

REPUBLICA MOLDOVA

**RAIONUL ȘOLDĂNEȘTI  
CONSILIUL SĂTESC ROGOJENI**

s. Rogojeni,  
r-ul Șoldănești  
Tel. (272)-63-2-36,63-2-77  
e-mail:primaria.rogojeni@apl.gov.md



РЕСПУБЛИКА МОЛДОВА

**РАЙОН ШОЛДЭНЭШТЬ  
СЕЛЬСКИЙ СОВЕТ  
РОГОЖЕНЬ**

с. Рогожень  
Р-н Шолдэнешть  
Тел. (272)-63-2-36,63-2-77  
e-mail:primaria.rogojeni@apl.gov.md

**DECIZIE nr.1/13  
a Consiliului sătesc Rogojeni din 25 februarie 2025**

“Cu privire la prelucrarea datelor cu caracter personal în APL Rogojeni”

În scopul reglementării prelucrării datelor cu caracter personal necesare pentru realizarea/executarea sarcinilor care rezultă din exercitarea prerogativelor de autoritate publică, în temeiul Codului Administrativ al Republicii Moldova nr.116/2018, art.14, alin.(3) al Legii Republicii Moldova nr.436/2006 privind administrația publică locală, Legii nr.71/2007 cu privire la registre, Legii nr.133/2011 privind protecția datelor cu caracter personal, Instrucțiunilor privind ținerea lucrărilor de secretariat referitoare la petițiile persoanelor fizice și juridice, adresate organelor de stat, întreprinderilor, instituțiilor și organizațiilor Republicii Moldova, aprobate prin Hotărârea Guvernului nr.208 din 31.03.1995, cerințelor față de asigurarea securității datelor cu caracter personal, aprobate prin Hotărârea Guvernului nr.1123 din 14.12.2010, avizul comisiei de specialitate pentru activități sociale, culturale, sport, tineret, turism, culte, învățământ, sănătate publică și muncă, Consiliul sătesc Rogojeni

**DECIDE :**

1. Se aprobă următoarele acte normative interne în domeniul prelucrării datelor cu caracter personal:

- 1.1. Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență al corespondenței și petițiilor parvenite în adresa Primăriei satului Rogojeni.
- 1.2. Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență a resurselor umane în cadrul Primăriei satului Rogojeni.
- 1.3. Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență contabilă în cadrul Primăriei satului Rogojeni.
- 1.4. Politică privind protecția datelor cu caracter personal în cadrul Primăriei satului Rogojeni.
- 1.5. Politică de confidențialitate privind prelucrarea datelor personale ale angajaților și potențialilor angajați în cadrul Primăriei satului Rogojeni.
- 1.6. Politică ANTI-SPAM în cadrul Primăriei satului Rogojeni.
- 1.7. Politică privind resursele informatice în cadrul Primăriei satului Rogojeni.
- 1.8. Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență supraveghere video.

2. Se desemnează primarul satului în calitate de persoană responsabilă de protecția datelor cu caracter personal în cadrul Primăriei satului Rogojeni și de implementarea politicii de securitate a sistemului de informații și mijloace.

3. Prezenta decizie se publică în Registrul de stat al actelor locale, se aduce la cunoștința angajaților contrasemnătură și se plasează pentru informare publică pe pagina oficială a Primăriei Rogojeni în rețeaua internet: WEB: [www.rogojeni.sat.md](http://www.rogojeni.sat.md) .

4. Controlul executării prezentei decizii se atribuie primarului Ruslan Groza.

AU VOTAT: pentru - 9,    contra - 0    s-au abținut -0

Președintele ședinței

Prodan Constantin

Secretara consiliului

Ardeleanu Viorica

## NOTA INFORMATIVĂ

### la Proiectul de decizie nr. 1/13 din 25 februarie 2025 “ Cu privire la prelucrarea datelor cu caracter personal în APL Rogojeni”

#### 1. Denumirea autorului

Proiectul este elaborat de către secretara consiliului sătesc Rogojeni, autor al proiectului de act normativ este primarul satului Rogojeni.

**2 Condițiile ce au impus elaborarea proiectului de act normativ și finalitățile urmărite** sunt prevederile Legii nr.133 din 8 iulie 2011 privind protecția datelor cu caracter personal;

Scopul proiectului de decizie este reglementării prelucrării datelor cu caracter personal necesare pentru realizarea / executarea sarcinilor care rezultă din exercitarea prerogativelor de autoritate publică ;

3. Descrierea gradului de compatibilitate pentru proiectele care au scop armonizarea legislației naționale cu legislația UE - Nu necesită

**4. Principalele prevederi ale proiectului** • Se propune aprobarea actelor normative interne în domeniul prelucrării datelor cu caracter personal :

1.1. Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență al corespondenței și petițiilor parvenite în adresa Primăriei satului Rogojeni.

1.2. Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență a resurselor umane în cadrul Primăriei satului Rogojeni.

1.3. Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență contabilă în cadrul Primăriei satului Rogojeni.

1.4. Politică privind protecția datelor cu caracter personal în cadrul Primăriei satului Rogojeni.

1.5. Politică de confidențialitate privind prelucrarea datelor personale ale angajaților și potențialilor angajați în cadrul Primăriei satului Rogojeni.

1.6. Politică ANTI-SPAM în cadrul Primăriei satului Rogojeni.

1.7. Politică privind resursele informatice în cadrul Primăriei satului Rogojeni.

1.8. Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență supraveghere video.

**5. Fundamentarea economico-financiară** Implementarea prevederilor Regulamentelor nu solicită alocarea surselor financiare .

**6. Modul de incorporare a actului în cadrul normativ în vigoare :**

Codului Administrativ al Republicii Moldova nr.116/2018, art.14, alin.(3) al Legii Republicii Moldova nr.436/2006 privind administrația publică locală, Legii nr.71/2007 cu privire la register, Legii nr.133/2011 privind protecția datelor cu caracter personal , Instrucțiunilor privind ținerea lucrărilor de secretariat referitoare la petițiile persoanelor fizice și juridice, adresate organelor de stat, întreprinderilor, instituțiilor și organizațiilor Republicii Moldova, aprobate prin Hotărârea Guvernului nr.208 din 31.03.1995, cerințelor față de asigurarea securității datelor cu caracter personal, aprobate prin Hotărârea Guvernului nr.1123 din 14.12.2010.

**7. Avizarea și consultarea publică a proiectului** Anunțul despre inițierea proiectului de Decizie se publică pe site-ul oficial al Primăriei WEB : rogojeni.sat.md ;

**8. Constatările expertizei anticorupție** - Nu necesită

**9. Constatările expertizei de compatibilitate** - Nu necesită

Secretara consiliului

Ardeleanu Viorica

**REGULAMENTUL**  
**privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de**  
**evidență al corespondenței și petițiilor parvenite în adresa Primăriei satului Rogojeni**

**I. Dispoziții generale**

1. Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență a corespondenței și petițiilor parvenite în adresa Primăriei satului Rogojeni (Regulamentul) este elaborat în conformitate cu prevederile Codului administrativ al Republicii Moldova, aprobat prin Legea nr. 116 din 19 iulie 2018, Legii nr. 71-XVI din 22 martie 2007 cu privire la registre, Legii nr.133 din 8 iulie 2011 privind protecția datelor cu caracter personal, Instrucțiunilor privind ținerea lucrărilor de secretariat referitoare la petițiile persoanelor fizice și juridice, adresa organelor de stat, întreprinderilor, instituțiilor și organizațiilor Republicii Moldova, aprobate prin Hotărîrea Guvernului nr. 208 din 31 martie 1995, Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărîrea Guvernului nr. 1123 din 14 decembrie 2010.

2. Prezentul Regulament reglementează modalitatea Ținerii sistemului de evidență a corespondenței și petițiilor parvenite în adresa Primăria satului Rogojeni, precum și procedura de înregistrare, securizare, modificare și radiere a datelor din Registru.

3. Noțiunile utilizate în prezentul Regulament au semnificația prevăzută de Legea cu privire la registre, Codului administrativ al Republicii Moldova, aprobat prin Legea nr.116 din 19 iulie 2018, Legea privind protecția datelor cu caracter personal, Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal.

Astfel, în sensul prezentului Regulament se definesc următoarele noțiuni:

Petiție - orice cerere, sesizare sau propunere adresată unei autorități publice de către o persoană fizică sau juridică;

Cerere - orice cerere prin intermediul căreia se solicită individual sau efectuarea unei operațiuni administrative;

Sesizare - orice sesizare prin intermediul căreia se informează autoritatea publică cu privire la o problemă de interes personal sau public;

Propunere - orice propunere prin intermediul căreia se urmărește realizarea de către autoritatea publică a unor acțiuni de interes public;

Registru de evidență a corespondenței - resursa informațională specializată (totalitatea informațiilor ținute în formă automatizată și manuală) care asigură evidența informației sistematizate, principalul obiectiv al căruia consta în asigurarea evidenței corespondenței parvenite la Centrul de Informare și Prestări Servicii din cadrul Primăriei satului Rogojeni.

