

REG. 0. PDPS

**REGULAMENT PRIVIND PRELUCRAREA ȘI PROTEȚIA
DATELOR CU CARACTER PERSONAL ALE STUDENȚILOR**

	ELABORAT	COORDONAT	COORDONAT și VERIFICAT	APROBAT
Responsabil	BACIU Sergiu Șef DSDCMC	MARIAN Silvia Șef SJS	COTELNIC Ala Prim-prorector	BELOSTECINIC Grigore Rector ASEM
Data	2015	2015	2015	Proces-verbal nr.4 al Senatului din 25.02.2015
Semnătura				

I. DISPOZIȚII GENERALE

1. Presentul Regulament stabilește regulile privind prelucrarea și protecția datelor cu caracter personal ale beneficiarilor de servicii educaționale oferite de ASEM, respectiv: elevi, studenți, masteranzi, doctoranzi, cursanți (*în continuare - studenți*), în cadrul procesului de studii.
2. 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).
3. Reglementările cuprinse în prezentul Regulament stabilesc exercitarea drepturilor și obligațiilor pe care ASEM, în calitate de operator de date cu caracter personal, le are în domeniul protecției datelor cu caracter personal ale studenților, în relațiile instituției cu studenții în cadrul procesului de studii, cu alte instituții de învățământ, precum și cu alte persoane fizice sau juridice.

II. CADRUL INSTITUȚIONAL PRIVIND PRELUCRARE DATELOR CU CARACTER PERSONAL ALE STUDENȚILOR

4. ASEM recunoaște și respectă dreptul la viață intimă, familială și privată, prelucrarea datelor cu caracter personal desfășurându-se în conformitate cu prevederile legale în vigoare.
5. Dată cu caracter personal este orice informație referitoare la o persoană fizică, care poate fi identificată, direct sau indirect, în special prin referire la un număr de identificare (cod personal), la unul sau mai multe elemente specifice proprii identității sale fizice, fiziologice, psihice, economice, culturale sau sociale. În componența datelor cu caracter personal se includ informațiile conținute în: buletinul de identitate sau un alt act de identitate, carnetul de muncă, documentele de evidență militară, certificatul medical, diploma de studii, fișa de studii, dosarul personal al studentului, polița de asigurare medicală.
6. Datele cu caracter personal ale studenților se prelucrează/stochează: pe suport de hârtie și/sau în format electronic (software și hardware).
7. Prelucrarea datelor se face prin softul: "Evidența studenților", iar mentenanța acestuia este efectuată de Departamentul de informatică.
8. Scopul prelucrării informațiilor ce conțin date cu caracter personal ale studenților constă în asigurarea înregistrării informațiilor referitoare și necesare pentru

desfășurarea următoarelor procese și activități: admiterea la studii, evidența studenților, planificarea și organizarea studiilor, promovarea studiilor, transferul studenților, exmatricularea și restabilirea la studii, absolvirea și certificarea studiilor și a prezentării rapoartelor de activitate și statistice către instituțiile statului, conform legislației în vigoare.

9. Datele cu caracter personal care fac obiectul prelucrării vor fi:
 - a) prelucrate în mod corect și conform prevederilor legii;
 - b) colectate în scopuri determinate, explicite și 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 științifică nu este considerată incompatibilă cu scopul colectării dacă se efectuează cu respectarea prevederilor legale în vigoare;
 - c) adecvate, pertinente și neexcesive în ceea ce privește scopul pentru care sunt colectate și/sau prelucrate ulterior;
 - d) exacte și, dacă este necesar, actualizate. Datele inexacte sau incomplete din punctul de vedere al scopului pentru care sunt colectate și ulterior prelucrate se șterg sau se rectifică;
 - e) stocate într-o formă care să permită identificarea subiecților datelor cu caracter personal pe o perioadă care nu va depăși durata necesară atingerii scopurilor pentru care sunt colectate și ulterior prelucrate.
10. La admitere la studii prelucrarea datelor cu caracter personal ale candidatului se efectuează cu consimțământul acestuia.
11. Prelucrarea datelor cu caracter personal ale studentului se efectuează fără consimțământul acestuia, deoarece se execută contractul de studii la care studentul este parte.
12. Prelucrarea datelor cu caracter personal privind starea de sănătate se permite pentru gestionarea serviciilor de sănătate și acordare de facilități pentru studenți.
13. Prelucrarea datelor cu caracter personal ale studenților se efectuează de următoarele subdiviziuni ale ASEM: Comisia de admitere, Departamentul studii, dezvoltare curriculară și management al calității, Departamentul de informatică, Decanatele facultăților, Școala masterală de excelență în economie și în business, Școala doctorală, Colegiul național de comerț. În fiecare subdiviziune, prin ordinul Rectorului ASEM, vor fi numite persoanele împuternicite să prelucreze datele cu caracter personal (*în continuare - utilizator*), cu indicarea responsabilităților concrete.
14. Utilizatorii vor prelucrea și accesa numai datele cu caracter personal necesare pentru îndeplinirea atribuțiilor lor de serviciu.
15. La încheierea operațiunilor de prelucrare, datele cu caracter personal se vor stoca în Arhiva ASEM și/sau în sistemul informațional de date cu caracter personal al ASEM.
16. La expirarea termenului de stocare, datele cu caracter personal vor fi distruse în modul stabilit de lege.

