

Aprobat



REGULAMENTUL PRIVIND PRELUCRAREA INFORMAȚIILOR CE CONȚIN DATE CU CARACTER PERSONAL ÎN SISTEMUL DE EVIDENȚĂ A RESURSELOR UMANE

I. DISPOZIȚII GENERALE

1.1. Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență a resurselor umane (în continuare Regulament) este elaborat în vederea implementării în cadrul Universității de Stat "Bogdan Petriceicu Hasdeu" din Cahul - a prevederilor Legii nr.133 din 8 iulie 2011 privind protecția datelor cu caracter personal, cu modificările ulterioare, a Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr.1123 din 14 decembrie 2010, precum și întru respectarea prevederilor art. 91 - 94 ale Codului muncii al Republicii Moldova.

1.2. Prezentul Regulament reglementează condițiile generale și cerințele față de prelucrarea datelor cu caracter personal ale angajaților Universității de Stat "Bogdan Petriceicu Hasdeu" din Cahul, în cadrul sistemului de evidență a resurselor umane.

II. SCOPUL

2.1. Scopul prelucrării informațiilor ce conțin date cu caracter personal în sistemul de evidență a resurselor umane constă în asigurarea înregistrării informațiilor angajaților referitoare la datele din buletinul de identitate, numărul de identificare sau la unul ori mai multe elemente specifice identității sale fizice, fiziologice, psihice, culturale sau sociale; date care dezvăluie originea rasială, sau etnică a persoanei, apartenența socială, datele privind starea de sănătate, precum și cele referitoare la condamnările penale, măsuri procesuale de constrângere sau sancțiunile contravenționale..

2.2. În cadrul sistemului de evidență a resurselor umane sunt prelucrate următoarele categorii de date cu caracter personal:

- numele, prenumele și patronimicul;
- numărul personal de identificare de stat (IDNP);
- data nașterii și domiciliul;
- codul personal de asigurări sociale (CPAS);
- datele privind locul de muncă și funcția ocupată;
- mărimea salariului brut și alte premii, sporuri, stimulări, suplimente;
- datele privind situația familială (la cererea solicitantului);
- numele, prenumele (după caz, patronimicul) persoanelor care se află la întreținerea persoanei respective (membrii familiei, alte rude și persoane, după caz);
- datele din certificatele de concediu medical acordate, necesare pentru calcularea indemnizației corespunzătoare;
- după caz, alte date necesare îndeplinirii scopului menționat, conform legislației în vigoare.

2.3. Prelucrarea datelor cu caracter personal menționate va fi efectuată pentru realizarea următoarelor scopuri:

- a) Prelucrarea informației privind modificările survenite la prelucrarea datelor cu caracter personal ce vizează angajații și care au impact asupra calculării plăților salariale, de exemplu: modificarea gradului de calificare a unor categorii de salariați, avansarea în treptele de salarizare, evaluarea performanțelor profesionale ale cadrului profesoral, vechimea în muncă;
- b) Prelucrarea certificatelor de concedii medicale ale angajaților în vederea stabilirii termenului absenței motivate de la serviciu;
- c) Perfectarea ordinelor referitoare la personal;
- d) Eliberarea certificatelor, adeverințelor, la cererea angajaților;
- e) Completarea și stocarea fișelor personale de evidență a salariaților.

2.4. Datele cu caracter personal ce fac obiectul reglementării prezentului Regulament vor fi stocate de către serviciul de evidență a resurselor umane, astfel încât să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sînt prelucrate, iar la expirarea termenului respectiv, înregistrările se vor distruge/șterge, în funcție de suportul pe care au fost efectuate. În cazul obligațiilor expres prevăzute de lege acestea pot rămîne la păstrare primind statut de document de arhivă.

2.5. Orice utilizare a datelor cu caracter personal, introduse în sistemul de evidență a resurselor umane în alte scopuri decît cele menționate mai sus este interzisă.

