ORDIN nr. 52 din 18 aprilie 2002
privind aprobarea Cerintelor minime de securitate a prelucrarilor de date cu caracter personal
Emitent : AVOCATUL POPORULUI
Publicat in : MONITORUL OFICIAL nr. 383 din 5 iunie 2002

Avocatul Poporului,
in temeiul Hotararii Senatului Romaniei nr. 33 din 4 octombrie 2001 pentru numirea Avocatului Poporului,
vazand prevederile art. 13 din Legea nr. 35/1997 privind organizarea si functionarea institutiei Avocatul Poporului si ale art. 7 din Regulamentul de organizare si functionare a institutiei Avocatul Poporului,
in aplicarea prevederilor art. 20 alin. (2) din Legea nr. 677/2001 pentru protectia persoanelor cu privire la prelucrarea datelor cu caracter personal si libera circulatie a acestor date, conform carora cerintele minime de securitate a prelucrarilor de date cu caracter personal vor fi elaborate de autoritatea de supraveghere si vor fi actualizate periodic, corespunzator progresului tehnic si experientei acumulate,
avand in vedere Nota privind cerintele minime de securitate a prelucrarilor de date cu caracter personal, inregistrata sub nr. 4.327 din 18 aprilie 2002, a adjunctului Avocatului Poporului,
avand in vedere exigenta elaborarii cerintelor minime de securitate a prelucrarilor de date cu caracter personal, care stau la baza adoptarii de catre operatorii de date cu caracter personal a masurilor tehnice si organizatorice adecvate, prin care se garanteaza un nivel corespunzator si legal de securitate a prelucrarii de date cu caracter personal, precum si a publicarii cerintelor respective in Monitorul Oficial al Romaniei, Partea I, in scopul ca acestea sa poata fi cunoscute in mod corespunzator de catre operatorii mentionati,
emite prezentul ordin.

ART. 1
Se aproba Cerintele minime de securitate a prelucrarilor de date cu caracter personal, prevazute in anexa la prezentul ordin.
ART. 2
Prezentul ordin va fi publicat in Monitorul Oficial al Romaniei, Partea I.
ART. 3
Anexa face parte integranta din prezentul ordin.

AVOCATUL POPORULUI,
prof. univ dr. IOAN MURARU

ANEXA 1

CERINTELE MINIME DE SECURITATE
a prelucrarilor de date cu caracter personal

Prezentele cerinte minime de securitate a prelucrarilor de date cu caracter personal trebuie sa stea la baza adoptarii si implementarii de catre operator a masurilor tehnice si organizatorice necesare pentru pastrarea confidentialitatii si integritatii datelor cu caracter personal. In concordanta cu acestea operatorii isi vor stabili propriile politici si proceduri de securitate.

Cerintele minime de securitate a prelucrarilor de date cu caracter personal acopera urmatoarele aspecte:

1. Identificarea si autentificarea utilizatorului

Prin utilizator se intelege orice persoana care actioneaza sub autoritatea operatorului, a persoanei imputernicite sau a reprezentantului, cu drept recunoscut de acces la bazele de date cu caracter personal.

Utilizatorii, pentru a capata acces la o baza de date cu caracter personal, trebuie sa se identifice. Identificarea se poate face prin mai multe metode, cum ar fi: introducerea codului de identificare de la tastatura (un sir de caractere), folosirea unei cartele cu cod de bare, folosirea unei cartele inteligente (smart card) sau a unei cartele magnetice.

Fiecare utilizator are propriul sau cod de identificare. Niciodata mai multi utilizatori nu trebuie sa aiba acelasi cod de identificare.

Codurile de identificare (sau conturi de utilizator) nefolosite o perioada mai indelungata trebuie dezactivate si distruse dupa un control prealabil intern al operatorului. Perioada dupa care codurile trebuie dezactivate si distruse se stabileste de operator.

Orice cont de utilizator este insotit de o modalitate de autentificare. Autentificarea poate fi facuta prin introducerea unei parole sau prin mijloace biometrice: amprenta dactiloscopica, amprenta vocala, angiografia retiniana etc.

