APROBAT
la ședința Senatului USEM
din 23 decembrie **2015**
Iu.Sedlețchi

REGULAMENT
PRIVIND PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL ALE SERVICIULUI RESURSE UMANE A UNIVERSITĂȚII DE STUDII EUROPENE DIN MOLDOVA

I. DISPOZIȚII GENERALE

1. Prezentul Regulament stabilește regulile privind prelucrarea și protecția datelor cu caracter personal ale beneficiarilor de servicii educaționale oferite de USEM, respectiv: cadre didactice, personal auxiliar (în continuare - angajați), în cadrul serviciului resurse umane.

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 USEM, în calitate de operator de date cu caracter personal, le are în domeniul protecției datelor cu caracter personal ale angajaților, în relațiile instituției cu angajații în cadrul activității, cu alte instituții de învățământ, precum și cu alte persoane fizice sau juridice.

II. CADRUL INSTITUȚIONAL PRIVIND PRELUCRARE DATELOR CU CARACTER PERSONAL ALE ANGAJAȚILOR USEM

4. USEM 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 informaţie 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 identităţii sale fizice, fiziologice, psihice, economice, culturale sau sociale. În componenţa datelor cu caracter personal se includ informaţiile conţinute în: buletinul de identitate sau un alt act de identitate, carnetul de muncă, documentele de evidenţă militară, certificatul medical, actele de studii, fişa de personal, dosarul personal al angajatului, poliţa de asigurare medicală.

6. Datele cu caracter personal ale angajaţilor se relucrează/stochează: pe suport de hârtie şi/sau în format electronic (software şi hardware).

7. Prelucrarea datelor se face prin softul: "Evidenţa angajaţilor", iar mentenanţa acestuia este efectuată de Departamentul de informatică.

8. Scopul prelucrării informaţiilor ce conţin date cu caracter personal ale angajaţilor constă în asigurarea înregistrării informaţiilor referitoare şi necesare pentru desfăşurarea următoarelor procese şi activităţi: angajarea în câmpul muncii, evidenţa angajaţilor, promovarea angajaţilor, transferul angajaţilor, eliberarea angajaţilor şi a prezentării rapoartelor de activitate şi statistice către instituţiile statului, conform legislaţiei în vigoare.

9. 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 ştiinţifică 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 subiecţilor datelor cu caracter personal pe o perioadă care nu va depăşi durata necesară atingerii scopurilor pentru care sunt colectate şi ulterior prelucrate.

10. La angajarea la serviciu prelucrarea datelor cu caracter personal ale angajatului se efectuează cu consimţământul acestuia.

11. Prelucrarea datelor cu caracter personal ale angajatului USEM se efectuează fără consimţământul acestuia, deoarece se execută contractul de muncă la care angajatul este parte.

12. Prelucrarea datelor cu caracter personal privind starea de sănătate se permite pentru gestionare a serviciilor de sănătate și acordare de facilități pentru angajați.

13. Prelucrarea datelor cu caracter personal ale angajaților se efectuează de următoarele subdiviziuni: Serviciul Resurse Umane; Direcția economico-financiară; decanatele facultăților, catedrele facultăților; școala doctorală.

În fiecare subdiviziune, prin ordinul Rectorului USEM, vor fi numite persoanele împuternicite să prelucreze datele cu caracter personal (în continuare - utilizator), cu indicarea responsabilităților concrete.

14. Utilizatorii vor prelucra 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 USEM și/sau în sistemul informațional de date cu caracter personal al USEM.

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

DREPTUL ANGAJAȚILOR

17. În conformitate cu legislația referitoare la protecția datelor cu caracter personal, angajații 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 serviciului resurse umane vor respecta procedura de acces la datele cu caracter personal.

