

Politica privind managementul incidentelor de securitate

1. Introducere

Această politică este destinată a fi utilizată atunci când a avut loc un incident de securitate care a avut ca rezultat sau există bănueli că a dus la pierderea datelor personale pe care organizația le prelucrează.

O cerință a Regulamentului (UE) 679/2016 (Regulamentul GDPR) este ca incidentele de securitate cu privire datele cu caracter personal care pot avea un risc pentru drepturile și libertățile persoanelor vizate trebuie raportate Autorității de Supraveghere (ANSPDCP) fără întârzieri nejustificate, în termen de 72 de ore de la conștientizarea acestora. În cazul în care notificarea nu poate fi făcută în 72 ore trebuie să se motiveze întârzierea. Acest document se folosește împreună cu șablonul pentru notificarea către ANSPDCP.

În cazul în care un incident afectează datele cu caracter personal, trebuie luată o decizie dacă incidentul poate conduce la un risc asupra drepturilor și libertăților persoanei fizice vizate. Regulamentul GDPR impune ca notificarea să aibă loc „fără întârzieri nejustificate” dacă încălcarea este susceptibilă să genereze „un risc ridicat pentru drepturile și libertățile persoanelor fizice”.

Acțiunile stabilite în acest document ar trebui utilizate numai ca îndrumare atunci când se va răspunde la un incident. Natura exactă a unui incident și impactul acestuia nu pot fi prezise cu niciun grad de certitudine și, prin urmare, este important să se utilizeze o atenție deosebită atunci când se decide ce acțiuni vor fi întreprinse. Cu toate acestea, etapele prezentate sunt utile pentru ca instituția să se asigure că obligațiile cu privire la incidentele de Securitate din cadrul Regulamentului GDPR sunt îndeplinite.

2. Procedura de notificare a incidentelor de securitate

Odată ce s-a hotărât că a avut loc un incident de securitate asupra datelor cu caracter personal, există două entități cu privire la care trebuie luată decizia dacă vor fi notificate sau nu. Acestea sunt:

1. Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP);
2. Persoanele vizate afectate.

Nu întotdeauna un incident de securitate trebuie notificat, ci doar în situația în care incidentul prezintă un risc pentru „*drepturile și libertățile persoanelor fizice*” (**articolul 33 din Regulamentul GDPR**).

Următoarele secțiuni descriu modul în care trebuie luată această decizie și ce trebuie făcut în cazul în care este necesară notificarea.

2.2. Decidem dacă vom notifica ANSPDCP sau nu

Regulamentul GDPR prevede că o încălcare a securității datelor cu caracter personal va fi notificată Autorității de Supraveghere „cu excepția cazului în care este puțin probabil ca încălcarea securității datelor cu caracter personal să ducă la un risc pentru drepturile și libertățile persoanelor fizice” (**articolul 33 din Regulamentul GDPR**). Acest lucru presupune ca organizația să evalueze nivelul riscului înainte de a decide dacă trebuie sau nu să notifice.

Factorii care trebuie luați în considerare ca parte a acestei evaluări a riscurilor ar trebui să includă:

- Datele personale au fost criptate;
- Dacă au fost criptate, cât de înalt a fost nivelul de criptare;
- În ce măsură datele au fost pseudonimizate (adică dacă persoanele pot fi, în mod rezonabil, identificate din date);
- Categoriile de date afectate (de exemplu nume, adresă, detalii bancare, date biometrice) și dacă au fost afectate categorii speciale de date;
- Volumul de date afectate;
- Numărul persoanelor vizate afectate;
- Natura incidentului (furt, pierderea unui laptop, distrugerea accidentală);
- Orice alți factori care sunt considerați relevanți.

Persoanele implicate în această evaluare a riscurilor ar trebui să includă persoane din următoarele departamente: Conducere, IT, Juridic, Responsabilul cu Protecția Datelor (DPO).

Metoda de evaluare a riscurilor, raționamentul și concluziile sale ar trebui să fie pe deplin documentate și semnate de conducere. Rezultatul evaluării riscurilor ar trebui să includă una dintre următoarele concluzii:

1. Încălcarea datelor cu caracter personal nu necesită notificare;
2. Încălcarea datelor cu caracter personal necesită doar notificarea către Autoritatea de Supraveghere (ANSPDCP);
3. Încălcarea datelor cu caracter personal necesită notificarea atât Autorității de Supraveghere (ANSPDCP), cât și persoanelor vizate.

Aceste concluzii pot fi supuse schimbării bazate pe feedbackul Autorității de Supraveghere (ANSPDCP) sau ulterior, ca urmare a descoperirii a altor informații suplimentare din care rezultă că impactul este grav și incidentul prezintă un risc asupra persoanelor fizice.

