

CAPITOLUL IV¹

Măsuri de securitate în activitățile de prelucrare de date cu caracter personal

Art. 39¹. În activitățile de prelucrare de date cu caracter personal, desfășurate în conformitate cu Legea nr. 677/2001 de Poliția Comunitară Roman vor fi respectate următoarele condiții minime:

(1) **Identificarea și autentificarea utilizatorului** (persoanele care acționează sub autoritatea Municipiului Roman - Poliția Comunitară cu drept recunoscut de acces la bazele de date cu caracter personal):

a) pentru accesarea bazelor de date cu caracter personal, utilizatorii se vor identifica în sistem prin introducerea de la tastatură a unui nume de cont și un cod de identificare format dintr-un șir de 8 caractere (cifre și litere);

b) fiecare utilizator va avea propriul său cod de identificare;

c) conturile și codurile de identificare nefolosite mai mult de 10 zile calendaristice, precum și cele ale utilizatorilor care nu mai fac parte din Poliția Comunitară sau nu vor mai fi autorizați să opereze cu date cu caracter personal vor fi dezactivate și distruse după un control prealabil intern într-o perioadă de 20 de zile calendaristice;

d) la introducerea codurilor de identificare, acestea nu vor fi afișate în clar pe monitor;

e) codurile de identificare vor fi schimbate trimestrial (ziua 1 a fiecărui trimestru) de către un utilizator autorizat de conducerea Poliției Comunitare;

f) sistemul informatic de lucru se va autobloca și va refuza automat accesul în sistem a utilizatorilor care au introdus codul de identificare greșit de 5 ori consecutiv, concomitent cu transmiterea unui mesaj de avertizare către un număr de 3 conturi de mail (conducerea Primăriei și a Poliției Comunitare). Deblocarea sistemului va fi realizată de către un utilizator autorizat de conducerea Poliției Comunitare;

g) utilizatorii care au primit un cont și un cod de identificare vor păstra confidențialitatea acestora și vor răspunde atât în fața operatorului Municipiul Roman prin Poliția Comunitară, cât și în fața legilor în vigoare;

h) accesul la bazele de date cu caracter personal ce poate fi efectuat manual (fără interpunerea unui sistem informatic) se va face numai pe baza unei liste aprobate de conducerea Poliției Comunitare.

(2) Tipul de acces la bazele de date cu caracter personal

- a) utilizatorii vor accesa în numele operatorului numai datele cu caracter personal necesare îndeplinirii atribuțiilor de serviciu;
- b) programatorii sistemelor de prelucrare a datelor cu caracter personal nu vor avea acces la datele cu caracter personal;
- c) imaginile furnizate de sistemul de supraveghere video vor fi stocate o perioadă de 30 de zile după care vor fi distruse prin ștergere. Prin excepție, aceste imagini vor fi arhivate în format electronic (DVD) în situația când acestea urmează a fi predate autorităților competente;
- d) conducerea Poliției Comunitare va desemna prin decizie internă un număr de 2 utilizatori care răspund de stocarea, distrugerea sau arhivarea imaginilor video;

(3) Colectarea datelor

- a) colectarea, introducerea sau modificarea de date cu caracter personal în sistemul informatic al Poliției Comunitare va fi efectuată numai de utilizatori autorizați prin decizie internă de conducerea instituției;
- b) sistemul informatic la bazele de date cu caracter personal va înregistra automat data și ora modificărilor, utilizatorul care a operat modificările. În același timp, sistemul va păstra separat datele șterse sau modificate;

(4) Execuția copiilor de siguranță

- a) trimestrial vor fi efectuate copii de siguranță ale bazelor de date cu caracter personal, precum și ale programelor folosite pentru prelucrările automatizate de către 2 utilizatori desemnați prin decizie internă;
- b) copiile de siguranță vor fi păstrate în încăperi separate, în fișete metalice cu sigiliu aplicat. Accesul la aceste copii de siguranță va fi monitorizat;

(5) Computerele și terminalele de acces

- a) accesul în încăperile unde sunt instalate computere și alte terminale de acces va fi restricționat la utilizatorii autorizați. Accesul altor persoane va fi permis strict în prezența sau cu permisiunea în scris a conducerii Poliției Comunitare;

(6) Fișierele de acces

- a) orice accesare a bazelor de date cu caracter personal va fi înregistrată automat într-un fișier de acces general (.log) pentru toți utilizatorii. Informațiile înregistrate de acest fișier sunt: codul de identificare al utilizatorului, numele fișierului accesat, numărul înregistrărilor efectuate, tipul de acces, codul operației efectuate sau programul folosit, data și momentul accesului (an, luna, zi, ora, minutul, secunda);
- b) orice încercare de acces neautorizat în sistem va fi înregistrată și semnalată;
- c) fișierele de acces vor fi păstrate cel puțin doi ani după care vor fi distruse prin ștergere. În cazul derulării unor investigații, aceste fișiere vor fi păstrate cât timp va fi necesar;
- c) fișierele de acces vor face posibilă identificarea utilizatorilor care au accesat bazele de date cu caracter personal în afara atribuțiilor de serviciu. Identificarea unor astfel de accesări va conduce la aplicarea de sancțiuni sau la sesizarea organelor competente;

(7) Sistemele de comunicații

- a) conducerea Poliției Comunitare va efectua trimestrial controlul autentificărilor și a tipului de acces a utilizatorilor în sistemul informatic;
- b) sistemul de telecomunicații va fi securizat astfel încât datele cu caracter personal să nu poată fi interceptate sau transmise spre alte terminale;
- c) prin sistemele de comunicații se vor transmite numai datele cu caracter personal strict necesare;

(8) Instruirea personalului

- a) utilizatorii vor urma cursuri de pregătire în vederea operării în sistemul informatic. În cadrul acestor cursuri vor fi prelucrate prevederile Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, prevederile Ordinului nr. 52/2001 privind 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;
- b) utilizatorii sistemului de acces la bazele de date cu caracter personal vor fi instruiți asupra confidențialității acestor date;
- c) utilizatorii sunt obligați să închidă sesiunea de lucru cand părăsesc locul de muncă;

(9) Folosirea computerelor

- a) se interzice folosirea de către utilizatori a programelor software care provin din surse externe sau dubioase;
- b) protecția împotriva virusilor informatici sau împotriva unor eventuale atacuri informatice va fi realizată prin implementarea unor sisteme automate de devirusare și de securitate a sistemelor informatice;
- c) computerelor care au acces la bazele de date cu caracter personal le va fi dezactivată din „bios” tasta „Print Screen”, împiedicându-se astfel imprimarea acestor date;

(10) Imprimarea datelor

- a) imprimarea pe suport de hârtie sau electronic a datelor cu caracter personal se va realiza numai de anumiți utilizatori desemnați în acest sens prin decizie internă;

(11) În funcție de situațiile concrete impuse de procedura de lucru cu datele cu caracter personal, conducerea Poliției Comunitare poate decide și impune măsuri suplimentare de securitate.