REG. 0. PDCPSI

REGULAMENT PRIVIND PRELUCRAREA ŞI PROTECȚIA DATELOR CU CARACTER PERSONAL ÎN SISTEMUL INFORMAȚIONAL

	ELABORAT	COORDONAT	COORDONAT și VERIFICAT	APROBAT
Responsabil	**Ion COVALENCO** Șef DI	**Silvia MARIAN** Șef SJS	**Ala COTELNIC** Prim-prorector	**Grigore BELOSTECINIC** Rector ASEM
Data	2015	2015	2015	Proces-verbal nr.4 al Senatului din 25.03.2015
Semnătura				

I. DISPOZIȚII GENERALE

1. Prezentul Regulament stabileşte regulile privind prelucrarea şi protecția datelor cu caracter personal în sistemul informațional al ASEM (în continuare, *SI*).

2. Reglementările cuprinse în prezentul Regulament stabilesc exercitarea drepturilor şi obligațiilor pe care ASEM, în calitate de operator de date cu caracter personal, în domeniul protecției datelor cu caracter personal ale angajaților şi studenților.

3. Regulamentul este elaborat în temeiul prevederilor:

- Codului Educației al Republicii Moldova nr. 152 din 17.07.2014, (Monitorul Oficial al Republicii Moldova, 2014, nr. 319-324, art. 634);
- Legii nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal (Monitorul Oficial al Republicii Moldova, 2011, nr. 170-175, art. 492);
- Hotărârii Guvernului nr.1123 din 14.12.2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal (Monitorul Oficial al Republicii Moldova, 2010, nr. 254-256, art. 1282).

4. Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale au drept scop stabilirea regulilor de implementare a măsurilor tehnice şi organizatorice necesare pentru asigurarea securității, confidențialității şi integrității datelor cu caracter personal.

5. Măsurile de protecție a datelor cu caracter personal sunt asigurate în scopul:

- prevenirii scurgerii informației care conține date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;
- prevenirii distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în rețelele telecomunicaționale şi resursele informaționale;
- neadmiterea dezvăluirii terților a informației cu accesibilitate limitată;
- eficientizarea resurselor informaționale atât pe suport de hârtie, cât şi în format electronic.

II. CADRUL INSTITUȚIONAL PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL ÎN SI

6. ASEM recunoaşte şi respectă dreptul la viață intimă, familială şi privată, prelucrarea datelor cu caracter personal desfăşurându-se în conformitate cu prevederile legale în vigoare.

7. Protecția datelor cu caracter personal în cadrul ASEM (în calitate de operator de date cu caracter personal) este asigurată printr-un complex de măsuri tehnice şi organizatorice de preîntâmpinare a prelucrării ilicite a datelor cu caracter personal.

8. Datele cu caracter personal care fac obiectul prelucrării vor fi:

a) prelucrate în mod corect şi conform prevederilor legii;
b) colectate în scopuri determinate, explicite şi legitime, iar ulterior să nu fie prelucrate într-un mod incompatibil cu aceste scopuri. Prelucrarea ulterioară a datelor cu caracter personal în scopuri statistice, de cercetare istorică sau ştiințifică nu este considerată incompatibilă cu scopul colectării, dacă se efectuează cu respectarea prevederilor legale în vigoare;
c) adecvate, pertinente şi neexcesive în ceea ce priveşte scopul pentru care sunt colectate şi/sau prelucrate ulterior;

d) exacte şi, dacă este necesar, actualizate. Datele inexacte sau incomplete din punctul de vedere al scopului pentru care sunt colectate şi ulterior prelucrate se şterg sau se rectifică;
e) stocate într-o formă care să permită identificarea subiecților datelor cu caracter personal pe o perioadă care nu va depăşi durata necesară atingerii scopurilor pentru care sunt colectate şi ulterior prelucrate.

9. Utilizatorii vor accesa numai datele cu caracter personal necesare pentru îndeplinirea atribuțiilor lor de serviciu.

10. La încheierea operațiunilor de prelucrare, datele cu caracter personal se vor stoca în Arhiva ASEM şi/sau în sistemul informațional de date cu caracter personal al ASEM.