2.3. Cum notificăm Autoritatea de Supraveghere

În cazul în care se decide să se realizeze notificarea către Autoritatea de Supraveghere, o cerință a Regulamentului GDPR este ca incidente de securitate cu privire la datele cu

caracter personal care pot avea un risc pentru drepturile și libertățile persoanelor vizate trebuie raportate Autorității de Supraveghere (ANSPDCP) fără întârzieri nejustificate, în termen de **72 de ore de la conștientizarea acestora**. În cazul în care notificarea nu poate fi făcută în 72 ore trebuie să se motiveze întârzierea.

Notificarea se va realiza la adresa de e-mail brese@dataprotection.ro, cu excepția cazului în care ANSPDCP va indica o altă modalitate pentru transmiterea notificării.

Notificarea va cuprinde, cel puțin, următoarele:

- (a) 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) 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) consecințele probabile ale încălcării securității datelor cu caracter personal;
- (d) 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.

Se va utiliza formularul de notificare furnizat sau, în situația în care ANSPDCP va furniza un model de formular, acesta din urmă. De asemenea, există un formular de notificare online, disponibil la adresa <http://www.dataprotection.ro/servlet/ViewDocument?id=1100>, însă el nu este adaptat la cerințele Regulamentului GDPR.

2.4. Decidem dacă vom notifica persoanele vizate sau nu

Regulamentul GDPR afirmă „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.”

Prin urmare, notificarea ANSPDCP se va face atunci când incidentul de securitate prezintă un risc, iar notificarea persoanelor vizate se va realiza atunci când incidentul prezintă un **risc ridicat**.

Factorii care trebuie luați în considerare ca parte a acestei evaluări a riscurilor ar trebui să includă:

- Datele personale au fost criptate;
- Dacă au fost criptate, cât de înalt a fost nivelul de criptare;
- În ce măsură datele au fost pseudonimizate (adică dacă persoanele pot fi, în mod rezonabil, identificate din date);
- Categoriile de date afectate (de exemplu nume, adresă, detalii bancare, date biometrice) și dacă au fost afectate categorii speciale de date;
- Volumul de date afectate;

- Numărul persoanelor vizate afectate;
- Natura incidentului (furt, pierderea unui laptop, distrugerea accidentală);
- Orice alți factori care sunt considerați relevanți.

Persoanele implicate în această evaluare a riscurilor ar trebui să includă persoane din următoarele departamente: Conducere, IT, Juridic, Responsabilul cu Protecția Datelor (DPO).

Aceste concluzii pot fi supuse schimbării bazate pe feedbackul Autorității de Supraveghere (ANSPDCP) sau ulterior, ca urmare a descoperirii a altor informații suplimentare din care rezultă că impactul este grav și incidentul prezintă un risc ridicat asupra persoanelor fizice.

Notificarea persoanelor vizate nu este obligatorie în situația în care ar necesita „eforturi disproporționate” din partea operatorului.

2.5. Cum notificăm persoanele vizate

Odată ce s-a decis că trebuie notificate persoanele vizate Regulamentul GDPR cere ca acest lucru să se facă fără întârzieri nejustificate.

Comunicarea către persoanele vizate afectate va descrie în limbaj simplu și clar natura încălcării securității datelor cu caracter personal (**articolul 34 din Regulamentul GDPR**) și trebuie să cuprindă și:

- (a) numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;
- (b) consecințele probabile ale încălcării securității datelor cu caracter personal;
- (c) 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.

În plus față de punctele solicitate de Regulamentul GDPR, ar putea fi oportun să se ofere ajutor persoanei vizate cu privire la acțiunile pe care acestea le pot lua pentru a reduce riscurile asociate cu încălcarea securității datelor cu caracter personal.

În majoritatea cazurilor, este oportună notificarea persoanelor vizate afectate prin poștă, e-mail sau ambele, pentru a se asigura că mesajul a fost primit și că au posibilitatea de a lua orice acțiune necesară.

3. Consecințe

Nerespectarea prezentei Politici de către angajații instituției sau alți colaboratori externi poate conduce către sancțiuni disciplinare (inclusiv încetarea contractului de muncă), rezilierea contractelor și, în funcție de circumstanțe, acționarea în instanță pentru recuperarea integrală a prejudiciilor aduse Instituției ca urmare a nerespectării prezentei Politici. Când există suspiciunea unor activități ilegale (cum ar fi, exemplificativ, sustragerea documentelor, copierea, distribuirea, transferul bazelor de date), Instituția va denunța activitatea infracțională organelor legii pentru tragerea la răspundere penală a făptuitorului.

Prezenta Politică va fi adusă de către conducerea Instituției la cunoștința tuturor angajaților, colaboratorilor sau a altor terți.