

APROBAT
Decizia consiliului satesc
nr.3.03 din 22.06.2023

REGULAMENT

cu privire la asigurarea securității datelor cu caracter personal în sistemul de evidență a resurselor umane în cadrul Primăriei s.Dominteni

I. DISPOZIȚII GENERALE

1. Regulamentul cu privire la asigurarea securității datelor cu caracter personal în Sistemul de evidență a resurselor umane, în cadrul **PRIMĂRIEI SATULUI DOMINTENI** stabilește responsabilitățile persoanelor din subdiviziunea Resurse Umane a Primăriei ce au acces la securitatea datelor cu caracter personal în cadrul acestui sistem de evidență.
2. Persoanele din subdiviziunile Resurse Umane ale **PRIMĂRIEI SATULUI DOMINTENI** ce au acces la datele cu caracter personal nu vor depăși limitele stabilite de Politica de securitate a **PRIMĂRIEI SATULUI DOMINTENI**, precum și normele legale stabilite prin prevederile Legii nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal, Hotărârii Guvernului nr.1123 din 14 decembrie 2010 „Privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal”, precum și a prevederilor prezentului Regulament.

II. SCOPUL PRELUCRĂRII INFORMAȚIILOR CE CONȚIN DATE CU CARACTER PERSONAL

3. Scopul prelucrării informațiilor ce conțin date cu caracter personal în sistemul de evidență a Resurselor Umane, constă în asigurarea înregistrării informațiilor referitor la recrutarea, angajarea, executarea clauzelor contractelor individuale de muncă, pensionarea salariaților, precum și a prezentării rapoartelor trimestriale și anuale către instituțiile statului, conform legislației în vigoare.
4. În cadrul sistemul de evidență a resurselor umane, sunt prelucrate următoarele categorii de date cu caracter personal:

- numele, prenumele, patronimicul;
- sexul;
- data și locul nașterii;
- semnătura;
- datele din actele de stare civilă;
- codul personal de asigurării sociale (CPAS);
- numărul de telefon mobil;
- profesie, funcție
- formare profesională - diplome- studii
- imagine
- mărimea salariului de funcție, sporuri, suplimente, stimulări din partea angajatorului, cazier juridic.
- datele membrilor de familie
- cetățenia
- sancțiuni disciplinare
- telefon/fax

- adresa (domiciliului/reședinței)
- loc de muncă
- IDNP (numărul personal de identificare de stat)
- situație militară

5. 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 executării contractului individual de muncă;
- b) stabilirea sistemului de salarizare a personalului în conformitate cu legislația în vigoare a Republicii Moldova;
- c) prelucrarea certificatelor de concedii medicale ale angajaților în vederea stabilirii indemnizațiilor corespunzătoare;
- d) elaborarea, înregistrarea și prelucrarea ordinelor rectorului referitor la personal;
- e) prezentarea la CNAM a evidenței nominale a noilor angajați și a celor concediați, format hârtie și format electronic;
- f) înregistrarea și prelucrarea dosarelor pentru concursul de suplinire a posturilor vacante;
- g) întocmirea declarației persoanei asigurate REV 1 pentru fiecare angajat și transmiterea acestora Casei Teritoriale de Asigurări Sociale, Centru pe suport de hârtie;
- h) asistarea procesului (prin furnizarea informației necesare) pentru completarea periodică (lunară) a raportului și dării de seamă privind venitul achitat și impozitul pe venit reținut din acesta;
- i) completarea lunară, trimestrială și anuală a rapoartelor statistice referitoare la personalul primăriei;
- j) prelucrarea cererilor și a documentelor necesare executării contractelor individuale de muncă;
- k) eliberarea certificatelor care atestă calitatea de salariat al primăriei la cererea angajaților;
- l) ținerea dosarelor personale ale salariaților;
- m) înregistrarea datelor în cartelele de muncă;
- n) alte scopuri, necesare realizării activităților ce țin de gestionarea resurselor umane.

6. Datele cu caracter personal ce fac obiectul reglementării prezentului Regulament vor fi stocate de către responsabilii din cadrul Primăriei, astfel încât să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sunt 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 rămâne la păstrare primind statut de document de arhivă.

7. Orice utilizare a datelor cu caracter personal, introduse în sistemul de evidență a Resurselor Umane în alte scopuri decât cele menționate mai sus este interzisă.

8. Prelucrarea datelor cu caracter personal în sistemul de evidență a resurselor umane se efectuează în conformitate cu prevederilor art. 5 alin. 5 lit. a), b) și e) al Legii privind protecția datelor cu caracter personal.

