UNIVERSITATEA PEDAGOGICĂ DE STAT „ION CREANGĂ”
DIN CHIȘINĂU

REGULAMENT
PRIVIND PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL A ANGAJAȚILOR UNIVERSITĂȚII PEDAGOGICE DE STAT „ION CREANGĂ” DIN CHIȘINĂU

CHIȘINĂU, 2017

UNIVERSITATEA PEDAGOGICĂ DE STAT „ION CREANGĂ”
DIN CHIȘINĂU

REGULAMENT
PRIVIND PRELUCRAREA ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL A ANGAJAȚILOR UNIVERSITĂȚII PEDAGOGICE DE STAT „ION CREANGĂ” DIN CHIȘINĂU

	Elaborat	Coordonat	Coordonat și verificat	Aprobat
Responsabil	SPÎNU Tatiana, șef DRU	CECAN Roman, șef CTI	CUȘCĂ Valentin, prorector pentru învățământul cu frecvență redusă, formare continuă și activitate financiară	CHICUȘ Nicolae, rector UPSC
Data	01.09.2017	06.09.2017	15.09.2017	Proces-verbal nr. 2 al ședinței Senatului UPSC din 28.09.2017
Semnătura				

CUPRINS

I. DISPOZIŢII GENERALE

1. Regulamentul privind prelucrarea şi protecţia datelor cu caracter personal a angajaţilor Universităţii Pedagogice de Stat „Ion Creangă" din Chişinău (în continuare Regulament) este elaborat în vederea implementării în cadrul Universităţii Pedagogice de Stat „Ion Creangă" din Chişinău (în continuare UPSC) a prevederilor art. 91 - 94 ale Codului Muncii al Republicii Moldova, Legii nr.133 din 08 iulie 2011 *Privind protecţia datelor cu caracter personal*, Codului Educaţional Nr. 152 din 17.07.2014 şi a Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr.1123 din 14 decembrie 2010, precum şi întru realizarea prevederilor Politicii de securitate privind protecţia datelor cu caracter personal şi prelucrarea acestora.
2. Prezentul Regulament reglementează condiţiile generale şi cerinţele faţă de prelucrarea datelor cu caracter personal, stabileşte modul, condiţiile şi procedurile de protecţie a datelor cu caracter personal a angajaţilor UPSC în cadrul sistemului de evidenţă a personalului.

II. SCOPUL

3. Scopul prelucrării informaţiilor ce conţin date cu caracter personal în sistemul de evidenţă a personalului constă în asigurarea înregistrării informaţiilor referitoare la angajaţi conform legislaţiei în vigoare.
4. În cadrul sistemului de evidenţă a personalului sunt prelucrate următoarele categorii de date cu caracter personal:
   - numele, prenumele, patronimicul, sexul şi cetăţenia;
   - numărul personal de identificare de stat (IDNP);
   - data naşterii, domiciliul, telefon, e-mail;
   - codul personal de asigurări sociale (CPAS), CPAM;
   - datele privind locul de muncă şi funcţia ocupată;
   - mărimea salariului brut şi alte premii, sporuri, stimulări, suplimente;
   - datele privind situaţia familială;
   - numele, prenumele (după caz, patronimicul) persoanelor care se află la întreţinerea persoanei respective;
   - datele din certificatele de concediu medical acordate;
   - date privind asigurarea medicală şi socială;
   - formarea profesională, studii, diplome;
   - date privind evidenţa militară;
   - vechimea în muncă, vechimea ştiinţifico-pedagogică;
   - date privind cursurile de formare continuă realizate;
   - date privind stimularea, sancţiuni disciplinare;
   - imaginea foto;
   - certificate privind starea sănătăţii;
   - semnătura;
   - alte date în conformitate cu prevederile legale.
5. Prelucrarea datelor cu caracter personal menţionate va fi efectuată pentru realizarea următoarelor scopuri:
   a) prelucrarea informaţiei privind modificările survenite la prelucrarea datelor cu caracter personal ce vizează angajaţii privitor la modificarea gradului de calificare (titlu ştiinţifico - didactic: doctor, conferenţiar universitar, profesor universitar), avansarea în treptele de salarizare, evaluarea performanţelor profesionale ale subdiviziunilor cu acordarea sporului pentru performanţă în activitate, vechimea în muncă didactico-ştiinţifică, formarea continuă;
   b) prelucrarea certificatelor de concedii medicale ale angajaţilor în vederea stabilirii