Registrator - angajatul Primăriei satului Rogojeni împuternicit cu atribuțiile de introducere, modificare, păstrare a informației din Registru,

Furnizorul de date - persoana fizică sau reprezentantul persoanei juridice de drept public sau privat, care prezintă registratorului date despre obiectul registrului în modul stabilit de lege sau acord.

4. Subiecți ai raporturilor juridice apărute ca rezultat al instruirii, administrării și Ținerii manuale a Registrului sînt:

- Primăria satului Rogojeni, în calitate de proprietar și deținător al Registrului;
- persoanele împuternicite de Ținerea Registrului și cele responsabile de efectuarea controlului intern al ultimului;
- persoanele fizice, ale căror date cu caracter personal vor fi stocate în Registru;
- persoanele interesate de a accesa și vizualiza datele din Registru.

5. Angajații Primăriei satului Rogojeni poartă răspundere personală pentru îndeplinirea cerințelor prezentului Regulament, asigurarea confidențialității, securității și păstrarea în stare corespunzătoare a informației din Registrul.

5.1. Petițiile anonime, înaintate în adresa Primăriei satului Rogojeni, în conformitate cu prevederile art.76 alin.(1) al Codului administrativ al Republicii Moldova, aprobat prin Legea nr.116 din 19.07.2018 nu se examinează.

## **II. Condiții generale față de ținerea sistemului de evidență a corespondenței și petițiilor (Registrul)**

6. Registrul de evidență a corespondenței și petițiilor reprezintă un sistem mixt ce utilizează atât evidența în formă electronică, cât și în formă manuală.

7. De către persoana împuternicită de ținerea Registrului din cadrul Primăriei va fi asigurată ținerea în formă manuală a unor componente al Registrului (ținând cont de competența funcțională) prin înscrierea informației, inclusiv păstrarea cărții Registrului de către angajat împuternicit în acest sens (registratorul) din cadrul subdiviziunii respective, în conformitate cu prevederile legislației în vigoare.

8. Persoana responsabilă din cadrul Primăriei va asigura suplimentar, evidența în formă electronică a corespondenței și petițiilor parvenite la Primăria satului Rogojeni.

9. Obiectul înregistrării reprezintă informația referitor la persoanele care au depus adresări/petiții în adresa Primăriei satului Rogojeni.

10. Registrul va ținut în limba de stat.

11. Registratorul este obligat:

- să introducă în Registru numai informație veridică, colectată de la adresant sau din alte surse interzise de lege;

- să asigure evidența în ordine cronologică a fiecărei înscrieri în Registru;

- să nu admită modificarea neîntemeiată a datelor introduse în Registru;

- să efectueze înregistrările în Registru astfel, încât să excludă posibilitatea de a fi radiată (ștersă, distrusă) în mod mecanic, chimic sau în orice alt mod, fără a lăsa urme vizibile ale radierii (ștergerii, distrugerii);

- să asigure accesul la informația din registru doar persoanelor care au dreptul de a primi informația respectivă, în conformitate cu legislația în vigoare;

- să prevină accesul neautorizat la datele din Registru, utilizarea, difuzarea, modificarea sau nimicirea lor ilegală.

12. Datele din registru vor reflecta starea veridică și actuală a informației privind persoanele care s-au adresat la primăria satului Rogojeni.

13. Atît formă manuală, cât și cea electronică a Registrului va cuprinde în mod obligatoriu:

- denumirea registrului;

- denumirea Primăriei satului Rogojeni ca proprietar, posesor și deținător al Registrului;

- numele, prenumele și funcția persoanei responsabile de introducerea datelor în Registru și a administratorului acestuia;

- numele, prenumele și funcția persoanei care va exercita controlul asupra ținerii Registrului;

- numărul Registrului, termenile de ținere și păstrare a acestora.

14. Datele cu caracter personal din Registru vor fi prelucrate în condițiile stabilite de legislația privind protecția datelor cu caracter personal. În acest sens, vor fi realizate măsuri de asigurare a gradului de executare a datelor registrului și de protecție a acestora contra distrugerii întâmplătoare sau neautorizate, modificării, dezvăluirii sau oricăror alte acțiuni ilegale la ținerea registrului.

15. Prelucrarea datelor cu caracter personal în sistemul de evidență al corespondenței și petițiilor parvenite în adresa Primăriei satului Rogojeni, se efectuează în conformitate cu prevederile art.5 alin.(5) lit.b), d), și e) al Legii privind protecția datelor cu caracter personal.

## **III. Condiții generale privind introducerea informației în Registru**

16. Informația privind corespondența parvenită în adresa Primăriei satului Rogojeni va fi recepționată și înregistrată în aceeași zi de persoana responsabilă din cadrul entității și după caz, în fișele de evidență

și control a acestora, iar versiunea electronică parvenită se înregistrează în arhiva electronică a Primăriei satului Rogojeni.

17. Înregistrarea informației în Registru se face prin introducerea mențiunilor necesare în cartea de înregistrări (formă manuală) și în Sistemul informatic (formă electronică) în baza datelor furnizate prin documentele transmise atât de furnizorul datelor registrului (petiționarul agentul economic, autoritatea publică), atât pe suport de hârtie sau în formă electronică, perfectate în modul stabilit de lege.

18. La înregistrarea corespondenței, pe prima pagină se va aplica ștampila de înregistrare în care se indică data primirii și indicele de înregistrare. Indicele de înregistrare constă după caz, din litera inițială a numelui și prenumelui adresantului, numărul și anul de înregistrare a înscrisului.

19. După caz, se va întocmi manual fișa de evidență și control pentru fiecare adresare (în condițiile stabilite prin Instrucțiunile privind ținerea lucrărilor de secretariat referitoare la petițiile persoanele fizice și juridice, adresate organelor de stat, întreprinderilor, instituțiilor și organizațiilor Republicii Moldova, aprobate prin Hotărârea Guvernului nr.208 din 31 martie 1995), introducându-se datele cu caracter personal ce vizează petiționarul (nume, prenume, adresa de domiciliu, numărul de telefon) precum și rezoluția conducerii Primăriei satului Rogojeni, termenul de soluționare stabilit de conducerea Primăriei satului Rogojeni, datele despre starea executării etc.

20. După examinarea și soluționarea definitivă, pe fișa de evidență și control se aplică semnătura persoanei responsabile de evidență, iar în sistemul informatic se face mențiunea despre finalizarea acestea și modificarea statutului ca "Închis".

21. Modificările și radierile făcute în Registru se efectuează în baza decizie și cu semnătura registrului în situația existenței unui motiv întemeiat în acest sens.

22. Dacă furnizorul datelor registrului se adresează cu un demers argumentat privind rectificarea datelor eronate sau inexacte, registratorul va face în modul stabilit, corecturile necesare și va informa despre aceasta furnizorul datelor.

23. Greșelile de ordin tehnic de către persoana împuternicită de ținerea Registrului se rectifică de către acesta. Corectarea greșelii se specifică într-o rubrică aparte, urmată de semnătura persoanei care a efectuat înscrierea.

24. Radierea obiectului din Registru se face prin inserarea unei note speciale (care trebuie să conțină semnăturile responsabile și data radierii) și nu reprezintă excluderea fizică a datelor despre obiect din Registru.

25. Rectificările și radierile inscrierilor din Registru se efectuează astfel încât textul inițial să fie citibil.

#### **IV. Condiții generale privind păstrarea și furnizarea informației din Registru**

26. Păstrarea Registrului este asigurată de registrator pînă la adoptarea deciziei conducerii Primăriei satului Rogojeni despre lichidarea registrului, dar nu mai mult decît pe perioada stabilita de lichidatorul documentelor-tip și a termenilor lor de păstrare pentru organele administrației publice, pentru instituțiile, organizațiile și întreprinderile Republicii Moldova, aprobat de Serviciul de Stat de Arhivă nr.57 din 27.07.2016.

27. Ținerea Registrului este supusă controlului intern și extern, în conformitate cu prevederile art.31 al Legii cu privire la registre.

28. În acest sens, persoana împuternicită de ținerea și păstrarea Registrului este obligată:

- să prevină accesul nesancționat la datele stocate în Registru;
- să întreprindă acțiuni în vederea neadmiterii cazurilor de utilizare ilegală, dezvăluire ilegală a informației conținute în acesta, de modificare sau nimicire a acestor date.

29. Persoanele împuternicite de ținerea și controlul registrului sînt obligate să nu divulge informația la care au primit acces în legătură cu exercitarea atribuțiilor funcționale, inclusiv după încetarea activității în cadrul Primăriei satului Rogojeni.