III. LOCAȚIA ȘI DESCRIEREA SISTEMULUI DE EVIDENȚĂ A RESURSELOR UMANE

9. Datele cu caracter personal conținute în sistemul de evidență a Resurselor Umane în cadrul entității se prelucrează și se stochează:

- 1) pe suport de hârtie;
- 2) în format electronic:

- a) Software – Sistemul de evidență a resurselor umane BIT SECRETAR
- b) Hardware – Nr. de inventariere – 00294.

10. Prelucrarea informațiilor în sistemul de evidență resurse umane pe suport de hârtie este structurată după criteriul “mape-dosare”, fiind păstrate în dulapuri, care sânt amplasate fizic în biroul specialistului resurse umane a **PRIMĂRIEI SATULUI DOMINTENI, rnl. Drochia, s. DOMINTENI, MD-5215.**

IV. DURATA DE STOCARE

11. Prelucrarea datelor cu caracter personal în sistemul de evidență a Resurselor Umane se efectuează pe perioada activității angajaților primăriei, la expirarea termenilor menționate datele din sistemul de evidență a angajaților primăriei sunt păstrate în formă arhivată pe perioada stabilită în Nomenclatorul dosarelor în cadrul primăriei. Actele normative ce reglementează regimul juridic și termenele de păstrare. Dosarele de concurs ale candidaților la funcțiile publice vacante din cadrul **PRIMĂRIEI SATULUI DOMINTENI** se păstrează la secretarul primăriei timp de un an, conform Hotărârii de Guvern nr. 201 din 11.03.2009 privind punerea în aplicare a Legii nr. 158-XVI din 04.07.2018 cu privire la funcția publică și statutul funcționarului public, după care sunt nimicite prin proces verbal. Prelucrarea datelor cu caracter personal în sistemul de evidență a datelor privind gestionarea resurselor umane se efectuează pe perioada activității angajaților.

Datele cu caracter personal a potențialilor angajați se preia din CV-ul transmis de către aceștia la adresa de e-mail. După primirea CV-ului prin intermediul poștei electronice, acesta se tipărește pe suport de hârtie, iar de pe adresa electronica se șterge. În cazul în care rezultatul în privința angajării persoanei a cărei date cu caracter personal au fost prelucrate, este negativ, CV-ul se distruge

12. La expirarea termenilor menționați datele din sistemul de evidență a datelor privind gestionarea resurselor umane ale **PRIMĂRIEI SATULUI DOMINTENI** sunt păstrate în formă arhivată, pe perioada stabilită de Nomenclatorul dosarelor din cadrul **PRIMĂRIEI SATULUI DOMINTENI**.

IV. DREPTURILE ANGAJAȚILOR SI PERSOANELOR VIZATE

13. Primăria 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.

14. 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.

15. 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.

16. Acordarea dreptului de acces al angajaților la informațiile ce-i vizează se efectuează doar prin solicitarea expresă, în formă scrisă, cu acordul nemijlocit al primarului. 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.

17. 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.

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

18. Măsurile generale de administrare a securității informaționale:

- 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.
- la terminarea sesiunilor de lucru, computerele și imprimantele se deconectează de la rețeaua electrică.
- operatorul asigură securitatea punctelor de primire și expediere a corespondenței, precum și securitatea contra accesului neautorizat la aparatele de copiere.
- accesul fizic la mijloacele de reprezentare a informației preluate din sistemul de evidență a Resurselor Umane este blocat împotriva vizualizării de către persoane neautorizate.
- mijloacele de prelucrare a informațiilor preluate din sistemul de evidență a Resurselor Umane sau soft-urile destinate prelucrării acestora sunt scoase din perimetrul de securitate doar în baza permisiunii scrise a operatorului.
- scoaterea și introducerea mijloacelor de prelucrare a informațiilor din sistemul de evidență a Resurselor Umane din/în perimetrul de securitate se înscriu în registru.

19. Măsurile de protecție a datelor cu caracter personal, prelucrate în sistemul de evidență a Resurselor Umane, se îndeplinesc ținând cont de necesitatea asigurării confidențialității și integrității acestora, prin protecție în formă manuală și electronică.