indemnizaţiilor corespunzătoare, concediului de îngrijire a copilului;
c) prelucrarea ordinelor rectorului referitoare la personal;
d) prelucrarea datelor cu privire la asigurarea obligatorie de asistenţă medicală la angajarea personalului şi la concediere;
e) eliberarea certificatelor de confirmare a activităţii, la cererea angajaţilor;
f) completarea şi stocarea dosarelor personale ale angajaţilor care includ date cu privire la persoană pe parcursul activităţii acesteia în cadrul UPSC.

6. Dosarele angajaţilor ce fac obiectul reglementării prezentului Regulament vor fi stocate de către UPSC astfel încât să permită identificarea persoanelor vizate strict pe durata activităţii acestora, iar la expirarea termenului respectiv de păstrare, primind statut de document de arhivă.
7. Orice utilizare a datelor cu caracter personal, introduse în sistemul de evidenţă a personalului în alte scopuri decât cele menţionate mai sus este interzisă.

III. LOCAŢIA ŞI DESCRIEREA SISTEMULUI DE EVIDENŢĂ A PERSONALULUI

8. Datele cu caracter personal conţinute în sistemul de evidenţă a personalului în cadrul UPSC se prelucrează/stochează/protejează:
   - pe suport de hârtie;
   - în format electronic.
9. Prelucrarea informaţiilor în sistemul de evidenţă a personalului pe suport de hârtie este structurată după criteriul „mape-dosare", fiind păstrate în dulapuri, care sunt amplasate fizic în biroul 27, blocul de studii nr. 2, din sediul UPSC.

IV. DURATA DE STOCARE

10. Prelucrarea datelor cu caracter personal în sistemul de evidenţă a personalului se efectuează pe perioada activităţii angajaţilor în cadrul UPSC (din momentul semnării contractului individual de muncă până la încetarea raporturilor de muncă) şi doar cu consimţământul expres al subiecţilor datelor cu caracter personal.
11. La expirarea termenelor menţionate în punctul 10, datele din sistemul de evidenţă a personalului sunt păstrate în formă arhivată, pe perioada stabilită de UPSC. Nomenclatorul dosarelor din cadrul Departamentului Resurse Umane şi Cancelarie, ulterior fiind supuse distrugerii sau ştergerii, în funcţie de suportul utilizat.

V. DREPTURILE ANGAJAŢILOR ŞI PERSOANELOR VIZATE

12. UPSC, în calitate de operator de date cu caracter personal, garantează respectarea drepturilor privind protecţia datelor cu caracter personal ce le revin angajaţilor, precum şi, după caz, altor persoane vizate.
13. Consimţământul pentru prelucrarea datelor cu caracter personal se exprimă prin semnarea acordului corespunzător.
14. În conformitate cu principiile de protecţie a datelor cu caracter personal, persoanele vizate 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.
15. Toate persoanele implicate în activitatea de administrare şi/sau prelucrare a informaţiilor din sistemul de evidenţă a personalului vor respecta procedura de acces la datele cu caracter personal.
16. Acordarea dreptului de acces a angajaţilor la informaţiile ce-i vizează se efectuează doar prin solicitarea expresă, în formă scrisă, cu acordul nemijlocit al conducerii UPSC. 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.

17. 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.