III. LOCAȚIA ȘI DESCRIEREA SISTEMULUI DE EVIDENȚĂ A RESURSELOR UMANE

3.1. Datele cu caracter personal conținute în sistemul de evidență a resurselor umane în cadrul Universității de Stat “Bogdan Petriceicu Hasdeu” din Cahul, se prelucrează/stochează:

- 1. pe suport de hîrtie;
- 2. în format electronic: care este instalat la computerul central – ”Resurse umane” din biroul 106 și cu drept de acces la al doilea computer în biroul 106 din sediul Universității de Stat “Bogdan Petriceicu Hasdeu” din Cahul.

3.2. Prelucrarea informațiilor în sistemul de evidență a resurselor umane pe suport de hîrtie este structurată după criteriul “mape-dosare”, fiind păstrate în dulapuri, care sînt amplasate fizic în biroul 106 din sediul Universității de Stat “Bogdan Petriceicu Hasdeu” din Cahul.

IV. DURATA DE STOCARE

4.1. Prelucrarea datelor cu caracter personal în sistemul de evidență a resurselor umane se efectuează pe perioada valabilității contractelor individuale de muncă, pe perioada activității angajaților Universității de Stat “Bogdan Petriceicu Hasdeu” din Cahul (din momentul semnării contractului pînă la finalizarea efectuării acțiunilor prevăzute de actele legislative în cazul încetării raporturilor de muncă).

4.2. La expirarea termenelor menționate în punctul 4.1., datele din sistemul de evidență a resurselor umane sînt păstrate în formă arhivată, pe perioada stabilită de, Nomenclatorul dosarelor din cadrul Universității de Stat “Bogdan Petriceicu Hasdeu” din Cahul, aprobat prin ordinul nr. 034 din 29 decembrie 2008, ulterior fiind supuse distrugerii sau ștergerii, în funcție de suportul pe care au fost efectuate.

V. DREPTURILE ANGAJAȚILOR ȘI PERSOANELOR VIZATE

5.1. Universitatea de Stat “Bogdan Petriceicu Hasdeu” din Cahul, în calitate de operator de date cu caracter personal, garantează respectarea drepturilor privind protecția datelor cu caracter personal ce le revin angajaților, precum și, după caz, altor persoane vizate.

5.2. În conformitate cu principiile de protecție a datelor cu caracter personal, persoanele vizate 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.

5.3. Toate persoanele implicate în activitatea de administrare și/sau prelucrare a informațiilor din sistemul de evidență a resurselor umane vor respecta procedura de acces la datele cu caracter personal.

5.4. Acordarea dreptului de acces a angajaților la informațiile ce-i vizează se efectuează doar prin solicitarea expresă, în formă scrisă, cu acordul nemijlocit al conducerii Universității de Stat "Bogdan Petriceicu Hasdeu" din Cahul. 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.

5.5. 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.

VI. MĂSURILE DE PROTECȚIE A DATELOR CU CARACTER PERSONAL PRELUCRATE ÎN SISTEMUL DE EVIDENȚĂ A RESURSELOR UMANE

6.1. Măsurile generale de administrare a securității informaționale

6.1.1. În cazul neutilizării temporare a purtătorilor de informație pe suport de hârtie sau electronic care conțin date preluate din sistemul de evidență a resurselor umane, aceștia se păstrează în safeuri care se încuie.

6.1.2. La terminarea sesiunilor de lucru, computerele și imprimantele se deconectează de la rețeaua electrică.

6.1.3. Operatorul asigură securitatea punctelor de primire și expediere a corespondenței, precum și securitatea contra accesului neautorizat la aparatele de copiere.

6.1.4. Accesul fizic la mijloacele de reprezentare a informației preluate din sistemul de evidență a resurselor umane este blocat împotriva vizualizării de către persoane neautorizate.

6.1.5. Mijloacele de prelucrare a informațiilor preluate din sistemul de evidență a resurselor umane sau soft-urile destinate prelucrării acestora sînt scoase din perimetrul de securitate doar în baza permisiunii scrise a operatorului.

6.1.6. Scoaterea și introducerea mijloacelor de prelucrare a informațiilor din sistemul de evidență a resurselor umane din/în perimetrul de securitate se înregistrează în registru.

