PROIECT

DECIZIE nr. din 2006
privind aprobarea Cernințelor minime de securitate a prelucrărilor de date cu caracter personal

În temeiul prevederilor art. 3 alin. (5) şi (6) din **Legea nr. 102/2005** privind înființarea, organizarea şi funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, cu modificările ulterioare, şi ale art. 6 alin. (2) lit. b) din Regulamentul de organizare şi funcționare a Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, aprobat prin Hotărârea Biroului Permanent al Senatului nr. **16/2005,**

în aplicarea prevederilor art. 20 alin. (2) din **Legea nr. 677/2001** pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter persoanal şi libera circulație a acestor date, cu modificările şi completările ulterioare,

luând în considerare faptul că cerințele 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 experienței acumulate,

văzând referatul de aprobare nr. ... din .... privind propunerea emiterii unei decizii de stabilire a cerințelor minime de securitate a prelucrărilor de date cu caracter personal,

preşedintele Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal emite prezenta

DECIZIE

Art. 1
Se aprobă Cerințele minime de securitate a prelucrărilor de date cu caracter personal, prevăzute în anexa care face parte integrantă din prezenta decizie.

Art. 2
Prezenta decizie intră în vigoare în termen de 30 zile de la publicare în Monitorul Oficial al României, Partea I.

Art. 3
Pe data intrării în vigoare a prezentei decizii, Ordinul Avocatului Poporului nr. 52/2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter, publicat în Monitorul Oficial al României, Partea I, nr. 383 din 5 iunie 2002, îşi încetează aplicabilitatea.

Preşedintele Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal,
Georgeta BASARABESCU

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 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, în formă scrisă, ce vor fi puse la dispoziție autorității de supraveghere, la solicitarea acesteia.
Prin **cerinte minime de securitate** este avut în vedere un complex de masuri tehnice, informatice, organizatorice, logistice, proceduri si politici de securitate prin care să se asigure nivelul minim de securitate prevăzut in art. 20 din Legea nr. 677/2001.
Prin **utilizator** este avută în vedere orice persoană fizică care acționează sub autoritatea operatorului, a persoanei împuternicite sau a reprezentantului, cu drept recunoscut de acces la bazele de date cu caracter personal.
Cerințele minime de securitate acoperă următoarele categorii de prelucrări de date cu caracter personal se referă la:

1. Prelucrari automate de date cu caracter personal

Accesul utilizatorilor la bazele de date ce contin date cu caracter personal se va efectua prin coduri personale de acces (nume de logare, nume de utilizator). Codurile de acces sunt protejate prin metode de autentificare (parole, certificate). Codurile de acces (conturi utilizator) sunt alocate individual pentru fiecare utilizator pe baza unei proceduri specifice. Conturile de utilizator nefolosite o perioadă mai îndelungată sunt sterse sau dezactivate permanent după un control prealabil intern al operatorului. Codurile de acces se vor dezactiva automat după un număr rezonabil de încercări nereuşite. Perioada şi numărul de incercări nereuşite după care codurile trebuie dezactivate sau şterse se stabileşte de operator.

Codurile de acces vor permite doar nivelul minim de acces la datele cu caracter personal ce sunt necesare pentru îndeplinirea atribuțiilor de serviciu.

Programatorii care dezvoltă aplicațiile care prelucrează datele cu caracter personal nu au 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.

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

Computerele 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.

Orice accesare a bazei de date cu caracter personal, inclusiv orice incercare de acces neautorizat, va fi inregistrată într-un fişier de acces. Fişierele de acces trebuie să facă posibilă identificarea de către operator, reprezentant sau de către persoana împuternicită a persoanelor care au accesat date cu caracter personal fără un motiv legitim, în vederea aplicării unor sancțiuni sau a sesizării organelor competente.

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

Computerele şi alte terminale de acces vor fi instalate în încăperi cu acces restricționat. Dacă nu pot fi asigurate aceste condiții, acestea 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.