VI. MĂSURILE DE PROTECŢIE A DATELOR CU CARACTER PERSONAL PRELUCRATE ÎN SISTEMUL DE EVIDENŢĂ A PERSONALULUI

18. 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 sistemul de evidenţă a personalului, aceştia se păstrează în safeuri care se încuie;
    b) la terminarea sesiunilor de lucru, computerele şi imprimantele se deconectează de la reţeaua electrică;
    c) operatorul 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 sistemul de evidenţă a personalului este blocat împotriva vizualizării de către persoane neautorizate;
    e) mijloacele de prelucrare a informaţiilor preluate din sistemul de evidenţă a personalului sau soft-urile destinate prelucrării acestora sunt scoase din perimetrul de securitate doar în baza permisiunii scrise a operatorului.
19. Măsurile de protecţie a datelor cu caracter personal, prelucrate în sistemul de evidenţă a personalului, se înfăptuiesc ţinând seama de necesitatea asigurării confidenţialităţii şi integrităţii acestora, prin protecţie în formă manuală, electronică şi externă.
20. Cerinţe speciale faţă de marcare: toate informaţiile ieşite din sistemul de evidenţă a personalului, care conţin date cu caracter personal, sunt supuse marcării, cu indicarea prescripţiilor pentru prelucrarea ulterioară şi răspândirea acestora, inclusiv cu indicarea numărului de identificare unic al operatorului de date cu caracter personal.
21. Accesul în biroul unde este amplasat sistemul de evidenţă a personalului este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară şi doar în timpul orelor de program. Accesul în birou este posibil doar cu autorizarea de acces şi cheia de la lacătul mecanic.
22. Biroul nu este lăsat niciodată fără supraveghere la ieşirea în exterior, uşa biroului se încuie cu lacătul.
23. Înainte de acordarea accesului fizic la sistemul de evidenţă a personalului, se verifică competenţele de acces.
24. Perimetrul de securitate se consideră perimetrul biroului în care se păstrează dosarele personale ale angajaţilor şi sistemul de evidenţă a personalului, fiind integru din punct de vedere fizic.
25. Computerele sunt amplasate în locuri cu acces limitat pentru persoane străine.
26. Uşile şi ferestrele sunt încuiate în cazul în care în încăpere lipsesc angajaţii autorizaţi de administrarea sistemului.
27. Amplasarea sistemului de evidenţă a personalului răspunde necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.
28. Securitatea electroenergetică este asigurată prin securitatea echipamentului electric utilizat pentru menţinerea funcţionalităţii sistemului de evidenţă a personalului, a cablurilor electrice, inclusiv protecţia acestora contra deteriorărilor şi conectărilor nesancţionate. În cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, este asigurată posibilitatea deconectării electricităţii la sistemele de evidenţă a personalului, inclusiv posibilitatea deconectării oricărui component TI.
29. Securitatea cablurilor de reţea: cablurile de reţea, prin care se efectuează operaţiunile de transmitere a datelor preluate din sistemul de evidenţă a personalului, sunt protejate contra conectărilor nesancţionate sau deteriorărilor. Pentru a exclude bruiajul, cablurile de tensiune sunt

separate de cele comunicaţionale.

30. Securitatea anti incendiară a sistemului de evidenţă a personalului: biroul unde sunt amplasate dosarele personale ale angajaţilor şi sistemul de evidenţă a personalului este dotat cu echipament anti incendiar şi corespunde cerinţelor şi normelor anti incendiare în vigoare.
31. 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 a personalului. La expirarea termenului de păstrare, informaţiile, care conţin date cu caracter personal şi care se conţin pe purtătorii de informaţii, se distrug.

