact neglijabil sau foarte ridicat asupra persoanei (persoanelor) implicate, în funcție de posibilitatea de a lua sau nu măsuri adecvate în timp util.
Cu toate acestea, un efect negativ secundar este probabil să se materializeze dacă CD-ul este trimis fără protecție adecvată și datele sunt accesate. Într-adevăr, persoana în cauză poate să consulte datele, să le vândă jurnaliștilor etc. Un astfel de efect secundar poate avea un impact foarte ridicat asupra persoanei (persoanelor) vizate.

În acest caz, dacă CD-ul poate fi retrimis la timp, impactul direct asupra persoanei vizate ar fi neglijabil și nu ar trebui să se notifice persoanele, în timp ce încălcarea secundară potențială poate avea un impact foarte ridicat și ar face necesară, cu siguranță, notificarea persoanelor vizate.

[12] Conform unor studii recente, între 55 % și 80 % din utilizatorii internetului folosesc aceeași parolă pentru mai multe conturi.

Dacă este vizată o singură persoană, este necesar să se notifice persoana respectivă?

Da, Directiva 2002/58/CE nu stabilește un număr minim de persoane vizate afectate de o încălcare a securității datelor pentru ca obligația de notificare să intre în vigoare. Directiva privind telecomunicațiile prevede la articolul 3 (alineatul) 1: *„Atunci când încălcarea securității datelor cu caracter personal ar putea afecta negativ datele cu caracter personal sau viața privată a unui abonat sau a unei persoane, prestatorul trebuie, pe lângă notificarea menționată la articolul 2, să notifice respectiva încălcare abonatului sau persoanei în cauză”*.

Prin urmare, operatorul ar trebui să efectueze notificarea, în funcție de efectele negative posibile, indiferent de numărul persoanelor vizate în cauză.

Cum trebuie tratate datele care este probabil să fie publice?

Două aspecte trebuie luate în considerare.

1. „Public” poate implica diferite niveluri de disponibilitate: datele pot fi disponibile gratuit pe internet, disponibile public în cadrul unui serviciu cu abonament, disponibile public offline la cerere etc.
   De exemplu, în Franța, listele electorale sunt afișate pe pereții primăriei orașului în timpul alegerilor, putând fi obținute de orice alegător sau orice partid politic, dar publicarea pe internet a listelor respective nu este permisă de lege.
   Astfel, trimiterea accidentală a versiunii electronice a listelor unui alegător eronat sau pierderea versiunii pe hârtie a listei nu ar constitui o încălcare a confidențialității, în timp ce publicarea pe internet a listei ar fi o încălcare și ar trebui să fie notificată în consecință.

2. Unele date pot fi publice pentru anumite persoane vizate și nu pot fi publice pentru altele.
   De exemplu, o listă de numere de telefon aferente unui nume de familie poate conține atât numere de telefon aflate la dispoziția publicului în cartea de telefon, cât și numere neincluse în cărțile de telefon.

În concluzie, ori de câte ori nivelul de disponibilitate sau de accesibilitate publică a datelor este modificat printr-o încălcare, aceasta ar trebui să fie considerată o încălcare a confidențialității și ar trebui să fie notificată (dacă încălcarea este susceptibilă să afecteze negativ persoanele vizate).

Cum se poate face notificarea atunci când datele de contact ale persoanelor afectate sunt insuficiente sau necunoscute?

Există cazuri în care prestatorul, deși are o relație contractuală directă cu utilizatorul final, nu dispune de suficiente detalii pentru a asigura o notificare corespunzătoare. În acest sens, chiar dacă se ia în considerare posibilitatea de a realiza notificarea prin anunțuri în mass-media,

obligația de a efectua notificări individuale prin depunerea tuturor eforturilor necesare rezonabile rămâne valabilă[13].

Deși obligația de a depune eforturile rezonabile revine furnizorului prin punerea în aplicare a tuturor mecanismelor rezonabile pentru a se asigura că toate persoanele vizate sunt informate cu privire la încălcare, aceasta nu exclude, cu toate acestea, posibilitatea de a solicita sprijin din partea altor furnizori sau operatori care dețin datele de contact. Astfel, având în vedere cazul 4, operatorul care nu avea datele de contact ale posesorilor de cărți de credit afectați putea să raporteze agentul de plată intermediar, care putea cu ușurință să contacteze persoanele vizate. Alte cazuri pot necesita colaborarea autorităților competente, cărora, în orice caz, ar trebui să li se aducă la cunoștință faptul că prestatorul nu poate garanta notificări individuale.

Este necesar să se notifice persoanele vizate care nu au fost afectate de încălcare?

Nu, cu condiția să se poată stabili cu certitudine persoanele vizate care nu au fost afectate de încălcare. De exemplu, dacă poate fi demonstrat că un subset de persoane vizate nu a fost afectat de incidentul de securitate, atunci nu este necesar ca respectivele persoane vizate să fie notificate. Cu toate acestea, operatorul trebuie să ia în considerare toate efectele negative probabile în luarea unei astfel de decizii. În funcție de natura încălcării, neprimirea unei notificări poate, de asemenea, să provoace neliniște anumitor persoane.

[13] În conformitate cu articolul 3 alineatul (7) din Regulamentul (UE) nr. 611/2013, atunci când furnizorul, în ciuda faptului că a depus eforturi rezonabile, nu este în măsură să identifice toate persoanele care riscă să fie afectate negativ de încălcarea securității datelor cu caracter personal, furnizorul de servicii va notifica aceste persoane prin anunțuri în mass-media națională sau regională de mare anvergură în statele membre în cauză, în termenul aplicabil. În aceeași ordine de idei, se afirmă că prestatorul continuă să depună toate eforturile rezonabile pentru a identifica persoanele respective și pentru a le notifica în cel mai scurt timp posibil.