Parolele sunt siruri de caractere. Cu cat sirul de caractere este mai lung, cu atat parola este mai greu de aflat. La introducerea parolelor acestea nu trebuie sa fie afisate in clar pe monitor. Parolele trebuie schimbate periodic in functie de politicile de securitate ale entitatii (operator sau persoana imputernicita). Schimbarea periodica a parolelor se face numai de catre utilizatori autorizati de operator.

Operatorul trebuie sa solicite realizarea unui sistem informational care sa refuze automat accesul unui utilizator dupa 5 introduceri gresite ale parolei.

Orice utilizator care primeste un cod de identificare si un mijloc de autentificare trebuie sa pastreze confidentialitatea acestora si sa raspunda in acest sens in fata operatorului.

Fiecare entitate va stabili o procedura proprie de administrare si gestionare a conturilor de utilizator.

Operatorii autorizeaza anumiti utilizatori pentru a revoca sau a suspenda un cod de identificare si autentificare, daca utilizatorul acestora si-a dat demisia ori a fost concediat, si-a incheiat contractul, a fost transferat la alt serviciu si noile sarcini nu ii solicita accesul la date cu caracter personal, a abuzat de codurile primite sau daca va absenta o perioada indelungata stabilita de entitate.

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

2. Tipul de acces

Utilizatorii trebuie sa acceseze numai datele cu caracter personal necesare pentru indeplinirea atributiilor lor de serviciu. Pentru aceasta operatorii trebuie sa stabileasca tipurile de acces dupa functionalitate (cum ar fi: administrare, introducere, prelucrare, salvare etc.) si dupa actiuni aplicate asupra datelor cu caracter personal (cum ar fi: scriere, citire, stergere), precum si 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 dupa ce acestea au fost transformate in date anonime.

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

Pentru activitatea de pregatire a utilizatorilor sau pentru realizarea de prezentari se vor folosi date anonime. Angajatii care predau cursurile de pregatire vor folosi date cu caracter personal pe parcursul propriei lor pregatiri.

Operatorul va stabili modalitatile stricte prin care se vor distruge datele cu caracter personal. Autorizarea pentru aceasta prelucrare de date cu caracter personal trebuie limitata la cativa utilizatori.

3. Colectarea datelor

Operatorul desemneaza utilizatori autorizati pentru operatiile de colectare si introducere de date cu caracter personal intr-un sistem informational.

Orice modificare a datelor cu caracter personal se poate face numai de catre utilizatori autorizati desemnati de operator.

Operatorul va lua masuri pentru ca sistemul informational sa inregistreze cine a facut modificarea, data si ora modificarii. Pentru o mai buna administrare operatorul va lua masuri ca sistemul informational sa mentina datele sterse sau modificate.

4. Executia copiilor de siguranta

Operatorul va stabili intervalul de timp la care se vor executa copiile de siguranta ale bazelor de date cu caracter personal, precum si ale programelor folosite pentru prelucrarile automatizate. Utilizatorii care executa aceste copii de siguranta vor fi numiti de operator, intr-un numar restrans. Copiile de siguranta se vor stoca in alte camere, in fisete metalice cu sigiliu aplicat, si, daca este posibil, chiar in camere din alta cladire.

Operatorul va lua masuri ca accesul la copiile de siguranta sa fie monitorizat.

5. Computerele si terminalele de acces

Computerele si alte terminale de acces vor fi instalate in incaperi cu acces restrictionat. Daca nu pot fi asigurate aceste conditii, computerele se vor instala in incaperi care se pot incuia sau se vor lua masuri ca accesul la computere sa se faca cu ajutorul unor chei ori cartele magnetice.

Daca pe ecran apar date cu caracter personal asupra carora nu se actioneaza o perioada data, stabilita de operator, sesiunea de lucru trebuie inchisa automat. Marimea acestei perioade se determina in functie de operatiile care trebuie executate.

Terminalele de acces folosite in relatia cu publicul, pe care apar date cu caracter personal, vor fi pozitionate astfel incat sa nu poata fi vazute de public si dupa o perioada scurta, stabilita de operator, in care nu se actioneaza asupra lor, acestea trebuie ascunse.