30. Registratorul este obligat să asigure accesul la informația din registru pentru angajații autorizați ai Primăriei satului Rogojeni și alte persoane, care au dreptul de a primi informația respectivă, în conformitate cu legislația în vigoare sau care demonstrează dreptul și interesul legitim de a primi aceste informații, din momentul în care acesta vor fi disponibile, dar nu mai tarziu de 5 zile de la data depunerii cererii.

31. Informația poate fi furnizată gratuit sau contra plată în conformitate cu Legea privind accesul la informație.

32. Extrasul din Registru trebuie să fie semnat de conducerea Primăriei satului Rogojeni, cu indicarea datei întocmirii/eliberării acestuia.

## **V. Condițiile suplimentare privind gestionarea Registrului în formă manuală**

33. Ținerea manuală a Registrului de evidență a corespondenței se efectuează sub formă de fișier sau prin introducerea mențiunilor în cartea pentru înregistrări.

34. În acest sens, evidența corespondenței în cadrul Primăriei satului Rogojeni este dusă prin intermediul mai multor Registre ținute în formă manual, cum ar fi:

- *Registrul cererilor / petițiilor*
- *Registrul cererilor de comunicare a informațiilor de interes public*
- *Registrul documentelor intrate*
- *Registrul documentelor expediate*
- *Registrul evidensei declarațiilor ( de căsătorie, de paternitate, Cereri de mamă solitară)*
- *Registrul Declarațiilor de naștere a copilului*
- *Registrul de evidență a certificatelor de Stare Civilă eliberate de primăria Rogojeni*
- *Registrul de evidență a declarațiilor de primire în spațiul locativ*
- *Registrul de evidență a Dispozițiilor normative ale primarului*
- *Registrul de evidență a Dispozițiilor individuale ale primarului*
- *Registrul documentelor eliberate pentru deschiderea Dosarelor de succesiune de către notari*
- *Registrul actelor notariale*
- *Registrul Declarațiilor de avere și interese personale*
- *Registrul contractelor cu persoane juridice și fizice*
- *Registre ce țin de calcularea și achitarea salariului angajaților*
- *Registrul cadastral al deținătorilor de terenuri.*
- *Registru de evidență a contribuabililor la impozitele funciar și pe bunurile imobiliare.*
- *Registru de înregistrare a contractelor de arendă a terenurilor private*
- *Registru de evidență a contribuabililor la impozitele funciare și pe bunurile imobiliare*
- *Registru conturilor personale la impozitele și taxele locale administrate de serviciul de colectare a impozitelor și taxelor locale din cadrul primăriei*
- *Registrul Dosarelor personale ale funcționarilor publici*
- *Registrul Contractelor de muncă.*

35. Registratorul, suplimentar la cele expuse în cap.IV, în cazul gestionării Registrului în formă manuală, este obligat:

- să efectueze înscrierile citeț și clar. Prescurtările vor fi făcute astfel pentru a fi evitate diferite interpretări. Textul greșit se taie cu o linie, fiind posibilă citirea textului greșit înscris;
- să nu înlocuiască neîntemeiat filele din cartea registrului prin extragerea lor, înclieierea unor noi file etc;
- să asigure, în cazul deteriorării cărții, posibilitatea restabilirii imediate a datelor din registru fără a cauza daune informației, ce se conține în ea;
- să asigure snuruirea cărților pentru înregistrări ( în caz că nu este o carte integrală) și numerotarea filelor. Numărul de file se indică pe ultima pagină și se autentifică (inclusiv conținutul cărții) prin aplicarea semnelor de control de către conducerea Primăriei: semnătura și ștampila.

36. Informația va fi introdusă în Registru de ordine cronologică, ținându-se cont de necesitatea prezenței mențiunilor privind:

- numărul de ordine a mențiunii;
- numărul și data de intrare;
- numele și prenumele;
- conținutul succint al documentului;
- numele și prenumele executantului, termenul de executare și rezoluția conducerii Primăriei satului Rogojeni;

-rezultatul examinării: admisă/respinsă/oferite explicații de rigoare/acte de reacționare adoptate de conducerea Primăriei satului Rogojeni;  
-alte date relevante.

37. Registrul se păstrează de persoana responsabilă într-un safeu metalic și va conține un compartiment separat în care se vor consemna înregistrările de audit a securității, prevăzute de pct.79 al Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal.

## **VI. Condiții suplimentare privind gestionarea Registrului în formă electronică**

38. Ținerea în formă electronică a Registrului de evidență a corespondenței este realizat de Primăria satului Rogojeni prin intermediul unui sistem informațional automatizat special constituit - Sistemul informatic.

39. Introducerea, modificarea și păstrarea informației în acest Registru este asigurată de registratorul desemnat din cadrul Centrului de Informare și Prestări Servicii.

40. La înscrierea informației privind corespondența parvenită, în Registru se înserează și o listă de date despre obiect, inclusiv date cu privire la faptul înregistrării în compartimentele special destinate, și anume:

- tipul adresării;
- data și numărul de intrare;
- termenul de rezolvare și data expirării;
- numele, prenumele adresantului;
- adresa de domiciliu, e-mail (în cazul existenței);
- numărul de telefon fix/mobil;
- conținutul succint al adresării;
- rezoluția conducerii Primăriei satului Rogojeni;
- persoana responsabilă de control și executorul;
- copia scanată, în format "pdf" a adresării;
- date privind executarea;
- date privind posibila prelungire (termenul, numărul documentul prin care s-a efectuat prelungirea, informarea adresantului);
- rezultatul examinării: admisă/respinsă/oferite explicații de rigoare/acte de reacționare adoptate de Primăria satului Rogojeni;
- alte date relevante privind examinarea corespondenței și petițiilor.

40.1. Sistemul informațional de evidență al corespondenței și petițiilor va fi gestionat, pe toată perioada ciclului de viață, în conformitate cu prevederile stabilite de cerințele 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, în special pct.11-13, 22,24,26,28,30,32-33, 35-37, 39-73, 75-78, 85-86, 88, 90.

## **VII. Măsurile de protecție a datelor cu caracter personal prelucrate în sistemul de evidență a corespondenței și petițiilor**

41. La terminarea sesiunilor de lucru, computerele și imprimantele se deconectează.

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

43. Accesul fizic la mijloacele de reprezentare a informației preluate din sistemul de evidență a corespondenței și petițiilor este blocat împotriva vizualizării de către persoane neautorizate.

44. Mijloacele de prelucrare a informațiilor preluate din registrul de evidență a corespondenței sau soft-urile destinate prelucrării acestora sînt scoase din perimetrul de securitate doar în baza permisiunii scrise a operatorului.

45. Scoaterea și introducerea mijloacelor de prelucrare a informațiilor din sistemul de evidență a corespondenței și petițiilor din/în perimetrul de securitate se înregistrează într-un registru specializat.

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

47. Cerințe speciale față de marcare: toate informațiile ieșite din sistemul de evidență a corespondenței și petițiilor, care conțin date cu caracter personal, sînt supuse marcării, cu indicarea numărului de identificare unic al operatorului de date cu caracter personal.

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

48. Accesul la biroul unde este amplasat sistemul de evidență a corespondenței și petițiilor este restricționat, fiind permis doar persoanele care au autorizația necesară și doar în timpul orelor de program. Accesul în birou este posibil doar cu autorizarea de acces și/sau cheia de la lacătul mecanic.

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

50. Înainte de acordarea accesului fizic la sistemul de evidență a corespondenței și petițiilor, se verifică competențele de acces.

51. Registrele de monitorizare se păstrează minimum un an, la expirarea termenului indicat, acesta se lichidează, iar datele și documentele ce se conțin în registrul supus lichidării se transmit în arhivă, conform cerințelor prevăzute în instrucțiunile cu privire la ținerea lucrărilor de secretariat.

52. Perimetrul de securitate se consideră perimetrul biroului în care este amplasat sistemul de evidență a corespondenței și petițiilor, fiind integru din punct de vedere fizic.

53. Zilnic se inspectează perimetrul de securitate al clădirii și al biroului, unde este amplasat sistemul de evidență a corespondenței și petițiilor, din punct de vedere fizic.

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

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

56. Amplasarea sistemului de evidență a corespondenței și a petițiilor răspunde necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.

57. Securitatea electroenergetică: este asigurată securitatea echipamentului electric utilizat pentru menținerea funcționalității sistemului de evidență a corespondenței și petițiilor, 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 registrul, inclusiv posibilitatea deconectării oricărui component TI.

58. Computerele, unde este amplasat fizic sistemul de evidență a corespondenței și petițiilor, 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.