Computerele sau terminalele de acces folosite în relația cu publicul, pe care sunt afişate date cu caracter personal, vor fi poziționate astfel încât acestea să nu poată fi dezvăluite publicului. După o perioadă scurtă, stabilită de operator, în care nu se acționează asupra lor, acestea trebuie ascunse.

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 unor metode de criptare pentru transmisia datelor cu caracter personal. Prin sistemele de telecomunicații se vor transmite numai datele cu caracter personal strict necesare pentru realizarea scopului comunicației respective.

Operatorul va stabili intervalul de timp rezonabil la care se vor executa copiile de siguranță ale bazelor de date cu caracter personal, precum şi ale programelor folosite pentru prelucrările automatizate. Copiile de siguranță se vor stoca în alte camere decât cele destinate utilizării computerelor, în fişete metalice cu sigiliu aplicat, şi, dacă este posibil, chiar în camere din altă clădire.

2. Prelucrari manuale de date cu caracter personal

În cadrul prelucrărilor de date cu caracter personal efectuate manual, accesul utilizatorilor se va realiza pe baza unei liste aprobate de conducerea entității. Modalitatea de acces şi datele care pot fi accesate de fiecare utilizator vor fi stabilite de către operator prin proceduri interne.

Documentele care conțin date cu caracter personal vor fi ținute în fişete sau dulapuri închise cu cheie sau cu un alt mecanism de securizare.
Documentele care conțin date cu caracter personal, folosite pentru realizarea anumitor operațiuni se vor preda persoanelor abilitate sau se vor închide imediat după terminarea acestora.

3. Prelucrari automate de date cu caracter personal care fac parte din categoria datelor cu caracter special (art. 7, art. 8, art. 9 şi art. 10 din Legea nr. 677/2001)

Pe lângă prevederile referitoare la prelucrările automate de date cu caracter personal (pct. 1) se vor impune suplimentar următoarele măsuri:

- accesul utilizatorilor la computerele sau terminalele de acces va fi posibil prin folosirea unor cartele magnetice sau a unor cartele inteligente („smart carduri") de preferință sau se va impune schimbarea periodică automată a codului de acces pentru autentificare. Perioada de schimbare automată a codului de acces pentru autentificare va fi stabilită prin procedură internă de către operator dar fără să depăşească o lună calendaristică;
- nivelul de autorizare şi acces la aceste date pentru fiecare utilizator se va stabili de către persoanele desemnate special pentru aceste sarcini;
- periodic, la intervale care nu vor depăşi un an, se vor efectua verificări privind accesul şi nivelul de acces ale utilizatorilor la datele cu caracter personal.

4. Prelucrari manuale de date cu caracter personal care fac parte din categoria datelor cu caracter special (art. 7, art. 8, art. 9 şi art. 10 din Legea nr. 677/2001)

Pe lângă prevederile referitoare la prelucrările manuale ale datelor cu caracter personal (pct. 2) se vor impune suplimentar următoarele măsuri:

- prelucrarea datelor cu caracter personal se va efectua numai de către utilizatorii desemnați de operator prin proceduri interne;
- accesul utilizatorilor se va face pe baza unor proceduri emise de operator;
- orice accesare a datelor cu caracter personal va fi înregistrată într-un registru de acces.

5. Documente obligatorii pentru prelucrarea datelor personale care fac parte din categoria datelor cu caracter special (art. 7, art. 8, art. 9 şi art. 10 din Legea nr.

677/2001)

Operatorii care prelucrează date cu caracter personal care fac parte din categoria datelor cu caracter special vor întocmi obligatoriu următoarele documente:

- proceduri de control al accesului in aceste zone (masuri tehnice si organizatorice privind securizarea zonei in care se prelucreaza aceste date);
- proceduri de asigurare a integrității si disponibilitatii datelor;
- proceduri privind securitatea transmisiilor de date si accesul securizat la aceste mijloace de transmitere a datelor.