



UNIUNEA EUROPEANĂ



GUVERNUL ROMÂNIEI

MINISTERUL
EDUCAȚIEI
CERCETĂRII ȘI
INOVĂRIIFondul Social European
POSDRU 2007-2013Instrumente Structurale
2007-2013FUNDAȚIA LUMINA
INSTITUȚIE DE ÎNVĂȚĂMÂNT**Investește în oameni!**

Proiect cofinanțat prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013
 AXA PRIORITARĂ nr 2 - „Corelarea învățării pe tot parcursul vieții cu piața muncii”
 DOMENIUL MAJOR DE INTERVENȚIE 2.3 - „Acces și participare la formare profesională continuă”
 Titlu proiect: „FPC – Formare pentru competitivitate”
 Numărul de identificare al proiectului: POSDRU/182/2.3/S/154499
 Beneficiar: Fundația Lumina Instituții de Învățământ

Newsletter 49

**Cerințele minime de securitate
a prelucrărilor de date cu caracter personal**

Continuăm publicarea de materiale necesare companiilor, de această dată pentru cele care doresc să devină operatori de date cu caracter personal.

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 trebuie schimbate periodic. 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.



UNIUNEA EUROPEANĂ



GUVERNUL ROMÂNIEI

MINISTERUL
EDUCAȚIEIFondul Social European
POSDRU 2007-2013Instrumente Structurale
2007-2013FUNDAȚIA LUMINA
INSTITUȚII DE ÎNVĂȚĂMÂNT**Investește în oameni!**

Proiect cofinanțat prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013
 AXA PRIORITARĂ nr 2 - „Corelarea învățării pe tot parcursul vieții cu piața muncii”
 DOMENIUL MAJOR DE INTERVENȚIE 2.3 - „Acces și participare la formare profesională continuă”
 Titlu proiect: „FPC – Formare pentru competitivitate”
 Numărul de identificare al proiectului: POSDRU/182/2.3/S/154499
 Beneficiar: Fundația Lumina Instituții de Învățământ

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 solicita 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 utilizatorului (în cazul proiectului FPC, Fundația Lumina Instituții de Învățământ – FLII).

2. Tipul de acces

Utilizatorii trebuie să acceseze numai datele cu caracter personal necesare pentru îndeplinirea atribuțiilor lor de serviciu.

Operatorul stabilește 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 permite accesul programatorilor la datele cu caracter personal după ce acestea au fost transformate în date anonime.

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

Pentru activitatea de pregătire a utilizatorilor sau pentru realizarea de prezentări se folosesc date anonime.

Angajații care predau cursuri de pregătire pot și ei folosi date cu caracter personal pe parcursul propriei lor pregătiri.

Operatorul stabilește în continuare modalitățile stricte prin care se vor distruge datele cu caracter personal. Autorizarea pentru aceasta 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.





UNIUNEA EUROPEANĂ



GUVERNUL ROMÂNIEI

MINISTERUL
EDUCAȚIEI
CERCETĂRII ȘI
INOVĂRIIFondul Social European
POSDRU 2007-2013Instrumente Structurale
2007-2013**Investește în oameni!**

Proiect cofinanțat prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013
 AXA PRIORITARĂ nr 2 - „Corelarea învățării pe tot parcursul vieții cu piața muncii”
 DOMENIUL MAJOR DE INTERVENȚIE 2.3 - „Acces și participare la formare profesională continuă”
 Titlu proiect: „FPC – Formare pentru competitivitate”
 Numărul de identificare al proiectului: POSDRU/182/2.3/S/154499
 Beneficiar: Fundația Lumina Instituții de Învățământ

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 de o zi 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.

Mărimea 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: a.- codul de identificare (numele utilizatorului pentru bazele de date cu caracter personal manuale); b.- numele fișierului accesat (fișei); c.-



UNIUNEA EUROPEANĂ



GUVERNUL ROMÂNIEI

MINISTERUL
EDUCAȚIEI, CERCETĂRII ȘI
TIC-uluiFondul Social European
POSDRU 2007-2013Instrumente Structurale
2007-2013FUNDAȚIA LUMINA
INSTITUȚII DE ÎNVĂȚĂMÂNT**Investește în oameni!**

Proiect cofinanțat prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013
 AXA PRIORITARĂ nr 2 - „Corelarea învățării pe tot parcursul vieții cu piața muncii”
 DOMENIUL MAJOR DE INTERVENȚIE 2.3 - „Acces și participare la formare profesională continuă”
 Titlu proiect: „FPC – Formare pentru competitivitate”
 Numărul de identificare al proiectului: POSDRU/182/2.3/S/154499
 Beneficiar: Fundația Lumina Instituții de Învățământ

numărul înregistrărilor efectuate; c.- tipul de acces; d.- codul operației executate sau programul folosit;
 e.- data accesului (an, luna, zi); f.- 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 va păstra 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 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 pentru protecția persoanelor, vizând 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 închidă sesiunea de lucru atunci când părăsesc locul de munca.

9. Folosirea computerelor



UNIUNEA EUROPEANĂ



GUVERNUL ROMÂNIEI



MINISTERUL
EDUCAȚIEI
CERCETĂRII ȘI
INOVĂRII



Fondul Social European
POSDRU 2007-2013



Instrumente Structurale
2007-2013



FUNDAȚIA LUMINA
INSTITUȚII DE ÎNVĂȚĂMÂNT

Investește în oameni!

Proiect cofinanțat prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013
AXA PRIORITARĂ nr 2 - „Corelarea învățării pe tot parcursul vieții cu piața muncii”
DOMENIUL MAJOR DE INTERVENȚIE 2.3 - „Acces și participare la formare profesională continuă”
Titlu proiect: „FPC – Formare pentru competitivitate”
Numărul de identificare al proiectului: POSDRU/182/2.3/S/154499
Beneficiar: Fundația Lumina Instituții de Învățământ

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 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 aceasta operațiune de către operator.

Operatorul stabilește 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.

