

PROCEDURĂ PENTRU PROTECȚIA DATELOR CU CARACTER PERSONAL

PROCEDURĂ PENTRU PROTECȚIA PERSOANELOR CU PRIVIRE LA PRELUCRAREA DATELOR CU CARACTER PERSONAL ȘI LIBERA CIRCULAȚIE A ACESTOR DATE LA NIVELUL PRIMĂRIEI COMUNEI PĂULEȘTI, JUDEȚUL PRAHOVA

Scopul

Scopul acestei proceduri este de a garanta și proteja drepturile și libertățile fundamentale ale persoanelor fizice, în special a dreptului la viața intimă, familială și privată, cu privire la prelucrarea datelor cu caracter personal.

I. REGULI GENERALE

Art. 1. Prezenta procedură stabilește măsuri tehnice și organizatorice pentru îndeplinirea obligațiilor referitoare la securitatea și controlul sistemelor informatice, în vederea asigurării confidențialității datelor și informațiilor precum și pentru păstrarea în siguranță a acestora, în cadrul activității curente executate de angajații PRIMĂRIEI COMUNEI PĂULEȘTI din Județul Prahova. Prin cerințe minime de securitate este avut în vedere un complex de măsuri tehnice, informatice, organizatorice, logistice, proceduri și politici de securitate prin care să se asigure nivelul minim de securitate prevăzut în Regulamentul (UE) 2016/679 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 (Regulamentul general privind protecția datelor RGPD 2018).

Art. 2. PRIMĂRIA COMUNEI PĂULEȘTI adoptă măsuri tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerilor accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat. În acest sens a fost desemnată persoana responsabilă cu protecția datelor cu caracter personal la nivelul Primăriei Comunei Păulești.

Art. 3. PRIMĂRIA COMUNEI PĂULEȘTI ia măsuri de stocare în siguranță a informațiilor, astfel încât să fie asigurat un nivel adecvat de protecție și securitate, în sensul Regulamentului (UE) 2016/679.

Art.4. Pentru îndeplinirea prevederilor legale aferente și în vederea satisfacerii cerințelor păstrării în siguranță a datelor și informațiilor, PRIMĂRIA COMUNEI PĂULEȘTI elaborează și implementează măsuri organizatorice și tehnice orientate pe anumite direcții de acțiune:

- Identificarea și autentificarea utilizatorului
- Tipul de acces
- Colectarea datelor
- Execuția copiilor de siguranță
- Computerele și terminalele de acces
- Fișierele de acces
- Instruirea personalului

II. PROCEDURI SPECIFICE

Art. 5. IDENTIFICAREA ȘI AUTENTIFICAREA UTILIZATORULUI

Prin utilizator se înțelege orice persoană care acționează sub autoritatea operatorului, a persoanei împuternicite sau a reprezentantului, cu drept recunoscut de acces la bazele de date cu caracter personal.

Utilizatorii, pentru a căpăta acces la o bază de date cu caracter personal, trebuie să se identifice. Identificarea în cadrul PRIMĂRIA COMUNEI PĂULEȘTI se face prin introducerea codului de identificare de la tastatură (un șir de caractere).

Fiecare utilizator are propriul său cod de identificare. Niciodată nu este alocat același cod de indentificare mai multor utilizatori.

Codurile de identificare (sau conturi de utilizator) nefolosite o perioadă mai îndelungată sunt dezactivate și distruse după un control prealabil intern al operatorului. Perioada după care codurile trebuie dezactivate și distruse este stabilită prin proceduri interne de operator.

Orice cont de utilizator este însoțit de o modalitate de autentificare. Autentificarea se face prin introducerea unei parole.

Parolele sunt șiruri de caractere, adecvate din punct de vedere al securității ca lungime și compoziție. La introducerea parolelor acestea nu sunt afișate în clar pe monitor. Parolele sunt schimbate periodic în funcție de politicile de securitate ale operatorului. Schimbarea periodică a parolelor se face numai de către utilizatori autorizați de operator.

Operatorul are implementate un sistem informațional care refuză automat accesul unui utilizator după un număr de introduceri greșite ale parolei.

Orice utilizator care primește un cod de identificare și un mijloc de autentificare este obligat prin fișa postului să păstreze confidențialitatea acestora și să răspundă în acest sens în fața operatorului.

Este stabilită o procedură proprie de administrare și gestionare a conturilor de utilizator.

Accesul utilizatorilor la bazele de date cu caracter personal efectuate manual se face numai pe baza unei liste aprobate de conducerea instituției.

Art. 6. TIPUL DE ACCES

Utilizatorii pot accesa numai datele cu caracter personal necesare pentru îndeplinirea atribuțiilor lor de serviciu. Pentru aceasta sunt stabile tipurile de acces după funcționalitate (administrare, introducere, prelucrare, salvare etc.) și după acțiuni aplicate asupra datelor cu caracter personal (scriere, citire, ștergere), precum și procedurile privind aceste tipuri de acces. Programatorii sistemelor de prelucrare a datelor cu caracter personal nu au acces la datele cu caracter personal. Operatorul permite accesul programatorilor la datele cu caracter personal numai după ce acestea au fost transformate în date anonime.

