Primăria COMUNEI RACOVA

Politica privind managementul incidentelor de securitate

Primăria COMUNEI RACOVA a întocmit politica privind managementul incidentelor de securitate pentru a fi utilizată în situațiile unui eventual incident de securitate care ar putea avea ca rezultat sau ar putea există bănuieli că ar duce la pierderea datelor personale care sunt prelucrate.

Art. 33 al Regulamentului nr. 679 din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46 CE (denumit în continuare RGPD) impune ca incidentele de securitate cu privire datele cu caracter personal care pot avea un risc pentru drepturile și libertățile persoanelor vizate să fie 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.

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. RGPD 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, iar prin urmare este important să se utilizeze o atenție deosebită atunci când se decide ce acțiuni vor fi întreprinse.

1. Procedura de notificare a incidentelor de securitate

Imediat ce s-a constatat că a avut loc un incident de securitate asupra datelor cu caracter personal, conform RGPD, COMUNEI RACOVA va notifica de urgență următoarele entități: Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), persoanele vizate afectate de incidentul de securitate constatat.

Incidentele de securitate se vor notifica, doar în cazurile în care incidentele prezintă un risc pentru „drepturile și libertățile persoanelor fizice" conform articolului 33 din RGPD.

2. Decizia de a notifica ANSPDCP

Primăria COMUNEI RACOVA evaluează nivelul riscului înainte de a decide dacă trebuie sau nu să notifice Autoritatea de Supraveghere conform articolului 33 din RGPD, care 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".

Se iau în considerare următorii factori ca parte a acestei evaluări a riscurilor care 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: Management, 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:

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

Aceste concluzii pot fi supuse schimbării bazate pe îndrumările 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.

3. Modalitatea de notificare a Autorității de Supraveghere

În cazul în care **Primăria COMUNEI RACOVA** va decide să se realizeze notificarea către Autoritatea de Supraveghere, va respecta cerința RGPD și va raporta incidentele de securitate cu privire la datele cu caracter personal care pot avea un risc pentru drepturile și libertățile persoanelor Autorității de Supraveghere (ANSPDCP) fără întârzieri nejustificate, în termen de 72 de ore de la conștientizarea acestora. În cazul în care Primăria Comuna BUHOCI nu va putea notifica ANSPDCP în termen de 72 ore trebuie să se motiveze întârzierea.

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

Conform art. 33 alin. (3) notificarea va cuprinde, cel puțin, următoarele:

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

Pentru notificare se va utiliza formularul de notificare furnizat de către ANSPDCP „Formularul de Notificare Breșa ANSPDCP” disponibil pe portalul de internet www.dataprotection.ro

4. Decizia notificării persoanelor vizate

Primăria Comuna RACOVA se va conforma RGPD în cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul informând persoana vizată fără întârzieri nejustificate cu privire la această încălcare.

Așadar se va notifica ANSPDCP atunci când incidentul de securitate prezintă un risc, iar notificarea persoanelor vizate se va realiza atunci când incidentul prezintă un risc ridicat.

Factorii luați în considerare ca parte a acestei evaluări a riscurilor trebuie 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: Management, IT, Juridic, Responsabilul cu Protecția Datelor (DPO).

Aceste concluzii pot fi supuse schimbării bazate pe îndrumările 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.

5. Modalitatea de notificare a persoanelor vizate

Primăria COMUNEI RACOVA va comunica fără întârziere către persoanele vizate afectate și va descrie în limbaj simplu și clar natura încălcării securității datelor cu caracter personal, conform articolului 34 din RGPD, notificare ce va cuprinde următoarele:

- numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;
- consecințele probabile ale încălcării securității datelor cu caracter personal;
- 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 cerințele solicitate de RGPD, **Primăria COMUNEI RACOVA** va oferi 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 toate cazurile, **Primăria COMUNEI RACOVA** va notifica persoanele 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.

În funcție de modificările aduse de legislație, precum și de îmbunătățirea continuă a procedurilor, a măsurilor de securitate asupra infrastructurii IT, **Primăria COMUNEI RACOVA** va actualiza politica privind managementul incidentelor de securitate, în situația în care modificările aduse vor fi substanțiale.

Modificarea politicii privind managementul incidentelor de securitate, va fi publică și comunicată către persoanele direct implicate la solicitările acestora. Fiecare actualizare a politicii privind managementul incidentelor de securitate, va fi indexată prin numerotarea documentului, acest lucru verificând-se în partea inferioară a documentului publicat.

Nerespectarea prezentei politici de către angajații **Primăria COMUNEI RACOVA** 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 sustragerea documentelor, copierea, distribuirea, transferul bazelor de date sau accesarea neautorizată ori compromiterea sistemelor informatice), **Primăria COMUNEI RACOVA** va denunța activitatea infracțională organelor legii pentru tragerea la răspundere penală a făptuitorului.

Prezenta politică va fi adusă de către conducerea **Primăria COMUNEI RACOVA** la cunoștința tuturor angajaților, colaboratorilor, instituțiilor partenere sau a altor terți.

Întocmit,
Consilier Superior

Aprobat,
Primar