59. Securitatea cablurilor de rețea: cablurile de rețea, prin care se efectuează operațiunile de transmitere a datelor preluate din sistemul de evidență a corespondenței și petițiilor, sînt protejate contra conectărilor nesancționate sau deteriorărilor. Pentru a exclude bruiajul, cablurile de tensiune sînt separate de cele comunicaționale.

60. Securitatea antiincendiară a sistemului de evidență a corespondenței și petițiilor: biroul unde este amplasat registrul este dotat cu echipament antiincendiar și corespunde cerințelor și normelor antiincendiarie în vigoare.

61. 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 corespondenței și petițiilor. La expirarea termenului de păstrare, informațiile, care conțin date cu caracter personal și care se conțin pe purtătorii de informații se distrug.

### **VIII. Identificarea și autentificarea utilizatorului sistemului de evidență a corespondenței și petițiilor**

62. Este efectuată identificarea și autentificarea utilizatorilor informațiilor preluate din sistemul de evidență a corespondenței, petițiilor și a proceselor executate în numele acestor utilizatori.

63. Toți utilizatorii (inclusiv administratorii de rețea, programatorii și administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului) care nu trebuie să conțină semnamentele nivelului de accesibilitate al utilizatorului.

64. 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 acesteia (plasarea înscrierilor în safeu)La momentul introducerii , parolelor nu se reflectă în clar pe monitor.

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

66. 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 unei perioade îndelungate (mai mult de 3 luni), codurile de identificare și autentificare se revocă sau se suspendă.

67. Folosirea tehnologiilor fără fir, echipamentelor portative și mobile se autosizează de persoanele responsabile.

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

69. Orice activitate de dezvăluire a datelor cu caracter personal către terți este documentată și supusă unei analize riguroase în prealabil privind scopul și termenul legal a intențiilor de dezvăluire a unui anumit volum de date cu caracter personal.

70. Orice încălcare a securității în ceea ce privește sistemul de evidență a corespondenței și petițiilor este supusă documentării, iar persoana responsabilă de realizarea politicii de securitate este informată în legătură cu acest lucru cît de urgent posibil.

71. Înainte de acordarea accesului la sistem, utilizatorii sînt informați despre faptul că folosirea registrului este controlată și că folosirea neautorizată a acestora este sancționată în conformitate cu legislația civilă, contravențională și penală.

## **IX. Auditul securității în sistemul de evidență a corespondenței și petițiilor**

72. Se organizează generarea înregistrărilor de audit a securității în sistemul de evidență a corespondenței și petițiilor pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.

73. Se efectuează înregistrarea tentativelor de intrare/ieșire a utilizatorului în sistem, conform următorilor parametri:

- a) data și numărul tentativei/ieșirii;
- b) ID-ul utilizatorului.

74. Se efectuează înregistrarea tentativelor de obținere a accesului ( de executare a operațiunilor) pentru aplicații și procese destinate prelucrării informațiilor din registrul de evidență a corespondenței, conform următorilor parametri:

- a) data și timpul tentativei de obținere a accesului (executare a operațiunii);
- b) ID-ul utilizatorului;
- c) specificațiile resursei protejate (identificator, nume logic, nume fișier, număr etc);
- d) tipul operațiunii solicitate (citire, înregistrare, ștergere etc)

75. Cazurile de deranjament al auditului securității în sistemul de evidență a corespondenței și petițiilor sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, sînt aduse la cunoștința persoanei responsabile de politică de securitate a datelor cu caracter personal, care întreprinde măsuri în vederea restabilirii capacității de lucru a sistemului de audit.

76. Rezultatele auditului securității în sistemul de evidență a corespondenței și petițiilor (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.

77. Durata minimă a stocării rezultatelor auditului securității în sistemul de evidență a corespondenței și petițiilor 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 investigațiile sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

## **X. Asigurarea integrității informațiilor din sistemul de evidență a corespondenței și petițiilor**

78. Copiile de siguranță a informațiilor din sistemul de evidență a corespondenței, petițiilor și soft-urilor folosite pentru prelucrările automatizate a acestora vor fi efectuate în regimul automat, zilnic, reeșind din volumul prelucrărilor efectuate. 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.

## **XI. Gestionarea incidentelor de securitate a sistemului de evidență a corespondenței și petițiilor**

79. Persoanele care asigură exploatarea sistemului de evidență a corespondenței și petițiilor 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.

80. 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 corespondenței și petițiilor.

81. În cazul producerii incidentelor de securitate personale 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.

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

## **XII. Dispoziții finale**

83. Prezentul Regulament este revizuit și ulterior aprobat de către Primăria satului Rogojeni periodic, însă cel puțin o dată în an, precum și la necesitate.

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

85. Regulamentul este adus la cunoștința angajaților contra semnătură.

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

## **LISTA**

**angajaților familiarizați cu prevederile Regulamentului privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență a corespondenței și petițiilor parvenite în adresa Primăriei satului Rogojeni**

<b>Nr. d/o</b>	<b>Numele, prenumele</b>	<b>Funcția</b>	<b>Am luat cunoștință (semnătura)</b>	<b>Data</b>
1.	Groza Ruslan	Primar		
2.	Ardeleanu Viorica	Secretara consiliului		
3.	Guzun Ana	Contabila șefă		
4.	Odagiu Maria	specialistă		

**REGULAMENT**  
**Cu privire la asigurarea securității datelor cu caracter personal**  
**în sistemul de evidență a resurselor umane în cadrul**  
**Primăriei satului Rogojeni**

**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 Rogojeni stabilește responsabilitățile persoanelor sub diviziunea 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 Rogojeni ce au acces la datele cu caracter personal nu vor depăși limitele stabilite de Politica de securitate a Primăriei satului Rogojeni, 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 sistemului de evidență a resurselor umane, sunt prelucrate următoarele categorii de date cu caracter personal:
  - *Numele, prenumele;*
  - *Sexul;*
  - *Data și locul nașterii;*
  - *Cetățenia;*
  - *IDNP;*
  - *Imagine;*
  - *Situația familială;*
  - *Situația militară;*
  - *Datele personale ale membrilor de familie;*
  - *Datele din permisul de conducere;*

- *Datele pentru transferul pe contul bancar a plăților salariale și a altor sume datorate cu titlu de indemnizații, compensații sau alte beneficii, după caz;*
- *Semnătura;*
- *Datele din actele de stare civilă;*

- *numărul dosarului de pensie;*
- *codul personal de asigurării sociale (CPAS);*
- *codul asigurării medicale (CPAM);*
- *numărul de telefon/fax;*
- *numărul de telefon mobil;*
- *adresa (domiciliului/reședinței);*
- *adresa e-mail;*
- *profesia și/sau locul de muncă;*
- *formarea profesională - diplome - studii;*
- *numele, prenumele (după caz, patronimicul) persoanelor care se află la întreținerea persoanei respective (membrii familiei, alte rude și persoane, după caz);*
- *mărimea concretă a drepturilor salariale calculate, taxele și impozitele aferente, inclusiv contribuțiile de asigurări sociale obligatorii de asistență medicală și socială, și alte sume datorate în virtutea legii sau contractului;*
- *datele din certificatele de concediu medical acordate, necesare pentru calcularea indemnizației corespunzătoare;*
- *informații de recrutare (inclusiv copii ale diplomelor de studii, referințe și alte informații incluse într-un CV sau scrisoare de intenție ca parte a procesului de aplicare);*
- *Informații despre utilizarea de către angajat a sistemelor noastre de informare și comunicații;*
- *după caz, alte date necesare îndeplinirii scopului menționat, conform legislației în vigoare.*

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 carnetele 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 conține în sistemul de evidență a Resurselor Umane în cadrul entității se prelucrează și se stochiază:
- 1) pe suport de hârtie;
  - 2) în format electronic:
- a) Software – Sistemul de evidență a resurselor umane: 1C
  - b) Hardware –Nr. de inventariere 31460024; 31420010
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 Rogojeni, raionul Șoldănești, s.Rogojeni, MD-7230.

### **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 ROGOJENI** 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 ROGOJENI** sunt păstrate în formă arhivată, pe perioada stabilită de Nomenclatorul dosarelor din cadrul **PRIMĂRIEI SATULUI ROGOJENI**.

### **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 desfășoară 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 privind protecția datelor cu caracter personal nr.133 din 08.07.2011.*

21. Biroul nu este lăsat niciodată fără supraveghere, la ieșirea în exterior ușa biroului se încuie cu lacătul. 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 nesanționate. 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 nesanționate 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 incendiare 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 s conțin pe purtătorii de informații, se distrug.

## **VI. AUDITUL SECURITĂȚII ÎN SISTEMUL 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 investigațiile sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

## **V. GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMULUI DE EVIDENȚĂ A RESURSELOR UMANE**

37. 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.

38. 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.

39. 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.

