GUVERNUL REPUBLICII MOLDOVA

ACADEMIA DE ADMINISTRARE PUBLICĂ

APROB:

Oleg BALAN,

Rector

O. Balan 2017

12.11.17.

REGULAMENTUL

PRIVIND PRELUCRAREA ŞI PROTECŢIA DATELOR CU CARACTER PERSONAL ALE STUDENŢILOR ÎN CADRUL ACADEMIEI DE ADMINISTRARE PUBLICĂ

Chişinău, 2017

I. DISPOZIŢII GENERALE

1. Prezentul Regulament stabileşte regulile privind prelucrarea şi protecţia datelor cu caracter personal ale beneficiarilor de servicii educaţionale (*în continuare - studenţi*), oferite de Academia de Administrare Publică (*în continuare - AAP*), în cadrul procesului de studii.
2. Regulamentul este elaborat în temeiul prevederilor:
   - Codului Educaţiei al Republicii Moldova nr. 152 din 17.07.2014;
   - Legii nr. 133 din 08.07.2011 privind protecţia datelor cu caracter personal;
   - Hotărârii Guvernului nr.1123 din 14.12.2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal.
3. Reglementările cuprinse în prezentul Regulament stabilesc exercitarea drepturilor şi obligaţiilor pe care AAP, în calitate de operator de date cu caracter personal, le are în domeniul protecţiei datelor cu caracter personal ale studenţilor, în relaţiile instituţiei cu studenţii în cadrul procesului de studii, cu alte instituţii de învăţământ, precum şi cu alte persoane fizice sau juridice.

II. CADRUL INSTITUŢIONAL PRIVIND PRELUCRARE DATELOR CU CARACTER PERSONAL ALE STUDENŢILOR

4. AAP asigură prelucrarea datelor cu caracter personal 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, diploma de studii, fişa de studii, dosarul personal al studentului, poliţa de asigurare medicală.
6. Datele cu caracter personal ale studenţilor se prelucrează/stochează: pe suport de hârtie şi/sau în format electronic (software şi hardware).
7. Prelucrarea datelor se face prin softul: "Evidenţa studenţilor", iar mentenanţa acestuia este efectuată de Departamentul studii superioare de master.
8. Scopul prelucrării informaţiilor ce conţin date cu caracter personal ale studenţilor constă în asigurarea înregistrării informaţiilor referitoare şi necesare pentru desfăşurarea următoarelor procese şi activităţi: admiterea la studii, evidenţa studenţilor, planificarea şi organizarea studiilor, promovarea studiilor, transferul studenţilor, exmatricularea şi restabilirea la studii, absolvirea şi certificarea studiilor 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 admitere la studii prelucrarea datelor cu caracter personal ale candidatului se efectuează cu consimţământul acestuia.
11. Prelucrarea datelor cu caracter personal ale studenţilor se efectuează de următoarele subdiviziuni ale AAP: Comisia de admitere, Departamentul studii superioare de master, Catedrele, Şcoala doctorală, Direcţia managementul personalului şi relaţii publice. În fiecare subdiviziune, prin ordinul Rectorului, vor fi numite persoanele împuternicite să prelucreze datele cu caracter personal, cu indicarea responsabilităţilor concrete.
12. Utilizatorii vor prelucra şi accesa numai datele cu caracter personal necesare pentru îndeplinirea atribuţiilor lor de serviciu.
13. La încheierea operaţiunilor de prelucrare, datele cu caracter personal se vor stoca în Arhiva AAP şi/sau în sistemul informaţional de date cu caracter personal al AAP.
14. La expirarea termenului de stocare, datele cu caracter personal vor fi distruse în modul stabilit de lege.

III. DREPTUL STUDENŢILOR

15. În conformitate cu legislaţia referitoare la protecţia datelor cu caracter personal, studenţii beneficiază de următoarele drepturi: la informare, de acces la date, de intervenţie, de opoziţie asupra datelor cu caracter personal ce-i vizează, precum şi dreptul de a se adresa în justiţie.
16. Toate persoanele implicate în activitatea de administrare şi/sau prelucrare a informaţiilor din cadrul procesului de studii vor respecta procedura de acces la datele cu caracter personal.
17. Acordarea dreptului de acces al studenţilor la informaţiile ce-i vizează se efectuează doar prin solicitarea expresă, în formă scrisă, cu acordul nemijlocit al conducerii AAP. Informaţiile furnizate vor fi acordate astfel, încât să nu prejudicieze drepturile terţilor. Persoanele care solicită date cu caracter personal trebuie să indice scopul solicitării, precum şi perioada concretă pentru care solicită informaţiile.
18. Există posibilitatea refuzării dreptului de acces în situaţia în care se aplică excepţiile prevăzute de lege. Necesitatea de a restricţiona accesul se poate impune în cazul în care există obligaţia de a proteja drepturile şi libertăţile unor terţe persoane, de exemplu, dacă în informaţiile solicitate apar şi alte persoane şi nu există posibilitatea de a obţine consimţământul acestora sau nu pot fi extrase, prin editare, datele cu caracter personal nerelevante.

