

ORDIN nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal

Avocatul Poporului,

în temeiul Hotărârii Senatului României nr. 33 din 4 octombrie 2001 pentru numirea Avocatului Poporului, văzând prevederile art. 13 din Legea nr. 35/1997 privind organizarea și funcționarea instituției Avocatul Poporului și ale art. 7 din Regulamentul de organizare și funcționare a instituției Avocatul Poporului, în aplicarea prevederilor art. 20 alin. (2) din Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, conform cărora cerințele minime de securitate a prelucrărilor de date cu caracter personal vor fi elaborate de autoritatea de supraveghere și vor fi actualizate periodic, corespunzător progresului tehnic și experienței acumulate, având în vedere Nota privind cerințele minime de securitate a prelucrărilor de date cu caracter personal, înregistrată sub nr. 4.327 din 18 aprilie 2002, a adjunctului Avocatului Poporului, având în vedere exigența elaborării cerințelor minime de securitate a prelucrărilor de date cu caracter personal, care stau la baza adoptării de către operatorii de date cu caracter personal a măsurilor tehnice și organizatorice adecvate, prin care se garantează un nivel corespunzător și legal de securitate a prelucrării de date cu caracter personal, precum și a publicării cerințelor respective în Monitorul Oficial al României, Partea I, în scopul ca acestea să poată fi cunoscute în mod corespunzător de către operatorii menționați, emite prezentul ordin.

Art. 1

Se aprobă Cerințele minime de securitate a prelucrărilor de date cu caracter personal, prevăzute în anexa la prezentul ordin.

Art. 2

Prezentul ordin va fi publicat în Monitorul Oficial al României, Partea I.

Art. 3

- Anexa face parte integrantă din prezentul ordin.

..****..

AVOCATUL POPORULUI,

prof. univ dr. IOAN MURARU

ANEXĂ: CERINȚELE MINIME DE SECURITATE a prelucrărilor de date cu caracter personal

Prezentele cerințe minime de securitate a prelucrărilor de date cu caracter personal trebuie să stea la baza adoptării și implementării de către operator a măsurilor tehnice și organizatorice necesare pentru păstrarea confidențialității și integrității datelor cu caracter personal. În concordanță cu acestea operatorii își vor stabili propriile politici și proceduri de securitate.

Cerințele minime de securitate a prelucrărilor de date cu caracter personal acoperă următoarele aspecte:

1. 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 se poate face prin mai multe metode, cum ar fi: introducerea codului de identificare de la tastatură (un șir de caractere), folosirea unei cartele cu cod de bare, folosirea unei cartele inteligente (smart card) sau a unei cartele magnetice.

Fiecare utilizator are propriul său cod de identificare. Niciodată mai mulți utilizatori nu trebuie să aibă același cod de identificare.

Codurile de identificare (sau conturi de utilizator) nefolosite o perioadă mai îndelungată trebuie dezactivate și distruse după un control prealabil intern al operatorului. Perioada după care codurile trebuie dezactivate și distruse se stabilește de operator.

Orice cont de utilizator este însoțit de o modalitate de autentificare. Autentificarea poate fi făcută prin introducerea unei parole sau prin mijloace biometrice: amprenta dactiloscopică, amprenta vocală, angiografia retiniană etc.

Parolele sunt șiruri de caractere. Cu cât șirul de caractere este mai lung, cu atât parola este mai greu de aflat. La introducerea parolelor acestea nu trebuie să fie afișate în clar pe monitor. Parolele trebuie schimbate periodic în funcție de politicile de securitate ale entității (operator sau persoană împuternicită). Schimbarea periodică a parolelor se face numai de către utilizatori autorizați de operator.

Operatorul trebuie să solicite realizarea unui sistem informațional care să refuze automat accesul unui utilizator după 5 introduceri greșite ale parolei.

Orice utilizator care primește un cod de identificare și un mijloc de autentificare trebuie să păstreze confidențialitatea acestora și să răspundă în acest sens în fața operatorului.

Fiecare entitate va stabili o procedură proprie de administrare și gestionare a conturilor de utilizator.

Operatorii autorizează anumiți utilizatori pentru a revoca sau a suspenda un cod de identificare și autentificare, dacă utilizatorul acestora și-a dat demisia ori a fost concediat, și-a încheiat contractul, a fost transferat la alt serviciu și noile sarcini nu îi solicită accesul la date cu caracter personal, a abuzat de codurile primite sau dacă va absenta o perioadă îndelungată stabilită de entitate.