III. DREPTUL STUDENȚILOR

17. În conformitate cu legislația referitoare la protecția datelor cu caracter personal, studenții beneficiază de următoarele drepturi: la informare, de acces la date, de intervenție, de opoziție asupra datelor cu caracter personal ce-i vizează, precum și dreptul de a se adresa în justiție.
18. Toate persoanele implicate în activitatea de administrare și/sau prelucrare a informațiilor din cadrul procesului de studii vor respecta procedura de acces la datele cu caracter personal.
19. Acordarea dreptului de acces al studenților la informațiile ce-i vizează se efectuează doar prin solicitarea expresă, în formă scrisă, cu acordul nemijlocit al conducerii ASEM. Informațiile furnizate vor fi acordate astfel, încât să nu prejudicieze drepturile terților. Persoanele care solicită date cu caracter personal trebuie să indice scopul solicitării, precum și perioada concretă pentru care solicită informațiile.
20. Există posibilitatea refuzării dreptului de acces în situația în care se aplică excepțiile prevăzute de lege. Necesitatea de a restricționa accesul se poate impune în cazul în care există obligația de a proteja drepturile și libertățile unor terțe persoane, de exemplu, dacă în informațiile solicitate apar și alte persoane și nu există posibilitatea de a obține consimțământul acestora sau nu pot fi extrase, prin editare, datele cu caracter personal nerelevante.

IV. MĂSURI DE PROTECȚIE A DATELOR DIN CADRUL PROCESULUI DE STUDII

21. Măsurile generale de administrare a securității informaționale:
 - a) În cazul neutilizării temporare a purtătorilor de informație pe suport de hârtie sau electronic care conțin date preluate din cadrul procesului de studii, aceștia se păstrează în safeuri/dulapuri care se încuie.
 - b) La terminarea sesiunilor de lucru, computerele și imprimantele se deconectează de la rețeaua electrică.
 - c) Utilizatorul asigură securitatea punctelor de primire și expediere a corespondenței, precum și securitatea contra accesului neautorizat la aparatele de copiere.
 - d) Accesul fizic la mijloacele de reprezentare a informației preluate din cadrul procesului de studii este blocat împotriva vizualizării de către persoane neautorizate.
 - e) Mijloacele de prelucrare a informațiilor preluate din cadrul procesului de studii sau soft-urile destinate prelucrării acestora sunt scoase din perimetrul de securitate doar în baza permisiunii scrise a operatorului.
 - f) Scoaterea și introducerea mijloacelor de prelucrare a informațiilor din cadrul procesului de studii din/în perimetrul de securitate se înregistrează în registru.

