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 ÎN CADRUL DIRECŢIEI PLANIFICARE ŞI EVIDENŢĂ CONTABILĂ A ACADEMIEI DE ADMINISTRARE PUBLICĂ

Chişinău, 2017

I. DISPOZIŢII GENERALE

1. Prezentul Regulament are ca scop stabilirea unor reguli pentru asigurarea unui nivel satisfăcător de protecţie a datelor cu caracter personal (în continuare, DCP) prelucrate de către Direcţia Planificare şi evidenţă contabilă (DPEC) a Academiei de Administrare Publică (AAP), în calitate de operator de date cu caracter personal.

2. Regulamentul este elaborat în temeiul prevederilor:

- Legii nr. 133 din 08.07.2011 privind protecţia 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 Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal (Monitorul Oficial al Republicii Moldova, 2010, nr. 254-256, art. 1282).

3. Reglementările cuprinse în prezentul Regulament stabilesc condiţiile generale şi cerinţele faţă de prelucrarea datelor cu caracter personal ale studenţilor şi angajaţilor AAP, precum şi ale altor persoane fizice sau juridice.

II. CADRUL INSTITUŢIONAL PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL

1. Scopul prelucrării informaţiilor ce conţin date cu caracter personal, în DPEC, constă în asigurarea înregistrării informaţiilor referitoare şi necesare pentru îndeplinirea obligaţiunilor direcţiei, respectiv:

a) ale studenţilor de la ciclurile II şi III de învăţământ – perfectarea contractelor de studii cu achitarea taxei, evidenţa achitărilor şi planificarea veniturilor din taxele de studii;

b) ale angajaţilor – stabilirea salariului lunar, inclusiv a premiilor, sporurilor şi altor stimulări salariale, în conformitate cu legislaţia în vigoare a Republicii Moldova;

c) ale altor persoane fizice sau juridice – pentru perfectarea contractelor arendă, comodat etc..

2. În cadrul sistemului de evidenţă, sunt prelucrate următoarele categorii de date cu caracter personal:

a) numele, prenumele şi patronimicul;

b) cod numeric personal (IDNP)/cod fiscal;

c) telefon/fax/email;

d) adresa sau reşedinţa;

e) starea de sănătate;

f) mărimea burselor, indemnizaţiilor;

g) mărimea salariului brut şi alte premii, sporuri, stimulări, suplimente;

h) după caz, alte date necesare îndeplinirii scopului menţionat, conform legislaţiei în vigoare.

3. Datele cu caracter personal sunt:

a) acumulate în scopuri determinate, explicite şi legitime, prelucrate într-un mod adecvat, compatibil 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 legislaţiei în vigoare;

b) actualizate, după caz. Datele inexacte sau incomplete, din punctul de vedere al scopului pentru care sunt acumulate, după prelucrare sunt rectificate sau excluse (anulate) din baza de date;

c) 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.

4. La admitere la studii, cât şi la angajare, a persoanelor, în cadrul AAP, prelucrarea datelor cu caracter personal se efectuează cu consimţământul acestora (acord în formă scrisă).

5. Prelucrarea ulterioară a datelor cu caracter personal ale persoanelor vizate se efectuează fără consimţământul acestora, în legătură cu executarea obligaţiilor contractuale la care s-au obligat părţile.

6. Acumularea datelor cu caracter personal privind starea de sănătate se permite pentru acordarea facilităţilor studenţilor (burse).

7. Datele cu caracter personal se prelucrează/se stochează atât pe suport de hârtie, cât şi în formă electronică.

8. Mentenanţa bazelor de date este efectuată de către DPEC cu suportul Direcţiei generale logistică (ingineri- electronişti/programatori), cu următoarele atribuţii:

a) efectuarea ajustărilor în program, în baza modificărilor legislaţiei RM;

b) eliminarea erorilor în funcţionarea programului;

c) examinarea solicitărilor parvenite din partea dpec;

d) examinarea şi nedivulgarea informaţiei cu accesibilitate limitată.

9. Prelucrarea informaţiilor pe suport de hârtie este structurată după criteriul "mape-dosare", fiind păstrate în dulapuri, care sunt amplasate fizic în birourile DPEC.

10.Utilizatorii datelor cu caracter personal din cadrul DPEC sunt responsabili pentru aceste date şi vor prelucra şi accesa numai datele cu caracter personal necesare pentru îndeplinirea atribuţiilor lor de serviciu.