19. Acordarea dreptului de acces al angajaților la informațiile ce-i vizează se efectuează doar prin solicitarea expresă, în formă scrisă, cu acordul nemijlocit al conducerii USEM. 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 PROTECŢIE A DATELOR DIN CADRUL SERVICIULUI RESURSE UMANE

21. Măsurile generale de administrare a securităţii informaţionale:

a) În cazul neutilizării temporare a purtătorilor de informaţie pe suport de hârtie sau electronic care conţin date preluate din cadrul serviciului resurse umane, aceştia se păstrează în safeuri /dulapuri care se încuie.

b) La terminarea zilei de muncă, computerele şi imprimantele se deconectează de la reţeaua electrică.

c) Utilizatorul asigură securitatea punctelor de primire şi expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele de copiere.

d) Accesul fizic la mijloacele de reprezentare a informaţiei preluate din cadrul serviciului resurse umane este blocat împotriva vizualizării de către persoane neautorizate.

e) Mijloacele de prelucrare a informaţiilor preluate din cadrul serviciului resurse umane sau soft - urile destinate prelucrării acestora sunt scoase din perimetrul de securitate doar în baza permisiunii scrise a operatorului.

f) Scoaterea şi introducerea mijloacelor de prelucrare a informaţiilor din cadrul serviciului resurse umane din/în perimetrul de securitate se înregistrează în registru.

22. Măsurile de protecţie a datelor cu caracter personal, prelucrate în cadrul serviciului resurse umane, se înfăptuiesc ţinând cont de necesitatea asigurării confidenţialităţii şi integrităţii acestora, prin protecţie în formă manuală, electronică şi externă.

23. Informaţia în format digital cu datele personale se copie automat, zilnic. Copiile de siguranţă se testează în scopul verificării siguranţei purtătorilor de informaţii şi integrităţii informaţiei indicate. Procedurile de restabilire a copiilor de siguranţă se actualizează şi se testează cu regularitate, în scopul asigurării eficacităţii acestora.

24. Cerinţe speciale faţă de marcare:toate informaţiile ieşite din cadrul serviciului resurse umane, care conţin date cu caracter personal, sunt supuse marcării, cu indicarea prescripţiilor pentru prelucrarea ulterioară şi diseminarea acestora.

25. Accesul în birourile unde sunt amplasate datele cu caracter personal din cadrul serviciului resurse umane este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară şi doar în timpul orelor de program. Accesul în birouri este posibil doar cu autorizarea de acces şi cheia de la lacătul mecanic.

26. Birourile nu sunt lăsate niciodată fără supraveghere la ieşirea în exterior, uşa biroului se încuie cu lacătul.

27. Registrele de monitorizare se păstrează minimum un an, la expirarea termenului indicat, acestea se lichidează, iar datele şi documentele ce se conţin 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 serviciului resurse umane, fiind integru din punct de vedere fizic.

29. Zilnic, se inspectează perimetrul de securitate al clădirii şi al biroului, unde sunt amplasate datele cu caracter personal din cadrul serviciului resurse umane, din punct de vedere fizic.

30. Computerele sunt amplasate în locuri cu acces limitat pentru persoane străine. Uşile şi ferestrele sunt încuiate în cazul în care în încăpere angajaţii utilizatorii.

31. Amplasarea datelor cu caracter personal din cadrul serviciului resurse umane răspunde necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.

32. Computerele, unde sunt amplasate datele cu caracter personal din cadrul serviciului resurse umane, 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 reţea: cablurile de reţea, prin care se efectuează operaţiunile de transmitere a datelor preluate din sistemul de evidenţă contabilă, sunt protejate contra conectărilor nesancţionate sau deteriorărilor. Pentru a exclude bruiajul, cablurile de tensiune sunt separate de cele comunicaţionale.

34. Securitatea antiincendiară: birourile unde sunt amplasate datele cu caracter personal din cadrul procesului de studii sunt dotate cu echipament antiincendiar şi corespunde cerinţelor şi normelor antiincendiare în vigoare.

35. Controlul instalării şi scoaterii componentelor TI: se efectuează controlul şi evidenţa instalării şi scoaterii mijloacelor de program, mijloacelor tehnice şi celor tehnice de program, utilizate în cadrul sistemului de evidenţă contabilă. La expirarea termenului de păstrare, informaţiile, care conţin date cu caracter personal şi care se conţin pe purtătorii de informaţii, se distrug.

V. IDENTIFICAREA ŞI AUTENTIFICAREA UTILIZATORILOR INFORMAŢIILOR PRELUATE DIN CADRUL SERVICIULUI RESURSE UMANE

36. Este efectuată identificarea şi autentificarea utilizatorilor informaţiilor preluate din cadrul serviciului resurse umane şi a proceselor executate în numele acestor utilizatori.