22. Măsurile de protecție a datelor cu caracter personal, prelucrate în cadrul procesului de studii, se îndeplinesc ținând cont de necesitatea asigurării confidențialității și integrității acestora, prin protecție în formă manuală, electronică și externă.
23. Informația în format digital cu datele personale se copie automat, zilnic. Copiile de siguranță se testează în scopul verificării siguranței purtătorilor de informații și integrității informației indicate. Procedurile de restabilire a copiilor de siguranță se actualizează și se testează cu regularitate, în scopul asigurării eficacității acestora.
24. Cerințe speciale față de marcare: toate informațiile ieșite din cadrul procesului de studii, care conțin date cu caracter personal, sunt supuse marcării, cu indicarea prescripțiilor pentru prelucrarea ulterioară și diseminarea acestora.
25. Accesul în birourile unde sunt amplasate datele cu caracter personal din cadrul procesului de studii este restricționat, fiind permis doar persoanelor care au autorizația necesară și doar în timpul orelor de program. Accesul în birouri este posibil doar cu autorizarea de acces și cheia de la lacătul mecanic.
26. Birourile nu sunt lăsate niciodată fără supraveghere la ieșirea în exterior, ușa biroului se încuie cu lacătul.
27. Registrele de monitorizare se păstrează minimum un an, la expirarea termenului indicat, acestea se lichidează, iar datele și documentele ce se conțin în registrul supus lichidării se transmit în arhivă.
28. Perimetrul de securitate se consideră perimetrul birourilor în care sunt amplasate datele cu caracter personal din cadrul procesului de studii, fiind integrat din punct de vedere fizic.
29. Zilnic, se inspectează perimetrul de securitate al clădirii și al biroului, unde sunt amplasate datele cu caracter personal din cadrul procesului de studii, din punct de vedere fizic.
30. Computerele sunt amplasate în locuri cu acces limitat pentru persoane străine. Ușile și ferestrele sunt încuiate în cazul în care în încăperea angajații utilizatorii.
31. Amplasarea datelor cu caracter personal din cadrul procesului de studii răspunde necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.
32. Computerele, unde sunt amplasate datele cu caracter personal din cadrul procesului de studii, dispun de UPS-uri, care sunt folosite pentru încheierea corectă a sesiunii de lucru a sistemelor (componentelor) în cazul deconectării de la sursa de alimentare cu energie electrică.
33. Securitatea cablurilor de rețea: cablurile de rețea, prin care se efectuează operațiunile de transmitere a datelor preluate din sistemul de evidență contabilă, sunt protejate contra conectărilor nesancționate sau deteriorărilor. Pentru a exclude bruiatul, cablurile de tensiune sunt separate de cele comunicaționale.

34. Securitatea antiincendiară: birourile unde sunt amplasate datele cu caracter personal din cadrul procesului de studii sunt dotate cu echipament antiincendiar și corespunde cerințelor și normelor antiincendiară în vigoare.
35. Controlul instalării și scoaterii componentelor TI: se efectuează controlul și evidența instalării și scoaterii mijloacelor de program, mijloacelor tehnice și celor tehnice de program, utilizate în cadrul sistemului de evidență contabilă. La expirarea termenului de păstrare, informațiile, care conțin date cu caracter personal și care se conțin pe purtătorii de informații, se distrug.

V. IDENTIFICAREA ȘI AUTENTIFICAREA UTILIZATORILOR INFORMAȚIILOR PRELUATE DIN CADRUL PROCESULUI DE STUDII

36. Este efectuată identificarea și autentificarea utilizatorilor informațiilor preluate din cadrul procesului de studii și a proceselor executate în numele acestor utilizatori.
37. Toți utilizatorii (inclusiv personalul care asigură mentenanța tehnică, administratorii de rețea, programatorii și administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu trebuie să conțină semnalmentele nivelului de accesibilitate al utilizatorului.
38. Pentru confirmarea ID-ului utilizatorului sunt utilizate parole. Utilizarea parolelor în procesul asigurării securității informaționale: pe lângă cerințele de păstrare a confidențialității parolelor, este interzisă înscrierea acestora pe suport de hârtie, cu excepția cazului de asigurare a securității păstrării acestora (plasarea înscrisurilor în safeu). La momentul introducerii, parolele nu se reflectă în clar pe monitor.
39. Se efectuează modificarea parolelor de fiecare dată când sunt depistați indicii unei eventuale compromiteri a sistemului sau parolei.
40. Întru asigurarea posibilității de stabilire a responsabilității fiecărui utilizator, sunt folosite identificatori și parole individuale ale acestora. Este asigurată posibilitatea utilizatorilor de a alege și schimba parolele individuale, inclusiv de activare a procedurii de evidență a introducerilor greșite ale acestora. După cinci tentative greșite de autentificare, accesul este blocat, în mod automatizat.
41. Se asigură, pentru o perioadă de 1 (*unu*) ani, păstrarea istoriilor anterioare ale parolelor în formă de hash a utilizatorilor și prevenirea folosirii repetate a acestora.
42. În cazul în care raporturile de muncă ale utilizatorului au încetat, au fost suspendate sau modificate, și, ca urmare, noile sarcini nu necesită accesul la datele cu caracter personal, precum și 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 și autentificare se revocă sau se suspendă.
43. Se efectuează, prin mijloace automatizate de suport, administrarea conturilor de acces a utilizatorilor care prelucrează datele cu caracter personal din cadrul