6. Fisierele de acces

Operatorul este obligat sa ia masuri ca orice accesare a bazei de date cu caracter personal sa fie inregistrata intr-un fisier de acces (numit log la prelucrarile automate) sau intr-un registru pentru prelucrarile manuale de date cu caracter personal, stabilit de operator. Informatiile inregistrate in fisierul de acces sau in registru vor fi:

- codul de identificare (numele utilizatorului pentru bazele de date cu caracter personal manuale);
- numele fisierului accesat (fisei);
- numarul inregistrarilor efectuate;
- tipul de acces;
- codul operatiei executate sau programul folosit;
- data accesului (an, luna, zi);
- timpul (ora, minutul, secunda).

Pentru prelucrarile automate aceste informatii vor fi stocate intr-un fisier de acces general sau in fisiere separate pentru fiecare utilizator. Orice incercare de acces neautorizat va fi, de asemenea, inregistrata.

Operatorul este obligat sa pastreze fisierele de acces cel putin 2 ani, pentru a fi folosite ca probe in cazul unor investigatii. Daca investigatiile se prelungesc, aceste fisiere se vor pastra atat timp cat se va considera necesar.

Fisierele de acces trebuie sa faca posibila identificarea de catre operator sau de catre persoana imputernicita a persoanelor care au accesat date cu caracter personal fara un motiv anume, in vederea aplicarii unor sanctiuni sau a sesizarii organelor competente.

7. Sistemele de telecomunicatii

Operatorul este obligat sa faca periodic controlul autentificarilor si tipurilor de acces pentru detectarea unor disfunctionalitati in ceea ce priveste folosirea sistemelor de telecomunicatii.

Operatorii sunt obligati sa conceapa sistemul de telecomunicatii astfel incat datele cu caracter personal sa nu poata fi interceptate sau transmise de oriunde. Daca sistemul de telecomunicatii nu poate fi astfel securizat, operatorul este obligat sa impuna folosirea metodei de criptare pentru transmisia datelor cu caracter personal.

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

8. Instruirea personalului

In cadrul cursurilor de pregatire a utilizatorilor operatorul este obligat sa faca informarea acestora cu privire la prevederile Legii nr. 677/2001 pentru protectia persoanelor cu privire la prelucrarea datelor cu caracter personal si libera circulatie a acestor date, la cerintele minime de securitate a prelucrarilor de date cu caracter personal, precum si cu privire la riscurile pe care le comporta prelucrarea datelor cu caracter personal, in functie de specificul activitatii utilizatorului.

Utilizatorii care au acces la date cu caracter personal vor fi instruiti de catre operator asupra confidentialitatii acestora si vor fi avertizati prin mesaje care vor aparea pe monitoare in timpul activitatii. Utilizatorii sunt obligati sa isi inchida sesiunea de lucru atunci cand parasesc locul de munca.

9. Folosirea computerelor

Pentru mentinerea securitatii prelucrarii datelor cu caracter personal (in special impotriva virusilor informatici) operatorul va lua masuri care vor consta in:

a) interzicerea folosirii de catre utilizatori a programelor software care provin din surse externe sau dubioase;

b) informarea utilizatorilor in privinta pericolului privind virusii informatici;

c) implementarea unor sisteme automate de devirusare si de securitate a sistemelor informatice;

d) dezactivarea, pe cat posibil, a tastei "Print screen", atunci cand sunt afisate pe monitor date cu caracter personal, interzicandu-se astfel scoaterea la imprimanta a acestora.

10. Imprimarea datelor

Scoaterea la imprimanta a datelor cu caracter personal se va realiza numai de utilizatori autorizati pentru aceasta operatiune de catre operator. Operatorii sunt obligati sa aprobe proceduri interne specifice privind folosirea si distrugerea acestor materiale.

Fiecare entitate isi va aproba propriul sistem de securitate, tinand seama de aceste cerinte minime de securitate a prelucrarilor de date cu caracter personal, iar in functie de importanta datelor cu caracter personal prelucrate, isi va impune masuri de securitate suplimentare.