11. La expirarea termenului de stocare, datele cu caracter personal vor fi distruse în modul stabilit de lege.

III. MĂSURI DE PROTECȚIE A DATELOR ÎN SISTEMUL INFORMAȚIONAL

12. Sunt supuse protecției prin mijloace/procedee specifice, toate resursele informaționale ale operatorului de date cu caracter personal gestionate, care conțin date cu caracter personal, păstrate pe suporturi fizice (dispozitive magnetice, optice, laser sau alte suporturi ale informației electronice) precum şi în sistemele informaționale (masive informaționale, sistemele de gestionare a bazelor de date, aplicații informatice, clasificatoare, sisteme operaționale, rețele, sisteme de telecomunicații, inclusiv mijloacele de confecționare şi multiplicare a documentelor etc.).

13. Accesul în sediile/oficiile/birourile ori spațiile unde sunt amplasate sistemele informaționale de date cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară, conform listei sau însemnelor corespunzătoare (insigne, ecusoane, cartele de identificare).

14. Amplasarea mijloacelor de prelucrare a datelor cu caracter personal trebuie să corespundă necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor şi altor posibile riscuri.

15. Folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare în perimetrul de securitate este admisă doar în cazul prezenței unei permisiuni speciale a administrației.

16. Accesul prin tehnologia fără fir la sistemele informaționale de date cu caracter personal este permis doar în cazul utilizării mijloacelor criptografice de protecție a informației.

17. În scopul elucidării tentativelor de acces neautorizat, se efectuează înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații şi procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:

a) data şi timpul tentativei de obținere a accesului (executare a operațiunii),
b) denumirea (identificatorul) aplicației sau procesului, a ID-ului utilizatorului,
c) specificațiile resursei protejate (identificator, nume logic, nume fişier, număr etc.),
d) tipul operațiunii solicitate (citire, înregistrare, ştergere etc.),
e) rezultatul tentativei de obținere a accesului – pozitivă sau negativă.

18. Personalul care asigură exploatarea sistemelor informaționale de date cu caracter personal trece, minimum o dată în an, instruirea referitor la responsabilitățile şi obligațiile în cazul executării acțiunilor de gestionare şi reacționare la incidentele de securitate.

19. Persoana responsabilă de politica de securitate a datelor cu caracter personal:

a) va defini clar responsabilitățile şi procesele de management al securității datelor cu caracter personal, cu integrarea lor corespunzătoare în structura organizațională şi de funcționare generală;
b) va asigura măsuri tehnice şi organizaționale necesare organizării procesului de management al securității datelor cu caracter personal;
c) va elabora procedurile de clasificare a informației, care conține date cu caracter personal, astfel încât să fie posibil de întocmit un nomenclator şi toate datele cu caracter personal care sunt prelucrate să fie localizate, indiferent de tipul purtătorului de date;
d) va instrui persoanele implicate în procesul de prelucrare a datelor cu caracter personal în vederea îndeplinirii de către acestea a atribuțiilor funcționale şi asumării responsabilităților de securitate a datelor cu caracter personal, inclusiv asupra confidențialității acestora.

20. Persoana responsabilă de politica de securitate a datelor cu caracter personal va informa imediat administrația despre orice caz de încălcare a normelor de securitate şi va lua măsuri de restabilire a securității.

a. Informația în format digital cu datele personale se copie automat, zilnic. Copiile de siguranță se testează în scopul verificării siguranței purtătorilor de informații şi integrității informației indicate. Procedurile de restabilire a copiilor de siguranță se actualizează şi se testează cu regularitate, în scopul asigurării eficacității acestora.

b. Calculatoarele pe care sunt stocate date cu caracter personal trebuie să fie conectate la surse de alimentare continuă (UPS-uri).

c. Cablurile de rețea, prin care se efectuează operațiunile de transmitere a datelor preluate din sistemul de evidență contabilă, trebuie protejate contra conectărilor nesancționate sau deteriorărilor. Pentru a exclude bruiajul, cablurile de tensiune trebuie separate de cele comunicaționale.

