AVOCATUL POPORULUI

ORDIN nr. 52...
din 18 aprilie 2002

privind aprobarea "Cerinţelor minime de securitate
a prelucrărilor de date cu caracter personal"

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 şi funcţionarea instituţiei Avocatul Poporului şi ale art. 7 din Regulamentul de organizare şi funcţionare a instituţiei Avocatul Poporului;

în aplicarea prevederilor art. 20 alin. (2) din Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, conform cărora cerinţele minime de securitate a prelucrărilor de date cu caracter personal vor fi elaborate de autoritatea de supraveghere şi vor fi actualizate periodic, corespunzător progresului tehnic şi experienţei acumulate;

având în vedere Nota privind cerinţele minime de securitate a prelucrărilor de date cu caracter personal, înregistrată sub nr. 4327 din 18 aprilie 2002, a adjunctului Avocatului Poporului;

având în vedere exigenţa elaborării cerinţelor 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 şi organizatorice adecvate, prin care se garantează un nivel corespunzător şi legal de securitate a prelucrării de date cu caracter personal, precum şi a publicării cerinţelor respective în Monitorul Oficial al României, în scopul ca acestea să poată fi cunoscute în mod corespunzător de către operatorii menţionaţi;

Avocatul Poporului emite prezentul

ORDIN:

Art. 1. Se aprobă "Cerinţele minime de securitate a prelucrărilor de date cu caracter personal", prevăzute în anexa la prezentul ordin.

Art. 2. Prezentul ordin se publică în Monitorul Oficial al României.

Art. 3. Anexa face parte integrantă din prezentul ordin.

AVOCATUL POPORULUI,
Prof. univ. dr. Ioan MURARU

Bucureşti, 18 aprilie 2002

16.

A N E X Ă
la Ordinul Avocatului Poporului
nr. 52 din 18 aprilie 2002

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 şi implementării de către operator a măsurilor tehnice şi organizatorice necesare pentru păstrarea confidențialității şi integrității datelor cu caracter personal. În concordanță cu acestea, operatorii îşi vor stabili propriile politici şi proceduri de securitate.

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

1. Identificarea şi 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 şir 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 acelaşi cod de identificare.

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

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

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

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

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

Operatorii autorizează anumiți utilizatori pentru a revoca sau suspenda un cod de identificare şi autentificare dacă utilizatorul acestora şi-a dat demisia sau a fost concediat, şi-a încheiat contractul, a fost transferat la alt serviciu şi 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.) şi după acțiuni aplicate asupra datelor cu caracter personal (cum ar fi: scriere, citire, ştergere), precum şi 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 utilizatorii autorizați pentru operațiile de colectare şi 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 şi ora modificării Pentru o mai bună administrare, operatorul va lua măsuri ca sistemul informațional să mențină datele şterse 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, cât şi 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 fişete metalice cu sigiliu aplicat şi, dacă este posibil, chiar în camere din altă clădire.

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

5. Computerele şi terminalele de acces

Computerele şi 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 sau cartele magnetice.

Dacă pe ecran apar date cu caracter personal, asupra cărora nu se acționează o perioadă dată de timp, stabilită de operator, sesiunea de lucru trebuie închisă automat. Mărimea acestei perioade de timp se determină în funcție de operațiile care trebuiesc 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 şi după o perioadă scurtă de timp, stabilită de operator, în care nu se acționează asupra lor acestea, trebuie ascunse.

6. Fişierele de acces

Operatorul este obligat să ia măsuri ca orice accesare a bazei de date cu caracter personal să fie înregistrată într-un fişier 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 fişierul de acces sau în registru vor fi:

- codul de identificare (numele utilizatorului pentru bazele de date cu caracter personal manuale);
- numele fişierului accesat (fişei);
- 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 fişier de acces general sau în fişiere separate pentru fiecare utilizator. Orice încercare de acces neautorizat va fi, de asemenea, înregistrată.

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

Fişierele de acces trebuie să facă posibilă identificarea, de către operator sau de către persoana împuternicită, a persoanelor care au accesat date cu

112

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 şi tipurilor de acces pentru detectarea unor disfuncționalități, în ceea ce priveşte folosirea sistemelor de telecomunicații.

Operatorii sunt obligați să conceapă sistemul de telecomunicații astfel încât datele cu caracter personal să nu poată fi interceptate sau să fie transmise de oriunde. Dacă sistemul de telecomunicații nu poate fi astfel securizat, operatorul este obligat să impună folosirea metodei de criptare pentru transmisia 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, la cerințele minime de securitate a prelucrărilor de date cu caracter personal, precum şi 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 şi vor fi avertizați prin mesaje care vor apărea pe monitoare în timpul activității. Utilizatorii sunt obligați să-şi închidă sesiunea de lucru atunci când părăsesc locul de muncă.

9. Folosirea computerelor

Pentru menținerea securității prelucrării datelor cu caracter personal (în special împotriva virușilor 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 virușii informatici;
c) implementarea unor sisteme automate de devirusare şi de securitate a sistemelor informatice;
d) dezactivarea, pe cât posibil, a tastei "Print screen", atunci când sunt afişate 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 cont 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.