40. „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 sânt obligate să ofere suportul necesar și să asigure accesul la informațiile necesare relevante obiectului controlului.”

## VI. DISPOZIȚII FINALE

41. Prezentul Regulament este aprobat de către organul de conducere al **PRIMĂRIEI SATULUI ROGOJENI** și revizuit periodic, la necesitate, în cazul modificării legislației în vigoare.
42. Prezentul Regulament se completează cu prevederile legislației în vigoare.
43. 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 Rogojeni raionul Șoldănești

Nr	Numele, prenumele	Funcția	Am luat cunoștință (semnătura)	Data
1.	Groza Ruslan	primar		
2.	Ardeleanu Viorica	secretara consiliului		
3.	Guzun Ana	contabila - șefa		
4.	Odagiu Maria	specialistă		

**REGULAMENTUL**  
**PRIVIND PRELUCRAREA INFORMAȚIILOR CE CONȚIN DATE**  
**CU CARACTER PERSONAL ÎN SISTEMUL DE EVIDENȚĂ CONTABILĂ**  
**A PRIMĂRIEI SATULUI ROGOJENI**

**I. DISPOZIȚII GENERALE**

**1.1.** Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență contabilă (în continuare Regulament) este elaborat în vederea implementării în cadrul **PRIMĂRIEI SATULUI ROGOJENI**, a prevederilor Legii nr.133 din 8 iulie 2011 privind protecția datelor cu caracter personal, Legii contabilității nr. 113 din 27 aprilie 2007 și 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.1 123 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 **PRIMĂRIEI SATULUI ROGOJENI** în cadrul sistemului de evidență contabilă.

**II. SCOPUL**

**2.1.** Scopul prelucrării informațiilor ce conțin date cu caracter personal în sistemul de evidență contabilă constă în asigurarea înregistrării informațiilor contabile referitoare la calculul drepturilor salariale ale angajaților, inclusiv a premiilor, stimulărilor, sporurilor, indemnizațiilor, compensațiilor și altor drepturi și obligații cu conținut pecuniar, precum și a prezentării rapoartelor financiare, trimestriale și anuale către instituțiile statului, conform legislației în vigoare.

**2.2.** Prelucrarea datelor cu caracter personal în sistemul de evidență contabilă se efectuează în conformitate cu prevederile art. 5 alin. 5 lit. a), b) și e) al Legii privind protecția datelor cu caracter personal.

**2.3.** În cadrul sistemului de evidență contabilă sânt prelucrate următoarele categorii de date cu caracter personal:

- numele, prenumele și patronimicul;
- sexul;
- numărul personal de identificare de stat (IDNP);
- data nașterii și domiciliul;
- telefon mobil/fix/fax;
- semnătura/semnătura digitală;
  
- date din acte de stare civilă,
- profesie, funcție
- formare profesională, diplome, studii

- cetățenia;
- situație economică sau financiară;
- imagine;
- date bancare,
- date din permisul de conducere
- sancțiuni disciplinare
- codul personal de asigurări sociale (CPAS);
- codul personal de asigurări medicale (CPAM);
- adresa domiciliului, reședinței,
- datele privind locul de muncă,
- mărimea salariului brut și alte premii, sporuri, stimulări,
- datele privind situația familială ;
- datele din certificatele de concediu medical

**2.4.** 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 **PRIMĂRIEI SATULUI ROGOJENI** și care au impact asupra calculării plăților salariale, precum și a persoanelor fizice și juridice cu care **PRIMĂRIA SATULUI ROGOJENI** intră în relații contractuale;
- b) Calcularea drepturilor salariale lunare, în conformitate cu legislația în vigoare a Republicii Moldova (conform contractelor individuale de muncă, contractelor civile, tabelelor de pontaj, ordinelor/dispozițiilor conducerii, raportului de activitate lunară);
- c) Prelucrarea certificatelor de concedii medicale ale angajaților în vederea stabilirii indemnizațiilor de incapacitate temporară de muncă;
- d) Prelucrarea copiilor ordinelor/dispozițiilor conducerii referitoare la personal;
- e) Calcularea și reținerea taxelor ce țin de plățile salariale aferente angajaților: primele de asigurare obligatorie de asistență medicală, contribuțiile la bugetul asigurărilor sociale de stat, impozitul pe venit, etc.;
- f) Calcularea și virarea primelor de asigurare obligatorie de asistență medicală și a contribuțiilor la bugetul asigurărilor sociale de stat, aferente plăților salariale - obligație a angajatorului;
- g) Furnizarea informației necesare pentru elaborarea rapoartelor lunare privind contribuțiile de asigurare socială de stat obligatorii (forma IPC 18) și rapoartelor trimestriale privind primele de asigurare obligatorie de asistență medicală (forma IPC 18);
- h) Întocmirea, lunară, a declarației persoanei asigurate REV 5 pentru fiecare angajat și transmiterea acestora Casei Teritoriale de Asigurări Sociale, în format electronic prin SIA E- REPORTING cu aplicarea semnăturii digitale;
- i) 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;
- j) Completarea lunară, trimestrială și anuală a dărilor de seamă cu prezentarea acestora Inspectoratului Fiscal de Stat, precum și perfectarea și eliberarea informației privind veniturile

k) calculate și achitate în folosul persoanei fizice și impozitul pe venit reținut din aceste venituri angajaților **PRIMĂRIEI SATULUI ROGOJENI**;

l) Prelucrarea cererilor și a documentelor confirmative privind acordarea scutirilor la impozitul pe venit reținut din salariu, în conformitate cu capitolul 4, titlul II din Codul Fiscal;

m) **Eliberarea certificatelor de salariu, la cererea angajaților**;

n) Completarea și stocarea fișelor personale de evidență a veniturilor sub formă de salariu și alte plăți efectuate de către patron în folosul angajatului pe fiecare an, precum și a impozitului pe venit reținut din aceste plăți (Anexa nr. 8 la Ordinul IFPS nr.676 din 14.12.2007);

o) Emiterea, transmiterea și primirea documentelor financiar-contabile (facturi, anexe la facturi, documente justificative, acte de prestare servicii);

p) Prezentarea documentelor financiare ce conțin date cu caracter personal către acționari/fondatori, comisiei de cenzori, auditului intern sau extern. În cazul datelor cu caracter personal ale angajaților sau ale altor persoane, **PRIMĂRIA SATULUI ROGOJENI** se află în relație juridică, îi va înștiința pe aceștia atunci când datele respective vor fi transmise către terți;

**2.5.** Datele cu caracter personal ce fac obiectul reglementării prezentului Regulament vor fi stocate de către astfel încât să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sânt 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.

**2.6.** Orice utilizare a datelor cu caracter personal, introduse în sistemul de evidență contabilă în alte scopuri decât cele menționate mai sus este interzisă.

### **III. LOCAȚIA ȘI DESCRIEREA SISTEMULUI DE EVIDENȚĂ CONTABILĂ**

**3.1.** Datele cu caracter personal conținute în sistemul de evidență contabilă în cadrul **PRIMĂRIEI SATULUI ROGOJENI** se prelucrează/stochează:

1. pe suport de hârtie;

2. în format electronic:

- Software - Sistemul de evidență contabilă IC- 2.098

- Hardware - Calculator cu Nr. de inventariere: nr. **31420001**;

**3.2** Prelucrarea informațiilor în sistemul de evidență contabilă pe suport de hârtie este structurată după criteriul “mape-dosare”, fiind păstrate în dulapuri, care sânt amplasate fizic în biroul contabilității **PRIMĂRIEI SATULUI ROGOJENI rnl. ȘOLDĂNEȘTI, s. Rogojeni, MD-7230.**

**3.3.** Mentenanța programului contabil IC a **PRIMĂRIEI SATULUI ROGOJENI** este efectuată de către compania **SRL „BIT GENERATOR”** fiind încheiat contractul cu următoarele principalele atribuții stabilite companiei prestatoare:

Efectuarea ajustărilor în program, în baza modificărilor legislației Republicii Moldova; Eliminarea erorilor în funcționarea programului;

Consultarea în rezolvarea dificultăților apărute în utilizarea programului;

Examinarea solicitărilor parvenite din partea **PRIMĂRIEI SATULUI ROGOJENI**;

Vizite la fața locului, la solicitarea **PRIMĂRIEI SATULUI ROGOJENI**;

Examinarea și nedivulgarea informației cu accesibilitate limitată ce a devenit cunoscută la prestarea acestor servicii.

### **IV. DURATA DE STOCARE**

**4.1.** Prelucrarea datelor cu caracter personal în sistemul de evidență contabilă se efectuează pe perioada

valabilității contractelor de achiziție publică, pe perioada activității angajaților Primăriei (din momentul semnării contractului până la finalizarea efectuării acțiunilor prevăzute de actele legislative în cazul încetării raporturilor de muncă).