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

19. 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 procesului de studii, aceştia se păstrează în safeuri/dulapuri care se încuie.
    b) La terminarea sesiunilor de lucru, 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 procesului de studii este blocat împotriva vizualizării de către persoane neautorizate.

e) Mijloacele de prelucrare a informaţiilor 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 şi introducerea mijloacelor de prelucrare a informaţiilor din cadrul procesului de studii din/în perimetrul de securitate se înregistrează în registru.

20. Măsurile de protecţie a datelor cu caracter personal, prelucrate în cadrul procesului de studii, se înfăptuiesc ţinând cont de necesitatea asigurării confidenţialităţii şi integrităţii acestora, prin protecţie în formă manuală, electronică şi externă.
21. 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.
22. Cerinţe speciale faţă de marcare: toate informaţiile ieşite din cadrul procesului de studii, care conţin date cu caracter personal, sunt supuse marcării, cu indicarea prescripţiilor pentru prelucrarea ulterioară şi diseminarea acestora.
23. Accesul în birourile unde sunt amplasate datele cu caracter personal din cadrul procesului de studii 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.
24. Birourile nu sunt lăsate niciodată fără supraveghere la ieşirea în exterior, uşa biroului se încuie cu lacătul.
25. 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.
26. Perimetrul de securitate se consideră perimetrul birourilor în care sunt amplasate datele cu caracter personal din cadrul procesului de studii, fiind integru din punct de vedere fizic.
27. Zilnic, se inspectează perimetrul de securitate al clădirii şi al biroului, unde sunt amplasate datele cu caracter personal din cadrul procesului de studii, din punct de vedere fizic.
28. Computerele sunt amplasate în locuri cu acces limitat pentru persoane străine. Uşile şi ferestrele sunt încuiate în cazul în care în încăpere angajaţii utilizatorii.
29. Amplasarea datelor cu caracter personal din cadrul procesului de studii răspunde necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.
30. 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.
31. 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.
32. 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.
33. 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 PROCESULUI DE STUDII

34. Este efectuată identificarea şi autentificarea utilizatorilor informaţiilor preluate din cadrul procesului de studii şi a proceselor executate în numele acestor utilizatori.
35. 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.
36. 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.
37. Se efectuează modificarea parolelor de fiecare dată când sunt depistaţi indicii unei eventuale compromiteri a sistemului sau parolei.
38. 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.
39. 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.
40. 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.
41. 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 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 procesului de studii. Se folosesc mijloace automatizate de înregistrare şi informare despre crearea, modificarea, dezactivarea şi încetarea acţiunii conturilor de acces.
42. 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.
43. Folosirea tehnologiilor fără fir, echipamentelor portative şi mobile se autorizează de persoanele responsabile.

44. 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.
45. Toţi angajaţii cu drepturi de acces beneficiază de o instruire iniţială în domeniul protecţiei datelor cu caracter personal.
46. 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.
47. Utilizatorul dezvăluie datele cu caracter personal către terţi, doar la indicaţia în scris a Rectorului AAP.
48. 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.
49. Înainte de acordarea accesului la datele cu caracter personal ale studenţilor, 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

50. Persoana responsabilă de realizarea politicii de securitate va organiza anual un audit referitor la protecţia datelor cu caracter personal ale studenţilor.
51. Departamentul Studii superioare de master va iniţia acţiuni corective şi preventive pentru a eficientiza procesele referitoare la protecţia datelor cu caracter personal ale studenţilor.
52. Direcţia generală logistică (ingineri electronişti/programatori):
- va asigura identificarea, protocolarea şi înlăturarea deficienţelor de soft-uri destinate prelucrării informaţiilor cu caracter personal ale studenţilor, 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.
- 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

53. Prezentul Regulament poate fi revizuit periodic, în funcţie de modificările şi completările legislative aplicabile, precum şi de nivelul de dezvoltare tehnologică.
54. Regulamentul este adus la cunoştinţa angajaţilor contra semnătură.