37. Toţi utilizatorii (inclusiv personalul care asigură mentenanţa tehnică, administratorii de reţea, programatorii şi administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu trebuie să conţină semnalmentele nivelului de accesibilitate al utilizatorului.

38. Pentru confirmarea ID-ului utilizatorului sunt utilizate parole. Utilizarea parolelor în procesul asigurării securităţii informaţionale: pe lângă cerinţele de păstrare a confidenţialităţii parolelor, este interzisă înscrierea acestora pe suport de hârtie, cu excepţia cazului de asigurare a securităţii păstrării acesteia (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 depistaţi indicii unei eventuale compromiteri a sistemului sau parolei.

40. Întru asigurarea posibilităţii de stabilire a responsabilităţii fiecărui utilizator, sunt folosite identificatori şi parole individuale ale acestora. Este asigurată posibilitatea utilizatorilor de a alege şi schimba parolele individuale, inclusiv de activare a procedurii de evidenţă a introducerilor greşite ale acestora. După cinci tentative greşite 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 şi prevenirea folosirii repetate a acestora.

42. 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 autorizaţii de acces primite în scopul comiterii unei fapte prejudiciabile, absenţă 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.

43. Se efectuează, prin mijloace automatizate de suport, administrarea conturilor de acces a utilizatorilor care prelucrează datele cu caracter personal din cadrul serviciului resurse umane, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea şi ştergerea acestora. Acţiunea 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 informaţiile din cadrul serviciului resurse umane. Se folosesc mijloace automatizate de înregistrare

şi informare despre crearea, modificarea, dezactivarea şi încetarea acţiunii conturilor de acces.

44. 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.

45. Folosirea tehnologiilor fără fir, echipamentelor portative şi mobile se autorizează de persoanele responsabile.

46. Se impun limite în privinţa persoanelor care au dreptul să vizualizeze informaţiile stocate în sistemul de evidenţă contabilă şi să copieze, să descarce, să şteargă sau să modifice orice informaţie stocată.

47. Toţi angajaţii cu drepturi de acces beneficiază de o instruire iniţială în domeniul protecţiei datelor cu caracter personal.

48. Orice activitate de dezvăluire a datelor cu caracter personal către terţi este documentată şi supusă unei analize riguroase în prealabil privind scopul şi temeiul legal a intenţiilor de dezvăluire a unui anumit volum de date cu caracter personal.

49. Utilizatorul dezvăluie datele cu caracter personal către terţi, doar la indicaţia în scris a Rectorului USEM.

50. Orice încălcare a securităţii 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.

51. Înainte de acordarea accesului la datele cu caracter personal ale angajaţilor, utilizatorii sunt informaţi despre faptul că sistemul informaţional al datelor cu caracter personal este controlat şi că folosirea neautorizată a acestora este sancţionată în conformitate cu legislaţia civilă, contravenţională şi penală.

VI. CONTROL ŞI ÎMBUNĂTĂŢIRE

52. Persoana responsabilă de realizarea politicii de securitate va organiza anual un audit referitor la protecţia datelor cu caracter personal ale angajaţilor.

53. Serviciul resurse umane va iniţia acţiuni corective şi preventive pentru a eficientiza procesele referitoare la protecţia datelor cu caracter personal ale angajaţilor.

54. Departamentul de Informatică va asigura identificarea, protocolarea şi înlăturarea deficienţelor de soft-uri destinate prelucrării informaţiilor cu caracter personal ale angajaţilor, inclusiv instalarea corectărilor şi pachetelor de reînnoire a acestora, protecţia contra infiltrării programelor dăunătoare în soft-uri, măsuri care

asigură posibilitatea reînnoirii automate şi la timp a mijloacelor de asigurare a protecţiei contra programelor dăunătoare şi signaturilor de virus.

55. Departamentul de Informatică va face periodic controlul autentificărilor şi tipurilor de acces pentru detectarea unor disfuncţionalităţi în ceea ce priveşte folosirea echipamentelor şi sistemelor de telecomunicaţii.

VII. DISPOZIŢII FINALE

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

57. Regulamentul este adus la cunoştinţa angajaţilor contra semnătură.

58. Prezentul Regulament intră în vigoare din momentul aprobării de către Senatul USEM.