4.2. La expirarea termenilor menționați, datele din sistemul de evidență contabilă sânt păstrate în formă arhivată, pe perioada stabilită de Nomenclatorul dosarelor din cadrul **PRIMĂRIEI SATULUI ROGOJENI**, ulterior fiind supuse distrugerii sau ștergerii, în funcție de suportul pe care au fost efectuate.

## V. DREPTURILE ANGAJAȚILOR ȘI PERSOANELOR VIZATE

5.1. **PRIMĂRIA SATULUI ROGOJENI**, 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 Injustiției.

5.3. Toate persoanele implicate în activitatea de administrare și/sau prelucrare a informațiilor din sistemul de evidență contabilă 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 **PRIMĂRIEI SATULUI ROGOJENI**. 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 CONTABILĂ

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 contabilă, 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 contabilă este blocat împotriva vizualizării de către persoane neautorizate.

6.1.5. Mijloacele de prelucrare a informațiilor preluate din sistemul de evidență contabilă sau soft-urile destinate prelucrării acestora sânt 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 contabilă din/în perimetrul de securitate se înregistrează în registru.

6.2. Măsurile de protecție a datelor cu caracter personal, prelucrate în sistemul de evidență contabilă, se

înfăptuiesc ținând cont de necesitatea asigurării confidențialității și integrității acestora, prin protecție în formă manuală, electronică.

**6.3.** Cerințe speciale față de marcare: toate informațiile ieșite din sistemul de evidență contabilă, care conțin date cu caracter personal, sânt supuse marcării, cu indicarea prescripțiilor pentru prelucrarea ulterioară și răspândirea 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 contabilă 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 contabilă, 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 contabilă, 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 contabilă, din punct de vedere fizic.

**6.10.** Computerele sânt amplasate în locuri cu acces limitat pentru persoane străine.

**6.11.** Ușile și ferestrele sânt încuiate în cazul în care în încăpere lipsesc angajații autorizați de administrarea sistemului.

**6.12.** Amplasarea sistemului de evidență contabilă 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 contabilă, 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 contabilă, inclusiv posibilitatea deconectării oricărui component TI.

**6.14.** Computerele, unde este amplasat fizic sistemul de evidență contabilă, dispun de UPS-uri, care sânt 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 contabilă, sânt protejate contra conectărilor nesancționate sau deteriorărilor. Pentru a exclude bruiajul, cablurile de tensiune sânt separate de cele comunicaționale.

**6.16.** Securitatea anti incendiară a sistemului de evidență contabilă: biroul unde este amplasat sistemul de evidență contabilă este dotat cu echipament anti incendiar și corespunde cerințelor și normelor anti incendiare 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 contabilă. 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 CONTABILĂ

7.1. Este efectuată identificarea și autentificarea utilizatorilor informațiilor preluate din sistemele de evidență contabilă 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 sânt utilizate parole. Utilizarea parolelor în procesul asigurării securității informaționale: pe lângă cerințele de păstrare a confidențialității parolelor, este interzisă înscrierea acestora pe suport de hârtie, cu excepția cazului de asigurare a securității păstrării acesteia (plasarea înscrisurilor în safeu). La momentul introducerii, parolele nu se reflectă în clar pe monitor.

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

7.5. Întru asigurarea posibilității de stabilire a responsabilității fiecărui utilizator, sânt 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 contabilă, 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 contabilă, încetează automat la expirarea perioadei stabilite în timp (pentru

7.9. 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 contabilă. Se folosesc mijloace automatizate de înregistrare și informare despre crearea, modificarea, dezactivarea și încetarea acțiunii conturilor de acces.

7.10. 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 contabilă.

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

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

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

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

7.14. Orice activitate de dezvoltare a datelor cu caracter personal către terți este documentată și supusă unei analize riguroase în prealabil privind scopul și temeiul legal a intențiilor de dezvoltare a unui anumit volum de date cu caracter personal.

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

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

## **VIII. AUDITUL SECURITĂȚII ÎN SISTEMELE DE EVIDENȚĂ CONTABILĂ**

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

8.2. Se efectuează înregistrarea tentativelor de intrare/ieșire a utilizatorului în sistem, conform următorilor parametri:

- a) data și timpul tentativei intrării/ieșirii;
- b) ID-ul utilizatorului;
- c) rezultatul tentativei de intrare/ieșire - pozitivă sau negativă.

8.3. Se efectuează înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative și proceselor, destinate prelucrării informațiilor din sistemele de evidență contabilă, 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.

8.4. Se efectuează înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării informațiilor din sistemul de evidență contabilă, 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.

**8.5.** 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.

**8.6.** Se efectuează înregistrarea ieșirii din sistemul de evidență contabilă, 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.

**8.7.** Cazurile de deranjament al auditului securității în sistemul de evidență contabilă sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, sînt 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.

**8.8.** Rezultatele auditului securității în sistemul de evidență contabilă (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.

**8.9.** Durata minimă a stocării rezultatelor auditului securității în sistemul de evidență contabilă 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 investigațiile sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

## **IX. ASIGURAREA INTEGRITĂȚII INFORMAȚIILOR DIN SISTEMUL DE EVIDENȚĂ CONTABILĂ**

**9.1.** Se asigură identificarea, protocolarea și înlăturarea deficiențelor de soft-uri destinate prelucrării informațiilor din sistemul de evidență contabilă, 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.

**9.2.** 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 contabilă.

**9.3.** Se asigură testarea funcționării corecte a componentelor de securitate a sistemului de evidență contabilă (automat - la pornirea sistemului, și după caz - la solicitarea persoanei responsabile de politica de securitate a prelucrării datelor cu caracter personal).

**9.4.** 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 contabilă 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 CONTABILĂ

**10.1.** Persoanele care asigură exploatarea sistemului de evidență contabilă 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.

**10.2.** 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 contabilă.

**10.3.** „În cazul producerii incidentelor de securitate persoanele responsabile va 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.”

**10.4.** Persoanele care se fac vinovate de încălcarea normelor privind obținerea, păstrarea, prelucrarea și protecția informațiilor din sistemul de evidență contabilă poartă răspundere civilă, contravențională și penală.

## XI. DISPOZIȚII FINALE

**11.1.** Prezentul Regulament este revizuit și ulterior aprobat de către conducerea **PRIMĂRIEI SATULUI ROGOJENI** periodic, însă cel puțin o dată în an, precum și la necesitate.

**11.2.** Prezentul Regulament se completează cu prevederile legislației în vigoare.

**11.3.** Regulamentul este adus la cunoștința angajaților contra semnăturii.

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

### LISTA ANGAJAȚILOR FAMILIARIZAȚI CU PREVEDERILE REGULAMENTULUI PRIVIND PRELUCRAREA INFORMAȚIILOR CE CONȚIN DATE CU CARACTER PERSONAL ÎN SISTEMUL DE EVIDENȚĂ CONTABILĂ A PRIMĂRIEI SATULUI ROGOJENI

N	Numele, prenumele	Funcția	Am luat cunoștință (semnătura)	Data
1	Groza Ruslan	primar		
2	Guzun Ana	contabila - șefa		
3	Ardeleanu Viorica	Secretara conconsiliului		
5				
6				
7				

**POLITICA**  
**PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL**  
**ÎN CADRUL PRIMĂRIEI SATULUI ROGOJENI**

## PREAMBUL

La prelucrarea datelor cu caracter personal în cadrul entităţii sunt aplicate principiile prevăzute de actele **internaţionale** - Declaraţia universală a drepturilor omului, Convenţia pentru apărarea drepturilor omului şi a libertăţilor fundamentale, Convenţia pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal şi a celor **naţionale** - Constituţia Republicii Moldova, Legea privind protecţia datelor cu caracter personal, Legea privind accesul la informaţie, Cerinţele faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal.

## II. INTRODUCERE

**PRIMĂRIA SATULUI ROGOJENI** (în continuare ”**primăria**” sau ”**entitatea**”) are sediul înregistrat în **raionul Şoldăneşti, s. Rogojeni, MD-7230**. Prezenta Politică privind protecţia datelor cu caracter personal (în continuare - Politică) este aprobată de către **PRIMĂRIA SATULUI ROGOJENI** care acţionează în baza legislaţiei.

Prezenta Politică este aprobată, inclusiv, în vederea conformării **PRIMĂRIEI SATULUI ROGOJENI** cu prevederile legislaţiei în vigoare în domeniul protecţiei datelor cu caracter personal.