20. Cerințe speciale față de marcare: toate informațiile ieșite din sistemul de evidență a Resurselor Umane, care conțin date cu caracter personal, sunt supuse marcării, cu indicarea prescripțiilor pentru prelucrarea ulterioară și răspândirea acestora,

***Model** Atenție! Documentul conține date cu caracter personal. Prelucrarea ulterioară a acestor date poate fi efectuată numai în condițiile prevăzute de Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal.*

21. Biroul nu este lăsat niciodată fără supraveghere, la ieșirea în exterior ușa biroului se încuie cu lacătul.

22. Înainte de acordarea accesului fizic la sistemul de evidență a Resurselor Umane se verifică competențele de acces.

23. 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.

24. Perimetrul de securitate se consideră perimetrul biroului în care este amplasat sistemul de evidență a Resurselor Umane, fiind integru din punct de vedere fizic.

25. Computerele sunt amplasate în locuri cu acces limitat pentru persoane străine.

26. Ușile și ferestrele sunt încuiate în cazul în care în încăperea lipsesc angajații autorizați de administrarea sistemului.

27. Amplasarea sistemului de evidență a Resurselor Umane răspunde necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor și altor posibile riscuri.

28. 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 sistemul de evidență a Resurselor Umane, inclusiv posibilitatea deconectării oricărui component TI.

29. Computerele, unde este amplasat fizic sistemul de evidență a Resurselor 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.

30. Securitatea cablurilor de rețea: cablurile de rețea, prin care se efectuează operațiunile de transmitere a datelor preluate din sistemul de evidență a Resurselor Umane, sunt protejate contra conectărilor nesancționate sau deteriorărilor. Pentru a exclude bruiajul, cablurile de tensiune sunt separate de cele comunicaționale.

31. Securitatea anti incendiară a sistemul de evidență a Resurselor Umane: biroul unde este amplasat sistemul de evidență a Resurselor Umane este dotat cu echipament anti incendiar și corespunde cerințelor și normelor anti incendiarie în vigoare.

32. 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 sistemul 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.

VI. AUDITUL SECURITĂȚII ÎN SISTEMULUI DE EVIDENȚĂ A RESURSELOR UMANE

33. Se organizează generarea înregistrărilor de audit a securității în sistemul de evidență a resurselor umane pentru evenimentele indicate în lista corespunzătoare, supuse auditului.

34. Înregistrările de audit a securității Sistemului de Evidență al Resurselor Umane în care sînt prelucrate date cu caracter personal, trebuie să conțină:

- numele și prenumele utilizatorului;
- numele fișei accesate (pagina și inscripția din registru);
- numărul înregistrărilor efectuate;
- tipul de acces;
- data accesului (an, lună, zi);
- timpul (ora, minuta) și durata accesului.

35. Rezultatele auditului securității în Sistemul de Evidență al Resurselor Umane (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.

36. Durata minimă a stocării rezultatelor auditului securității în Sistemul de Evidență al Resurselor Umane 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.

neautorizat prin aplicarea măsurilor de securitate adecvate și asigurarea confidențialității și integrității acestora.

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

38. Persoanele care asigură exploatarea sistemul de evidență a Resurselor Umane trec, minim o dată în an, instruirea cu privire la responsabilitățile și obligațiile în cazul executării acțiunilor de gestionare și reacționare la incidentele de securitate.

39. 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.

40. 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.

41. „În cazul producerii incidentelor de securitate, persoanele responsabile vor întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia și va înlătura cauzele incidentului de securitate cu informarea în termen de 72 ore din momentul producerii incidentului de securitate a Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova. Totodată, în cadrul controalelor efectuate de Centrul Național pentru Protecția Datelor cu Caracter Personal, persoanele responsabile sînt obligate să ofere suportul necesar și să asigure accesul la informațiile necesare relevante obiectului controlului.”

VIII. DISPOZIȚII FINALE

42. Presentul Regulament este aprobat de către organul de conducere al **PRIMĂRIEI SATULUI DOMINTENI** și revizuit periodic, la necesitate, în cazul modificării legislației în vigoare.
43. Presentul Regulament se completează cu prevederile legislației în vigoare.
44. Modificarea și completarea prezentului Regulament se face în modul stabilit pentru aprobarea acestuia.

**LISTA ANGAJAȚILOR FAMILIARIZAȚI CU PREVEDERILE REGULAMENTULUI
cu privire la asigurarea securității datelor cu caracter personal în sistemul
de evidență a resurselor umane în cadrul PRIMĂRIEI SATULUI DOMINTENI**

Nr.	Numele, prenumele	Funcția	Am luat cunoștință (semnătura)	Data
1	Prisacari Nina	Secretarul Consiliului local		22.06.23
2				
3				
4				
5				
6				
7				