11. Informaţiile înregistrate pot fi comunicate numai persoanelor vizate, reprezentanţilor legali ai acestora sau autorităţilor publice în cadrul unei competenţe speciale de anchetă (*serviciile financiare şi fiscale, de poliţie, justiţie, securitate socială*), prin solicitarea în formă scrisă, cu acordul conducerii AAP. Persoanele care solicită date cu caracter personal trebuie să indice scopul solicitării, perioada concretă pentru care solicită informaţiile şi să anexeze documentul ce atestă dreptul de a solicita şi primi informaţia în cauză.

12. 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, primind statut de document de arhivă.

III. DREPTURILE PERSOANELOR VIZATE

1. În conformitate cu principiile de protecţie a datelor cu caracter personal, persoanele vizate beneficiază de următoarele drepturi: la informare, de acces la datele personale, de intervenţie, de

opoziţie asupra datelor cu caracter personal ce-i vizează, precum şi dreptul de a se adresa în justiţie.

2. Acordarea dreptului de acces al persoanelor la informaţiile cu caracter personal, ce-i vizează, se efectuează doar prin solicitarea expresă, în formă scrisă, datată şi semnată, cu acordul nemijlocit al conducerii AAP. Solicitantul este în drept să primească informaţia şi la adresa juridică (poştă electronică sau serviciu de corespondenţă), dacă are siguranţa că la informaţia în cauză nu vor avea acces persoane străine.

3. AAP poate refuza eliberarea informaţiei ce conţine date cu caracter personal, în condiţiile legii (restricţionarea eliberării). Necesitatea de a restricţiona accesul la DCP 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 DPEC

1. DPEC are obligaţia de a lua toate măsurile tehnice şi organizatorice necesare pentru păstrarea datelor cu caracter personal la un nivel de securitate adecvat.

2. 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 dulapuri cu acces restricţionat.

b. Accesul la baza de date se face doar de către utilizatorii DPEC. Contul de utilizator este însoţit de o modalitate de autentificare pentru fiecare calculator. Autentificarea se realizează prin introducerea unei parole.

c. La terminarea sesiunilor de lucru, calculatoarele şi imprimantele sunt deconectate.

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

e. Accesul fizic la mijloacele de reprezentare a informaţiei preluate din cadrul DPEC este interzis persoanelor neautorizate.

3. Informaţia în format digital ce conţine date personale se copiază 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.

4. Accesul în birourile unde sunt amplasate datele cu caracter personal, utilizate în cadrul DPEC, 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.

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

6. Registrele de monitorizare se păstrează minimum trei ani, la expirarea termenului indicat, acestea se lichidează, iar datele şi documentele ce se conţin în registrul supus lichidării se transmit în arhivă.

7. Perimetrul de securitate se consideră perimetrul birourilor în care sunt amplasate datele cu caracter personal din cadrul procesului de studii, fiind integral din punct de vedere fizic. Calculatoarele sunt amplasate în locuri cu acces limitat pentru persoanele străine.

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

9. Calculatoarele, unde sunt amplasate datele cu caracter personal utilizate în cadrul procesului de lucru, 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.

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

V. IDENTIFICAREA ŞI AUTENTIFICAREA UTILIZATORILOR

1. Este efectuată identificarea şi autentificarea utilizatorilor sistemelor informaţionale de date cu caracter personal şi a proceselor executate în numele acestor utilizatori.

2. Toţi utilizatorii (inclusiv personalul care asigură susţinerea 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.

3. 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.

4. Se efectuează modificarea parolelor de fiecare dată când sunt depistaţi indicii unei eventuale compromiteri a sistemului sau parolei.

5. 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 automat.

6. 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 al 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.

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

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

9. Orice activitate de dezvăluire a datelor cu caracter personal către terţi este documentată şi supusă unei analize riguroase, identificând scopul şi temeiul legal al intenţiilor de dezvăluire a unui anumit volum de date cu caracter personal.

10. Orice încălcare a securităţii în ceea ce priveşte protejarea datelor cu caracter personal este supusă documentării, iar persoana responsabilă de realizarea politicii de securitate este informată în legătură cu acest lucru cât mai urgent.

11. Înainte de acordarea accesului la datele cu caracter personal, 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

1. DPEC va iniţia acţiuni corective şi preventive pentru a eficientiza procesele referitoare la protecţia datelor cu caracter personal ale studenţilor.

2. Direcţia generală logistică (ingineri- electronişti):

- va asigura identificarea, protocolarea şi înlăturarea deficienţelor de soft-uri destinate prelucrării informaţiilor cu caracter personal ale studenţilor, angajaţilor şi altor persoane fizice/juridice, 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

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

2. Regulamentul este adus la cunoştinţa utilizatorilor (angajaţilor) DPEC, contra semnătură.