VII. IDENTIFICAREA ŞI AUTENTIFICAREA UTILIZATORULUI SISTEMULUI DE EVIDENDĂ A PERSONALULUI

32. Este efectuată identificarea şi autentificarea utilizatorilor informaţiilor preluate din sistemele de evidenţă contabilă şi a proceselor executate în numele acestor utilizatori.
33. 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.
34. 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.
35. Se efectuează modificarea parolelor de fiecare dată când sunt depistaţi indicii unei eventuale compromiteri a sistemului sau parolei.
36. 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 trei tentative greşite de autentificare, accesul este blocat, în mod automatizat.
37. Se asigură, pentru o perioadă de un an, păstrarea istoriilor anterioare ale parolelor în formă de hash a utilizatorilor şi prevenirea folosirii repetate a acestora.
38. 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.
39. Se efectuează, prin mijloace automatizate de suport, administrarea conturilor de acces a utilizatorilor care prelucrează datele cu caracter personal în sistemul de evidenţă a personalului, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea şi ştergerea acestora. Acţiunea conturilor de acces a utilizatorilor temporari, care prelucrează date cu caracter personal înregistrate în sistemul de evidenţă contabilă, 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 o lună, conturile de acces ale utilizatorilor neactivi, care prelucrează informaţiile din sistemul de evidenţă a personalului. Se folosesc mijloace automatizate de înregistrare şi informare despre crearea, modificarea, dezactivarea şi încetarea acţiunii conturilor de acces.
40. 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 utilizatorilor la sistemul de evidenţă a personalului.
41. Folosirea tehnologiilor fără fir, echipamentelor portative şi mobile se autorizează de persoanele responsabile.

42. Se impun limite în privința persoanelor care au dreptul:
    a) să vizualizeze informațiile stocate în sistemul de evidență a personalului;
    b) să copieze, să descarce, să șteargă sau să modifice orice informație stocată.
43. Toți angajații cu drepturi de acces beneficiază de o instruire inițială în domeniul protecției datelor cu caracter personal.
44. 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.
45. Orice încălcare a securității în ceea ce privește sistemul de evidență a personalului este supusă documentării, iar persoana responsabilă de realizarea politicii de securitate este informată în legătură cu acest lucru cât de urgent posibil.
46. Înainte de acordarea accesului în sistem, utilizatorii sunt informați despre faptul că folosirea sistemului de evidență a personalului este controlată și că folosirea neautorizată a acestora este sancționată în conformitate cu legislația civilă, contravențională și penală.

VIII. AUDITUL SECURITĂȚII ÎN SISTEMUL DE EVIDENȚĂ A PERSONALULUI

47. Se organizează generarea înregistrărilor de audit a securității în sistemul de evidență a personalului pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.
48. Se efectuează înregistrarea tentativelor de intrare/ieșire a utilizatorului în sistem, conform următorilor parametri:
    a) a)data și timpul tentativei intrării/ieșirii;
    b) ID-ul utilizatorului;
    c) rezultatul tentativei de intrare/ieșire - pozitivă sau negativă.
49. Se efectuează înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative și proceselor, destinate prelucrării informațiilor din sistemele de evidență a personalului, înregistrarea modificărilor drepturilor de acces ale utilizatorilor și statutul obiectelor de acces conform următorilor parametri:
    a) data și timpul tentativei de pornire;
    b) denumirea/identificatorul programului aplicativ sau al procesului;
    c) ID-ul utilizatorului;
    d) rezultatul tentativei de pornire - pozitivă sau negativă.
50. Se efectuează înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării informațiilor din sistemul de evidență a personalului, conform următorilor parametri:
    a) data și timpul tentativei de obținere a accesului (executare a operațiunii);
    b) denumirea (identificatorul) aplicației sau a procesului;
    c) ID-ul utilizatorului;
    d) specificațiile resursei protejate (identificator, nume logic, nume fișier, număr etc.);
    e) tipul operațiunii solicitate (citire, înregistrare, ștergere etc.);
    f) rezultatul tentativei de obținere a accesului (executare a operațiunii) - pozitivă sau negativă.
51. Se efectuează înregistrarea modificărilor drepturilor de acces (competențelor) utilizatorului și statutului obiectelor de acces, conform următorilor parametri:
    a) data și timpul modificării competențelor;
    b) ID-ul administratorului care a efectuat modificările;
    c) ID-ul utilizatorului și competențele acestuia sau specificarea obiectelor de acces și statutul nou al acestora.
52. Se efectuează înregistrarea ieșirii din sistemul de evidență a personalului, înregistrarea modificărilor drepturilor de acces ale subiecților și statutul obiectelor de acces, conform următorilor parametri:
    a) data și timpul eliberării;