## III. NOȚIUNI GENERALE

În prezenta Politică, sânt defmite/utilizate următoarele noţiuni:

*Date cu caracter personal* - orice informaţie referitoare la o persoană fizică identificată sau identificabilă (persoana vizată); o persoană fizică identificabilă este persoana care poate fi identificată, direct sau indirect, prin referire la un număr de identificare, date de localizare, un identificator online sau la unul ori mai multe elemente specifice identităţii sale fizice, fiziologice, psihice, economice, culturale sau sociale;

*Date privind sănătatea* — reprezintă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistenţă medicală, care dezvăluie informaţii despre starea de sănătate a acesteia;

*Operator* - reprezintă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile şi mijloacele prelucrării sunt stabilite prin actele normative, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în actele normative;

*Persoană împuternicită de către operator* - persoana fizică sau persoana juridică, autoritatea publică agenţia sau alt organism, care prelucrează date cu caracter personal în numele operatorului;

*Autentificare* - verificarea identificatorului atribuit subiectului de acces, confirmarea autenticităţii;

*Integritate* - certitudinea, ne contradictorialitatea şi actualitatea informaţiei care conţine date cu caracter personal, protecţia ei de distrugere şi modificare neautorizată;

*Politica privind protecţia datelor cu caracter personal* — document, elaborat de către operatorul de date - **PRIMĂRIA SATULUI ROGOJENI**, care oferă o descriere precisă a măsurilor de securitate şi trăsăturilor de protecţie selectate pentru securitatea datelor, ținându-se cont de potenţialele pericole pentru datele cu caracter personal prelucrate şi riscurile reale la care sânt expuse acestea;

*Perimetru de securitate* - zona care reprezintă în sine o barieră de trecere asigurată cu mijloace de control fizic şi/sau tehnic al accesului;

*Purtător de date cu caracter personal* - suport magnetic, optic, laser, de hârtie sau alt suport al informaţiei, pe care se creează, se fixează, se transmite, se recepţionează, se păstrează sau, în alt mod, se utilizează documentul şi care permite reproducerea acestuia;

*Utilizator* - persoana care acţionează sub autoritatea deţinătorului de date cu caracter personal, cu drept recunoscut de acces la sistemele informaţionale de date cu caracter personal;

*Prelucrarea datelor cu caracter personal* - orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminare sau punere la dispoziție în orice alt mod în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;

*Restricționarea prelucrării* - reprezintă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;

*Sistent de evidență a datelor cu caracter personal* - orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie că este centralizată, descentralizată ori repartizată după criterii funcționale sau geografice;

*Consimțământ* - manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a subiectului de date prin care acesta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care îl privesc să fie prelucrate;

*Pseudonimizare* - reprezintă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;

*încălcarea securității datelor cu caracter personal* - reprezintă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea;

*Destinatar* - reprezintă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Cu toate acestea, autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu actele normative nu sunt considerate destinatari; prelucrarea acestor date de către autoritățile publice respective respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării.

### III. OBIECTIVELE POLITICII PRIVIND PROTECȚIA DATELOR

Obiectivele principale ale Politicii sunt disponibilitatea, integritatea și confidențialitatea tuturor informațiilor, inclusiv datelor cu caracter personal prelucrate de **PRIMĂRIA SATULUI ROGOJENI** atât în cadrul prelucrării manuale, cât și în cadrul sistemelor și proceselor de tehnologie informațională.

Securitatea informațională reprezintă o componentă esențială a derulării optime a proceselor bazate pe IT în cadrul **PRIMĂRIEI SATULUI ROGOJENI**. Baza unei securități IT adecvate o constituie respectarea prezentei Politici și a altor acte normative interne în acest sens. Aceasta cuprinde cerințe și reguli pentru protecția tuturor informațiilor, inclusiv datele cu caracter personal, sistemelor și proceselor IT împotriva influențelor naturale, erorilor umane și tehnice, precum și împotriva acțiunilor deliberate care pot provoca pagube materiale, respectiv imateriale, sau care pot duce la încălcări ale legislației.

Având în vedere că siguranța IT nu poate fi garantată exclusiv cu ajutorul unor sisteme tehnice, prezenta Politică vizează, de asemenea, aspecte de ordin organizatorico- juridic și de altă natură.

**PRIMĂRIA SATULUI ROGOJENI** va proteja datele cu caracter personal atât a cetățenilor/petiționarilor, a angajaților săi, cât și a altor persoane vizate.

Reglementările prezentei Politici reprezintă un standard minim pentru **PRIMĂRIA SATULUI ROGOJENI**, inclusiv și pentru toți angajații Societății. Pornind de la această reglementare, toți

angajații **PRIMĂRIEI SATULUI ROGOJENI** urmează să respecte strict prevederile Politicii și regulilor interne ale **entității** privind protecția datelor cu caracter personal și sistemelor IT.

În consecință, prin prezenta Politică se stabilesc acțiuni și măsuri pentru implementarea și respectarea de către **PRIMĂRIA SATULUI ROGOJENI** a prevederilor legale în vigoare privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și pentru:

*J* prelucrarea datelor cu caracter personal conform dispozițiilor legale;

*J* respectarea drepturilor persoanelor vizate;

■ *S* evidența operațiunilor de prelucrare a datelor cu caracter personal în conformitate cu termenii legali; adoptarea măsurilor necesare pentru a se evita încălcarea securității datelor cu caracter personal;

*J* asigurarea condițiilor necesare accesării și utilizării datelor cu caracter personal, exclusiv de către persoanele autorizate (angajații), potrivit atribuțiilor menționate în Fișa postului.

#### **IV. PRINCIPIILE PRELUCRĂRII DATELOR CU CARACTER PERSONAL**

*J* Legalitate, echitate și transparență: datele sunt prelucrate în mod legal, echitabil și transparent față de persoana vizată;

*J* Limitări legate de scop: datele sunt colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri;

*J* Reducerea la minimum a datelor: datele sunt adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate;

*J* Exactitate: datele sunt exacte și pot fi actualizate;

■ *S* Limitări legate de stocare: datele sunt păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor pentru care au fost colectate;

*J* Integritate și confidențialitate: datele sunt prelucrate într-un mod care asigură securitatea adecvată a acestora. **PRIMĂRIA SATULUI ROGOJENI** este responsabilă de respectarea principiilor enumerate și trebuie să poată demonstra această respectare.

#### **V. DISPOZIȚII PRIVIND IERARHIA ȘI RESPONSABILITATEA PERSOANEI RESPONSABILE DE POLITICA DE SECURITATE**

Organul ierarhic superior al entității - **PRIMĂRIA SATULUI ROGOJENI**, conform competenței:

*J* aprobă politicile, procedurile și alte documente care reglementează prelucrarea datelor cu caracter personal;

Numește prin decizie internă angajații care primesc atribuții de prelucrare a datelor cu caracter personal și dispune măsuri de instruire și responsabilizare a lor în acord cu cerințele specifice din Fișa postului;

*J* dispune măsuri tehnice și organizatorice menite să asigure protejarea intereselor legitime ale angajaților cu privire la confidențialitatea și securitatea datelor cu caracter personal care le aparțin, respectiv prelucrarea acestora cu respectarea prevederilor legale în domeniu în scopuri determinate, explicite și legitime, în baza drepturilor și obligațiilor ce revin operatorului, în calitate de angajator;

■ *S* stabilește proceduri care asigură angajaților accesul, corectarea și actualizarea datelor cu caracter personal, precum și exercitarea drepturilor ce le revin din postura de persoane vizate;

*J* dispune măsuri tehnice și organizatorice eficiente, în acord cu specificul de activitate al operatorului, capabile să implementeze conformitatea cu prevederile legislației aferente în vigoare a activităților de prelucrare a datelor cu caracter personal, respectiv a celor cu caracter special, realizate în cadrul proceselor operaționale și de suport și implementează în acest sens proceduri de lucru și responsabilități clar definite.

#### **Responsabilul IT:**

Stabilește măsuri tehnice în vederea securizării datelor personale;

*J* asigură securizarea tuturor sistemelor, serviciilor și a echipamentelor informatice care sunt folosite pentru stocarea datelor cu caracter personal și care aparțin entității;

*S* efectuează controale regulate pentru a se asigura că sistemele hardware și software de securitate funcționează corect;

■ *S* furnizează organului de conducere rezultatele oricăror evaluări ale riscurilor IT, pentru a controla riscul dezvăluirii neautorizate, utilizării necorespunzătoare, modificării sau distrugerii datelor cu caracter personal conținute în sistemele IT, aplicații și bazele de date ale operatorului.

#### **Angajații și prestatorii de servicii:**

Toți angajații și prestatorii de servicii ai entității vor opera datele cu caracter personal în conformitate cu termenii menționați în Politică și în cele ce urmează:

*J* datele cu caracter personal sunt prelucrate conform legilor și reglementărilor aplicabile privind confidențialitatea și protecția datelor;

■ *S* datele cu caracter personal sunt tratate cu strictă confidențialitate și sunt stabilite măsuri pentru a le asigura integritatea și securitatea. În general, datele cu caracter personal pot fi divulgate doar în conformitate cu un contract de prestări servicii, o autorizație din partea conducerii sau în mod permis sau cerut de lege;

datele cu caracter personal sunt accesate, utilizate și dezvăluite de către angajați și de prestatorii de servicii, numai pe baza „necesității de a cunoaște”, cu aprobările corespunzătoare ale organului de conducere și doar după ce se li se va asigura o protecție adecvată.