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

2. Tipul de acces

Utilizatorii trebuie să acceseze numai datele cu caracter personal necesare pentru îndeplinirea atribuțiilor lor de serviciu. Pentru aceasta operatorii trebuie să stabilească tipurile de acces după funcționalitate (cum ar fi: administrare, introducere, prelucrare, salvare etc.) și după acțiuni aplicate asupra datelor cu caracter personal (cum ar fi: scriere, citire, ștergere), precum și procedurile privind aceste tipuri de acces.

Programatorii sistemelor de prelucrare a datelor cu caracter personal nu vor avea acces la datele cu caracter personal. Operatorul va permite accesul programatorilor la datele cu caracter personal după ce acestea au fost transformate în date anonime.

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

Pentru activitatea de pregătire a utilizatorilor sau pentru realizarea de prezentări se vor folosi date anonime. Angajații care predau cursurile de pregătire vor folosi date cu caracter personal pe parcursul propriei lor pregătiri.

Operatorul va stabili modalitățile stricte prin care se vor distruge datele cu caracter personal. Autorizarea pentru această prelucrare de date cu caracter personal trebuie limitată la câțiva utilizatori.

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

4. Execuția copiilor de siguranță

Operatorul va stabili 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 vor fi numiți de operator, într-un număr restrâns. Copiile de siguranță se vor stoca în alte camere, în fișete metalice cu sigiliu aplicat, și, dacă este posibil, chiar în camere din altă clădire.

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

5. Computerele și terminalele de acces

Computerele și alte terminale de acces vor fi instalate în încăperi cu acces restricționat. Dacă nu pot fi asigurate aceste condiții, computerele se vor instala în încăperi care se pot încuia sau se vor lua măsuri ca accesul la computere să se facă cu ajutorul unor chei ori cartele magnetice.

Dacă pe ecran apar date cu caracter personal asupra cărora nu se acționează o perioadă dată, stabilită de operator, sesiunea de lucru trebuie închisă automat. Mărirea 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.

6. Fișierele de acces

Operatorul este obligat să 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.

7. Sistemele de telecomunicații

Operatorul este obligat să facă periodic controlul autentificărilor și tipurilor de acces pentru detectarea unor disfuncționalități în ceea ce privește folosirea sistemelor de telecomunicații.

Operatorii sunt obligați să conceapă sistemul de telecomunicații astfel încât datele cu caracter personal să nu poată fi interceptate sau transmise de oriunde. Dacă sistemul de telecomunicații nu poate fi astfel securizat, operatorul este obligat să impună folosirea metodei de criptare pentru transmiterea datelor cu caracter personal.

Prin sistemele de telecomunicații se vor transmite numai datele cu caracter personal strict necesare.

8. Instruirea personalului

În cadrul cursurilor de pregătire a utilizatorilor operatorul este obligat să facă informarea acestora cu privire la prevederile Legii nr. 677/2001 pentru 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 utilizatorului.

Utilizatorii care au acces la date cu caracter personal vor fi instruiți de către operator asupra confidențialității acestora și vor fi avertizați prin mesaje care vor apărea pe monitoare în timpul activității. Utilizatorii sunt obligați să își încheie sesiunea de lucru atunci când părăsesc locul de muncă.

9. Folosirea computerelor

Pentru menținerea securității prelucrării datelor cu caracter personal (în special împotriva virusilor informatici) operatorul va lua măsuri care vor consta în:

- a)** interzicerea folosirii de către utilizatori a programelor software care provin din surse externe sau dubioase;
- b)** informarea utilizatorilor în privința pericolului privind virusii informatici;
- c)** implementarea unor sisteme automate de devirusare și de securitate a sistemelor informatice;
- d)** dezactivarea, pe cât posibil, a tastei "Print screen", atunci când sunt afișate pe monitor date cu caracter personal, interzicându-se astfel scoaterea la imprimantă a acestora.

10. Imprimarea datelor

Scoaterea la imprimantă a datelor cu caracter personal se va realiza numai de utilizatori autorizați pentru această operațiune de către operator. Operatorii sunt obligați să aprobe proceduri interne specifice privind folosirea și

distrugerea acestor materiale.

Fiecare entitate își va aproba propriul sistem de securitate, ținând seama de aceste cerințe minime de securitate a prelucrărilor de date cu caracter personal, iar în funcție de importanța datelor cu caracter personal prelucrate, își va impune măsuri de securitate suplimentare.

Publicat în Monitorul Oficial cu numărul 383 din data de 5 iunie 2002