procesului de studii, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea și ștergerea acestora. Acțiunea conturilor de acces a utilizatorilor temporari, care prelucrează date cu caracter personal, încetează automat la expirarea perioadei stabilite în timp (pentru fiecare tip de cont de acces în parte). Se dezactivează automat, după o perioadă de maxim 1 (*una*) lună, conturile de acces ale utilizatorilor neactivi, care prelucrează informațiile din cadrul procesului de studii. Se folosesc mijloace automatizate de înregistrare și informare despre crearea, modificarea, dezactivarea și încetarea acțiunii conturilor de acces.

44. În scopul depistării și evitării cazurilor de acordare a drepturilor de acces neautorizat, se revizuieste cu regularitate, maximum la fiecare șase luni și după oricare schimbare a statutului utilizatorului, drepturile de acces ale.
45. Folosirea tehnologiilor fără fir, echipamentelor portative și mobile se autorizează de persoanele responsabile.
46. Se impun limite în privința persoanelor care au dreptul să vizualizeze informațiile stocate în sistemul de evidență contabilă și să copieze, să descarce, să șteargă sau să modifice orice informație stocată.
47. Toți angajații cu drepturi de acces beneficiază de o instruire inițială în domeniul protecției datelor cu caracter personal.
48. Orice activitate de dezvăluire a datelor cu caracter personal către terți este documentată și supusă unei analize riguroase în prealabil privind scopul și temeiul legal a intențiilor de dezvăluire a unui anumit volum de date cu caracter personal.
49. Utilizatorul dezvăluie datele cu caracter personal către terți, doar la indicația în scris a Rectorului ASEM.
50. Orice încălcare a securității în ceea ce privește 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.
51. Înainte de acordarea accesului la datele cu caracter personal ale studenților, utilizatorii sunt informați despre faptul că sistemul informațional al datelor cu caracter personal este controlat și că folosirea neautorizată a acestora este sancționată în conformitate cu legislația civilă, contravențională și penală.

VI. CONTROL ȘI ÎMBUNĂȚIRE

52. Persoana responsabilă de realizarea politicii de securitate va organiza anual un audit referitor la protecția datelor cu caracter personal ale studenților.
53. Departamentul Studii, Dezvoltare Curriculară și Management al calității va iniția acțiuni corective și preventive pentru a eficientiza procesele referitoare la protecția datelor cu caracter personal ale studenților.
54. Departamentul de Informatică va asigura identificarea, protocolarea și înlăturarea deficiențelor de soft-uri destinate prelucrării informațiilor cu caracter personal ale studenților, inclusiv instalarea corectărilor și pachetelor de reînnoire

a acestora, protecția contra infiltrării programelor dăunătoare în soft-uri, măsuri care asigură posibilitatea reînnoirii automate și la timp a mijloacelor de asigurare a protecției contra programelor dăunătoare și signaturilor de virus.

55. Departamentul de Informatică va face periodic controlul autentificărilor și tipurilor de acces pentru detectarea unor disfuncționalități în ceea ce privește folosirea echipamentelor și sistemelor de telecomunicații.

VII. DISPOZIȚII FINALE

56. Prezentul Regulament poate fi revizuit periodic, în funcție de modificările și completările legislative aplicabile, precum și de nivelul de dezvoltare tehnologică.
57. Regulamentul este adus la cunoștința angajaților contra semnătură.
58. Prezentul Regulament intră în vigoare din momentul aprobării de către Senatul ASEM.