Compartimentul/contractorul care asigură suportul tehnic poate avea acces la datele cu caracter personal pentru rezolvarea unor cazuri excepționale.

Alte măsuri specifice implementate de control al accesului sunt:

- în spațiile destinate desfășurării activității instituției sunt instalate sisteme de alarmă antiefracție ;
- în spațiul aferent intrării în cadrul instituției sunt instalate sisteme de supraveghere video;
- monitorizarea și intervenția în caz de alarmă este asigurată de o firmă de protecție și pază.

Art. 7. COLECTAREA DATELOR

Operatorul desemnează utilizatori autorizați pentru operațiile de colectare și introducere de date cu caracter personal într-un sistem informațional.

Orice modificare a datelor cu caracter personal se poate face numai de către utilizatori autorizați desemnați de operator.

Operatorul ia măsuri pentru ca sistemul informațional să înregistreze cine a făcut modificarea, data și ora modificării. Pentru o mai bună administrare operatorul are implementate măsuri ca sistemul informațional să mențină datele șterse sau modificate.

Art. 8. EXECUȚIA COPIILOR DE SIGURANȚĂ

Operatorul stabilește intervalul de timp la care se vor executa copiile de siguranță ale bazelor de date cu caracter personal, precum și ale programelor folosite pentru prelucrările automatizate. Utilizatorii care execută aceste copii de siguranță sunt numiți de operator, într-un număr restrâns. Copiile de siguranță se vor stoca în alte camere, în fișete metalice.

Operatorul ia măsuri ca accesul la copiile de siguranță să fie monitorizat.

Se generează zilnic de către sistemul informatic, în mod automat, un back-up pentru o eventuală recuperare a datelor, în cazul distrugerii sau disfuncționalității sistemelor informatice.

Art. 9. COMPUTERELE ȘI TERMINALELE DE ACCES

Computerele și alte terminale de acces sunt instalate în încăperi cu acces restricționat. Unde nu pot fi asigurate aceste condiții, computerele sunt instalate în încăperi care se pot încuia. Dacă pe ecran apar date cu caracter personal asupra cărora nu se acționează o perioadă dată, stabilită de operator, sesiunea de lucru se închide automat. Mărimea acestei perioade se determină în funcție de operațiile care trebuie executate.

Terminalele de acces folosite în relația cu publicul, pe care apar date cu caracter personal, vor fi poziționate astfel încât să nu poată fi văzute de public și după o perioadă scurtă, stabilită de operator, în care nu se acționează asupra lor, acestea trebuie ascunse.

Serverele care găzduiesc bazele de date pot fi accesate doar în mod controlat, pe baza de drepturi de acces; nu pot fi accesate din afara rețelei PRIMĂRIA COMUNEI PĂULEȘTI. Nu este permisă scoaterea din instituție a mediilor de stocare mobile (CD/DVD, USB Stick, Portable HDD), decât cu aprobare prealabilă din partea conducerii Primăriei.

Art. 10. FIȘIERELE DE ACCES

Operatorul ia măsuri ca orice accesare a bazei de date cu caracter personal să fie înregistrată într-un fișier de acces (numit log la prelucrările automate) sau într-un registru pentru prelucrările manuale de date cu caracter personal, stabilit de operator.

Informațiile înregistrate în fișierul de acces sau în registru vor fi:

- codul de identificare (numele utilizatorului pentru bazele de date cu caracter personal manuale);
- numele fișierului accesat (fișei);
- numărul înregistrărilor efectuate;
- tipul de acces;
- codul operației executate sau programul folosit;
- data accesului (an, lună, zi);
- timpul (ora, minutul, secunda).

Pentru prelucrările automate aceste informații vor fi stocate într-un fișier de acces general sau în fișiere separate pentru fiecare utilizator. Orice încercare de acces neautorizat va fi, de asemenea, înregistrată.

Operatorul este obligat să păstreze fișierele de acces cel puțin 2 ani, pentru a fi folosite ca probe în cazul unor investigații. Dacă investigațiile se prelungesc, aceste fișiere se vor păstra atât timp cât se va considera necesar.

Fișierele de acces trebuie să facă posibilă identificarea de către operator sau de către persoana împuternicită a persoanelor care au accesat date cu caracter personal fără un motiv anume, în vederea aplicării unor sancțiuni sau a sesizării organelor competente.

Art. 11. INSTRUIREA PERSONALULUI

Operatorul face informarea personalului cu privire la prevederile Regulamentului (UE) 2016/679 privind protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, la cerințele minime de securitate a prelucrărilor de date cu caracter personal, precum și cu privire la riscurile pe care le comportă prelucrarea datelor cu caracter personal, în funcție de specificul activității. Utilizatorii care au acces la date cu caracter personal sunt instruiți de către operator asupra confidențialității acestora și sunt avertizați prin mesaje care vor apărea pe monitoare în timpul activității.