6.2. Măsurile de protecție a datelor cu caracter personal, prelucrate în sistemul de evidență a resurselor umane, se înfăptuiesc ținînd cont de necesitatea asigurării confidențialității și integrității acestora, prin protecție în formă manuală, electronică și externă.

- 6.3.** Cerințe speciale față de marcarea: toate informațiile ieșite din sistemul de evidență a resurselor umane, care conțin date cu caracter personal, sînt supuse marcării, cu indicarea prescripțiilor pentru prelucrarea ulterioară și răspîndirea acestora, inclusiv cu indicarea numărului de identificare unic al operatorului de date cu caracter personal.
- 6.4.** Accesul în biroul unde este amplasat sistemul de evidență a resurselor umane este restricționat, fiind permis doar persoanelor care au autorizația necesară și doar în timpul orelor de program. Accesul în birou este posibil doar cu autorizarea de acces și cheia de la lacătul mecanic.
- 6.5.** Biroul nu este lăsat niciodată fără supraveghere la ieșirea în exterior, ușa biroului se încuie cu lacătul.
- 6.6.** Înainte de acordarea accesului fizic la sistemul de evidență a resurselor umane, se verifică competențele de acces.
- 6.7.** 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.
- 6.8.** Perimetrul de securitate se consideră perimetrul biroului în care este amplasat sistemul de evidență a resurselor umane, fiind integru din punct de vedere fizic.
- 6.9.** Zilnic, se inspectează perimetrul de securitate al clădirii și al biroului, unde este amplasat sistemul de evidență a resurselor umane, din punct de vedere fizic.
- 6.10.** Computerele sînt amplasate în locuri cu acces limitat pentru persoane străine.
- 6.11.** Ușile și ferestrele sînt încuiate în cazul în care în încăpere lipsesc angajații autorizați de administrarea sistemului.
- 6.12.** Amplasarea sistemului de evidență a resurselor umane răspunde necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.
- 6.13.** Securitatea electroenergetică: este asigurată securitatea echipamentului electric utilizat pentru menținerea funcționalității sistemului de evidență a resurselor umane, a cablurilor electrice, inclusiv protecția acestora contra deteriorărilor și conectărilor nesancționate. În cazul apariției situațiilor excepționale, de avarie sau de forță majoră, este asigurată posibilitatea deconectării electricității la sistemele de evidență a resurselor umane, inclusiv posibilitatea deconectării oricărui component TI.
- 6.14.** Computerele, unde este amplasat fizic sistemul de evidență a resurselor umane, dispun de UPS-uri, care sînt folosite pentru încheierea corectă a sesiunii de lucru a sistemelor (componentelor) în cazul deconectării de la sursa de alimentare cu energie electrică.
- 6.15.** Securitatea cablurilor de rețea: cablurile de rețea, prin care se efectuează operațiunile de transmitere a datelor preluate din sistemul de evidență a resurselor umane, sînt protejate contra conectărilor nesancționate sau deteriorărilor. Pentru a exclude bruiajul, cablurile de tensiune sînt separate de cele comunicaționale.
- 6.16.** Securitatea antiincendiară a sistemului de evidență a resurselor umane: biroul unde este amplasat sistemul de evidență a resurselor umane este dotat cu echipament antiincendiar și corespunde cerințelor și normelor antiincendiară în vigoare.
- 6.17.** 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 a resurselor umane. La expirarea termenului de păstrare, informațiile, care conțin date cu caracter personal și care se conțin pe purtătorii de informații, se distrug.

VII. IDENTIFICAREA ȘI AUTENTIFICAREA UTILIZATORULUI SISTEMULUI DE EVIDENȚĂ A RESURSELOR UMANE

7.1. Este efectuată identificarea și autentificarea utilizatorilor informațiilor preluate din sistemele de evidență a resurselor umane și a proceselor executate în numele acestor utilizatori.

7.2. 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.

7.3. Pentru confirmarea ID-ului utilizatorului sînt utilizate parole. Utilizarea parolelor în procesul asigurării securității informaționale: pe lângă cerințele de păstrare a confidențialității parolelor, este interzisă înscrierea acestora pe suport de hîrtie, cu excepția cazului de asigurare a securității păstrării acestora (plasarea înscrisurilor în safeu). La momentul introducerii, parolele nu se reflectă în clar pe monitor.