b) denumirea informației și căile de acces la aceasta;
c) specificarea echipamentului (dispozitivului) care a eliberat informația (numele logic);
d) ID-ul utilizatorului care a solicitat informația;
e) volumul documentului eliberat (numărul paginilor, filelor, copiilor) și rezultatul eliberării - pozitiv sau negativ.

53. Cazurile de deranjament al auditului securității în sistemul de evidență a personalului sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, sunt aduse la cunoștința persoanei responsabile de politica de securitate a datelor cu caracter personal, care întreprinde măsuri în vederea restabilirii capacității de lucru a sistemului de audit.
54. Rezultatele auditului securității în sistemul de evidență a personalului (operațiunile de prelucrare a informațiilor și mijloacele de efectuare a auditului), se protejează contra accesului neautorizat prin aplicarea măsurilor de securitate adecvate și asigurarea confidențialității și integrității acestora.
55. Durata minimă a stocării rezultatelor auditului securității în sistemul de evidență a personalului constituie 2 (doi) ani, în scopul asigurării posibilității de folosire a acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigații sau procese judiciare. În cazul în care investigările sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

IX. ASIGURAREA INTEGRITĂȚII INFORMAȚIILOR DIN SISTEMUL DE EVIDENȚĂ A PERSONALULUI

56. Se asigură identificarea, protocolarea și înlăturarea deficiențelor de soft-uri destinate prelucrării informațiilor din sistemul de evidență a personalului, 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.
57. Se utilizează tehnologii și mijloace de constatare a intrărilor ilegale, ce permit monitorizarea evenimentelor și constatarea atacurilor, inclusiv asigură identificarea tentativelor folosirii neautorizate a informațiilor din sistemul de evidență a personalului.
58. Se asigură testarea funcționării corecte a componentelor de securitate a sistemului de evidență a personalului (automat - la pornirea sistemului, și, după caz, la solicitarea persoanei responsabile de politica de securitate a prelucrării datelor cu caracter personal).
59. Copiile de siguranță: reieșind din volumul prelucrărilor efectuate, individual, se stabilește de către operator intervalul de timp în care se execută copiile de siguranță a informațiilor din sistemul de evidență a personalului și soft-urilor folosite pentru prelucrările automatizate a acestora. 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.

X. GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMULUI DE EVIDENȚĂ A PERSONALULUI

60. Persoanele care asigură exploatarea sistemului de evidență a personalului trec, minimum o dată în an, instruirea cu privire la responsabilitățile și obligațiile în cazul executării acțiunilor de gestionare și reacționare la incidentele de securitate.
61. Prelucrarea incidentelor de securitate include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor și restabilirea securității. Se monitorizează și documentează, în mod permanent, incidentele de securitate în sistemul de evidență a personalului.
62. Persoanele care se fac vinovate de încălcarea normelor privind obținerea, păstrarea, prelucrarea și protecția informațiilor din sistemul de evidență a personalului poartă răspundere civilă, contravențională și penală.

XI. DISPOZIȚII FINALE

63. Prezentul Regulament poate fi revizuit periodic, în funcție de modificările și completările actelor normative aplicabile, precum și de nivelul dezvoltării tehnologiilor informaționale.
64. Regulamentul este adus la cunoștința angajaților implicați în prelucrarea datelor cu caracter personal contra semnătură și se plasează pagina web a UPSC pentru informarea tuturor angajaților și persoanelor interesate.
65. Prezentul Regulament intră în vigoare după aprobarea de către Senat, iar modificările și completările necesare se vor efectua în modul stabilit pentru aprobarea lui.