LICEUL TEHNOLOGIC
"TASE DUMITRESCU", MIZIL
INTRARE IEŞIRE Nr. 708 / 22.05.2018

APROBAT,

DIRECTOR,

PROF. GHEŢE VIORICA

POLITICA DE SECURITATE
A PRELUCRARILOR DE DATE CU CARACTER PERSONAL
IN CADRUL
LICEULUI TEHNOLOGIC „TASE DUMITRESCU", MIZIL

CERINŢELE MINIME DE SECURITATE a prelucrărilor de date cu caracter personal

Prezentele cerinţe 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 confidenţialităţii şi integrităţii datelor cu caracter personal. În concordanţă cu acestea operatorii s-au stabilit propriile politici şi proceduri de securitate.
Cerinţele minime de securitate a prelucrărilor de date cu caracter personal acoperă următoarele aspecte:

1. *Identificarea şi autentificarea utilizatorului*

Prin utilizator se înţelege orice persoană care acţionează sub autoritatea operatorului, a persoanei împuternicite sau a reprezentantului, cu drept recunoscut de acces la bazele de date cu caracter personal. Utilizatorii care prelucreaza date personale sunt nominalizati prin Decizie interna a conducatorului institutiei de

invatamant.

Utilizatorii, pentru a căpăta acces la o bază de date cu caracter personal, trebuie să se identifice. Identificarea se poate face prin introducerea codului de identificare de la tastatură (un şir de caractere).

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

Codurile de identificare (sau conturi de utilizator) nefolosite o perioadă mai îndelungată trebuie dezactivate şi distruse după un control prealabil intern al operatorului. Perioada după care codurile trebuie dezactivate şi distruse se stabileşte de operator. Parolele de acces vor fi pastrate in plicuri sigilate si depozitate in seiful institutiei.

Orice cont de utilizator este însoţit de o modalitate de autentificare. Autentificarea poate fi făcută prin introducerea unei parole.

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.

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

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

Utilizatorilor le este interzis sa permita accesul altor persoane la calculatoarele care le-au fost incredintate drept resurse materiale in vederea exercitarii sarcinilor de lucru, precum si utilizarea surselor de stocare externe care apartin altor persoane.

Operatorii autorizează anumiţi utilizatori pentru a revoca sau a suspenda un cod de identificare şi autentificare, dacă utilizatorul acestora şi-a dat demisia ori 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 entităţii.

2. Tipul de acces

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

Operatorul va stabili modalităţile stricte prin care se vor distruge datele cu caracter personal. Autorizarea pentru această prelucrare de date cu caracter personal este limitată la un numar de mic utilizatori (personal didactic auxiliar) si la profesorii diriginti ai claselor de elevi.

3. Colectarea datelor

Operatorul desemnează utilizatori autorizaţi pentru operaţiile de colectare şi introducere de date cu caracter personal într-un sistem informaţional prin Decizie interna a conducatorului institutiei.

Orice modificare a datelor cu caracter personal se poate face numai de către utilizatori autorizaţi desemnaţi de operator.

Operatorul va lua măsuri pentru ca sistemul informaţional să înregistreze cine a făcut modificarea, data şi ora modificării. Pentru o mai bună administrare operatorul va lua măsuri ca sistemul informaţional să menţină datele şterse sau modificate.

4. Execuţia copiilor de siguranţă

Intervalul de timp la care se vor executa copiile de siguranţă ale bazelor de date cu caracter personal, precum şi ale programelor folosite pentru prelucrările automatizate este de 3 luni. Utilizatorii care execută aceste copii de siguranţă vor fi numiţi de operator, într-un număr restrâns. Copiile de siguranţă se vor stoca în alte camere, în fişete metalice cu sigiliu aplicat, şi, dacă este posibil, chiar în camere din altă clădire.

5. Computerele şi terminalele de acces

Computerele şi alte terminale de acces vor fi instalate în încăperi cu acces restricţionat. Dacă nu pot fi asigurate aceste condiţii, computerele se vor instala în încăperi care se pot încuia.
Dacă pe ecran apar date cu caracter personal asupra cărora nu se acţionează o perioadă dată, stabilită de operator, sesiunea de lucru trebuie închisă automat. Mărimea acestei perioade se determină în funcţie de operaţiile care trebuie executate.
Terminalele de acces folosite pe care apar date cu caracter personal, vor fi poziţionate astfel încât să nu poată fi văzute de persoane neautorizate şi după o perioadă scurtă, stabilită de operator, în care nu se acţionează 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. Informaţiile 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 operaţiei executate sau programul folosit;

- data accesului (an, lună, zi);

- timpul (ora, minutul, secunda).

7. Sistemele de telecomunicaţii

Operatorul este obligat să facă periodic controlul autentificărilor şi tipurilor de acces pentru detectarea unor disfuncţionalităţi în ceea ce priveşte folosirea sistemelor de telecomunicaţii.
Operatorii sunt obligaţi să conceapă sistemul de telecomunicaţii astfel încât datele cu caracter personal să nu poată fi interceptate sau transmise de oriunde. Dacă sistemul de telecomunicaţii nu poate fi astfel securizat, operatorul este obligat să impună folosirea metodei de criptare pentru transmisia datelor cu caracter personal.
Prin sistemele de telecomunicaţii 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 GDRP NR. 679/2016 si a Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, la cerinţele 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 funcţie de specificul activităţii utilizatorului.
Utilizatorii care au acces la date cu caracter personal vor fi instruiţi de către operator asupra confidenţialităţii acestora . Utilizatorii sunt obligaţi să îşi închidă sesiunea de lucru atunci când părăsesc locul de muncă.

9. Folosirea computerelor

Pentru menţinerea securităţii prelucrării datelor cu caracter personal (în special împotriva viruşilor 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 privinţa pericolului privind viruşii 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.

e)fiecare computer are instalat un program antivirus

10. Imprimarea datelor

Scoaterea la imprimantă a datelor cu caracter personal se va realiza numai de utilizatori autorizaţi pentru această operaţiune de către operator. Datele in format de letric , precum si toate documentele cu caracter personal se vor stoca in arhiva unitatii, conform legislatiei in vigoare privind arhivele si in termenele stabilite conform Nomenclatorului arhivistic al documentelor aprobat de Directia Judeteana Prahova a Arhivelor Nationale.
Documentele care contin date personale si care nu necesita arhivare (copii Xerox, documente listate eronat) se va aplica procedura de distrugere prin taiere, maruntire a ducumentelor.

Intocmit,

Moise Liliana