IV. IDENTIFICAREA ŞI AUTENTIFICAREA UTILIZATORILOR INFORMAȚIILOR PRELUATE DIN SI

21. Toți utilizatorii (inclusiv personalul care asigură mentenanța tehnică, administratorii de rețea, programatorii şi administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu trebuie să conțină semnalmentele nivelului de accesibilitate al utilizatorului.

22. Pentru confirmarea ID-ului utilizatorului sunt utilizate parole. Este interzisă înscrierea parolelor pe suport de hârtie, cu excepția cazului de asigurare a securității păstrării acesteia (în safeu). La momentul introducerii, parolele nu se reflectă în clar pe monitor.

23. Parolele urmează a fi modificate de fiecare dată când există suspiciunea compromiterii sistemului sau a parolei. Parolele vechi se păstrează în arhivă, fără a mai fi folosite repetat.

24. Numărul încercărilor de autentificare la informațiile cu caracter personal trebuie limitat la 3.

25. În cazul în care raporturile de muncă ale utilizatorului au încetat, au fost suspendate sau modificate, şi, ca urmare, noile sarcini nu necesită accesul la datele cu caracter personal, precum

şi în cazul de modificare a drepturilor de acces ale utilizatorului, abuz al utilizatorului de autorizații de acces primite în scopul comiterii unei fapte prejudiciabile, absență a utilizatorului la postul de muncă pe parcursul unei perioade îndelungate (mai mult de 3 luni), codurile de identificare şi autentificare se revocă sau se suspendă.

26. În scopul depistării şi evitării cazurilor de acordare a drepturilor de acces neautorizat, se revizuieşte cu regularitate, maximum la fiecare şase luni şi după oricare schimbare a statutului utilizatorului, drepturile de acces ale acestuia.

27. Toți angajații cu drepturi de acces beneficiază de o instruire inițială în domeniul protecției datelor cu caracter personal.

28. Utilizatorul dezvăluie datele cu caracter personal către terți, doar la indicația în scris a Rectorului ASEM.

29. Orice încălcare a securității, în ceea ce priveşte protejării datelor cu caracter personal, este supusă documentării, iar persoana responsabilă de realizarea politicii de securitate este informată în legătură cu acest lucru cât de urgent posibil.

30. Înainte de acordarea accesului la datele cu caracter personal, utilizatorii sunt informați despre faptul că sistemul informațional al datelor cu caracter personal este controlat şi că folosirea neautorizată a acestora este sancționată în conformitate cu legislația civilă, contravențională sau penală.

V. CONTROL ŞI ÎMBUNĂTĂȚIRE

31. Persoana responsabilă de realizarea politicii de securitate va organiza anual un audit referitor la protecția datelor cu caracter personal.

32. Departamentul de Informatică va iniția acțiuni corective şi preventive pentru a eficientiza procesele referitoare la protecția datelor cu caracter personal.

33. Departamentul de Informatică va asigura identificarea, protocolarea şi înlăturarea deficiențelor de soft-uri destinate prelucrării informațiilor cu caracter personal, inclusiv protecția contra infiltrării programelor dăunătoare în soft-uri, măsuri care asigură posibilitatea reînnoirii automate şi la timp a mijloacelor de asigurare a protecției contra programelor dăunătoare şi signaturilor de virus.

34. Departamentul de Informatică va face periodic controlul autentificărilor şi tipurilor de acces pentru detectarea unor disfuncționalități în ceea ce priveşte folosirea echipamentelor şi sistemelor de telecomunicații.

VI. DISPOZIȚII FINALE

35. Prezentul Regulament poate fi revizuit periodic, în funcție de modificările şi completările legislative aplicabile, precum şi de nivelul de dezvoltare tehnologică.

36. Regulamentul este adus la cunoştința angajaților contra semnătură.

37. Prezentul Regulament intră în vigoare din momentul aprobării de către Senatul ASEM.

Tipografia Departamentului Editorial-Poligrafic al ASEM
Chişinău, 2005, str. Mitropolit Gavriil Bănulescu-Bodoni 59
Tel. 402-910