7.4. Se efectuează modificarea parolelor de fiecare dată cînd sînt depistați indicii unei eventuale compromiteri a sistemului sau parolei.

7.5. Întru asigurarea posibilității de stabilire a responsabilității fiecărui utilizator, sînt 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 trei tentative greșite de autentificare, accesul este blocat, în mod automatizat.

7.6. Se asigură, pentru o perioadă de 1 /un/ an, păstrarea istoriilor anterioare ale parolelor în formă de hash a utilizatorilor și prevenirea folosirii repetate a acestora.

7.7. 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.

7.8. Se efectuează, prin mijloace automatizate de suport, administrarea conturilor de acces a utilizatorilor care prelucrează datele cu caracter personal în sistemul de evidență a resurselor umane, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea și ștergerea acestora. Acțiunea conturilor de acces a utilizatorilor temporari, care prelucrează date cu caracter personal înregistrate în sistemul de evidență a resurselor umane, 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 sistemul de evidență a resurselor umane. Se folosesc mijloace automatizate de înregistrare și informare despre crearea, modificarea, dezactivarea și încetarea acțiunii conturilor de acces.

7.9. 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 utilizatorilor la sistemul de evidență a resurselor umane.

7.10. Folosirea tehnologiilor fără fir, echipamentelor portative și mobile se autorizează de persoanele responsabile.

7.11. Se impun limite în privința persoanelor care au dreptul:

- a) să vizualizeze informațiile stocate în sistemul de evidență a resurselor umane;
- b) să copieze, să descarce, să șteargă sau să modifice orice informație stocată.

7.12. Toți angajații cu drepturi de acces beneficiază de o instruire inițială în domeniul protecției datelor cu caracter personal.

7.13. 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.

7.14. Orice încălcare a securității în ceea ce privește sistemul de evidență a resurselor umane este supusă documentării, iar persoana responsabilă de realizarea politicii de securitate este informată în legătură cu acest lucru cât de urgent posibil.

7.15. Înainte de acordarea accesului în sistem, utilizatorii sînt informați despre faptul că folosirea sistemului de evidență a resurselor umane este controlată și că folosirea neautorizată a acestora este sancționată în conformitate cu legislația civilă, contravențională și penală.

VIII. ASIGURAREA INTEGRITĂȚII INFORMAȚIILOR DIN SISTEMUL DE EVIDENȚĂ A RESURSELOR UMANE

8.1. Se asigură identificarea, protocolarea și înlăturarea deficiențelor de soft-uri destinate prelucrării informațiilor din sistemul de evidență a resurselor umane, 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 semnăturilor de virus.

8.2. 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 resurselor umane.

8.3. Se asigură testarea funcționării corecte a componentelor de securitate a sistemului de evidență a resurselor umane (automat – la pornirea sistemului, și după caz – la solicitarea persoanei responsabile de politica de securitate a prelucrării datelor cu caracter personal).

8.4. 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 resurselor umane 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.

IX. GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMULUI DE EVIDENȚĂ A RESURSELOR UMANE

9.1. Persoanele care asigură exploatarea sistemului de evidență a resurselor umane 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.

9.2. 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 resurselor umane.

9.3. Persoanele care se fac vinovate de încălcarea normelor privind obținerea, păstrarea, prelucrarea și protecția informațiilor din sistemul de evidență a resurselor umane poartă răspundere civilă, contravențională și penală.

X. DISPOZIȚII FINALE

10.1. Prezentul Regulament este revizuit și ulterior aprobat de către conducerea Universității de Stat "Bogdan Petriceicu Hasdeu" din Cahul, periodic, însă cel puțin o dată în an, precum și la necesitate.

10.2. Prezentul Regulament se completează cu prevederile legislației în vigoare.

10.3. Regulamentul este adus la cunoștința angajaților contra semnăturii.

10.4. Modificarea și completarea prezentului Regulament se face în modul stabilit pentru aprobarea lui.