Conform celor menționate anterior, angajații și prestatorii de servicii se obligă și se asigură că:

*J* prelucrează date cu caracter personal doar dacă aceste atribuții sunt înscrise în Fișa postului /obligațiilor contractuale și doar potrivit instrucțiunilor în vigoare aplicabile, stabilite la nivelul entității, respectiv în scopurile și folosind mijloacele comunicate/puse la dispoziția acestora de către entitate;

*J* respectă politicile, regulile, regulamentele, deciziile și orice alte documente și instrucțiuni din partea operatorului aflate în legătură cu aplicarea legislației aferente, respectiv prelucrarea datelor cu caracter personal, inclusiv prevederile prezentei Politici, măsurile tehnice, organizatorice și de securitate implementate și/sau stabilite de către operator în legătură cu prelucrarea datelor cu caracter personal, din momentul înștiințării lor prin orice mijloc de comunicare ales (afișare, luarea la cunoștință pe bază de semnătură, e-mail etc.);

*J* respectă caracterul confidențial și măsurile tehnice, organizatorice și de securitate impuse la nivelul entității cu privire la și în sensul protejării datelor cu caracter personal și protecției drepturilor și libertăților persoanelor vizate; nu vor copia, dezvălui și/sau transmite, total sau parțial, datele cu caracter personal nici unei persoane, în niciun mod, și nici nu vor utiliza astfel de informații pentru sine sau pentru interesele altor persoane, în afara instrucțiunilor primite de la operator;

*J* colectează, actualizează, revizuiesc datele cu caracter personal operate, le arhivează, le șterg ori le prelucrează de orice manieră exclusiv în baza politicilor stabilite la nivelul entității;

*J* notifică toți terții cu care intră în contact în timpul exercitării atribuțiilor de serviciu, atât celor cu care colaborează în prezent, cât și celor care vor fi contactați în viitor, informându-i că

datele cu caracter personal le sunt prelucrate, scopul și durata prelucrării, precum și referitor la drepturile acestora - cum vor folosi formele de notificare puse la dispoziție de către operator;

*J* solicită consimțământul terților, atât celor cu care colaborează în prezent, cât și celor ce vor fi contactați în viitor, exprimat într-o formă concretă (e-mail, notificare scrisă, sms), în vederea prelucrării datelor cu caracter personal în măsura în care se află într-o situație pentru care legile privind protecția datelor impun acordarea consimțământului;

Interzic accesul neautorizat la date cu caracter personal;  
informează organul de conducere despre situațiile în care are loc o încălcare a securității datelor cu caracter personal sau au o suspiciune că o astfel de încălcare a avut loc, sub orice formă (cum ar fi distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod, în mod accidental sau ilegal), în termen de cel mult 24 de ore de la data la care au luat la cunoștință de aceasta;

Cel mai târziu la data încetării contractului individual de muncă/contractului de prestări servicii vor preda operatorului bunurile utilizate în desfășurarea activității care conțin date cu caracter personal, indiferent de modul în care au intrat în posesia acestora. Semnarea de către ambele părți a fișei de lichidare nu instituie o prezumție absolută în sensul îndeplinirii acestei obligații de către salariat/prestator;

*J* respectă caracterul confidențial al măsurilor tehnice, organizatorice și de securitate stabilite și/sau implementate la nivelul entității în scopul protejării datelor cu caracter personal prelucrate, pe întreaga durată a Contractului individual de muncă/prestări servicii și după încetarea acestuia;

*J* respectă măsurile tehnice și organizatorice corespunzătoare pentru a proteja datele cu caracter personal împotriva pierderii, utilizării în mod abuziv sau accesării fără autorizare, dezvăluirii în mod incorect, modificării sau distrugerii și alte forme ilegale de prelucrare, astfel cum acestea sunt comunicate;

/ atunci când se colectează date cu caracter personal, se asigură că operatorul are dreptul de a colecta aceste date și că persoanele de la care sunt colectate au primit o notificare necesară în mod legal și au fost informate cu privire la drepturile lor;

*J* colectează doar acele date cu caracter personal necesare pentru realizarea de către entitate a activităților specifice;

*J* nu utilizează date cu caracter personal în alte scopuri, decât pentru activitatea desfășurată de către operator;

*J* folosesc date cu caracter personal doar pentru scopurile pentru care au fost colectate.

Operatorul de date cu caracter personal reieșind din specificul activității, prin prezenta Politică, transpune procedurile și măsurile necesare în vederea asigurării nivelului adecvat de protecție la prelucrarea datelor cu caracter personal în cadrul sistemelor de evidență gestionate.

Politica se va revizui cel puțin o dată în an ca rezultat al modificărilor sau reevaluării competențelor entității, fiind pusă în sarcina conducătorilor, de a desemna persoana/ele care vor purcede nemijlocit la ajustarea prevederilor prezentului act.

Politica, în mod obligatoriu va fi adusă la cunoștință, sub semnătură, tuturor angajaților /prestatorilor de servicii responsabili de prelucrarea datelor cu caracter personal, înaintea acordării accesului la prelucrarea datelor cu caracter personal, inclusiv și la operarea modificărilor odată cu necesitatea asigurării nivelului adecvat de protecție a datelor cu caracter personal.

Responsabil de implementarea și monitorizarea respectării prevederilor politici, va fi desemnată persoana care conform fișei postului și/sau ordinului intern, va dispune de resurse suficiente (timp, resurse umane, echipament și buget) și va avea acces liber la informația necesară pentru îndeplinirea funcțiilor sale în măsura în care aceasta nu operează în afara cadrului acestei politici.

Persoana responsabilă desemnată, indiferent de funcțiile exercitate, în cadrul monitorizării implementării/respectării prevederilor politicii, se va subordona nemijlocit conducătorului **PRIMĂRIEI SATULUI ROGOJENI** sau persoanei care îndeplinește interimatul funcției.

Persoana responsabilă de prezenta politică asigură definirea clară a diferitelor responsabilități cu privire la securitatea prelucrării datelor cu caracter personal (prevenire, supraveghere, detectare și prelucrare), precum și operarea cu ele, în afara presiunilor ca rezultat al intereselor personale sau alte împrejurări.

Persoana responsabilă de prezenta politică va defini clar responsabilitățile și procesele de management al securității datelor cu caracter personal, cu integrarea lor corespunzătoare în structura

organizațională și de funcționare generală, va asigura măsuri tehnice și organizaționale necesare organizării procesului de management al securității datelor cu caracter personal, va elabora procedurile de clasificare a informației care conține date cu caracter personal astfel încât să fie posibil de întocmit un nomenclator și toate datele cu caracter personal care sînt prelucrate să fie localizate, indiferent de tipul purtătorului de date, va instrui persoanele implicate în procesul de prelucrare a datelor cu caracter personal în vederea îndeplinirii de către acestea a atribuțiilor funcționale și asumării responsabilităților de securitate a datelor cu caracter personal, inclusiv asupra confidențialității acestora.

## **VI. REGULI „CLEAN DESK”**

Pentru a îmbunătăți securitatea și confidențialitatea informațiilor **PRIMĂRIEI SATULUI ROGOJENI** a adoptat reguli „Clean Desk” pentru stațiile de lucru pentru computere și imprimante.

Acest lucru asigură că toate informațiile sensibile și confidențiale, fie că sunt pe suport hârtie, pe un dispozitiv de stocare sau pe un dispozitiv hardware, sunt blocate sau eliminate în mod corespunzător când o stație de lucru nu este utilizată.

Aceste reguli vor reduce riscul accesului neautorizat, pierderii și deteriorării informațiilor în timpul și în afara orelor normale de funcționare sau atunci când stațiile de lucru sunt lăsate nesupravegheate. Regulile reprezintă un control important al securității și confidențialității și sunt necesare pentru respectarea legislației cu privire la protecția datelor.

Aceste reguli se aplică tuturor angajaților **PRIMĂRIEI SATULUI ROGOJENI** care activează atât pe perioadă determinată, cât și nedeterminată sau prin cumul, precum și prestatorilor de servicii.

### **REGULI!**

Ori de câte ori un birou nu este ocupat pentru o perioadă lungă de timp, se vor aplica următoarele reguli: Toate documentele sensibile și confidențiale trebuie să fie scoase de pe birou și blocate într-un sertar sau dulap de depozitare. Acestea includ dispozitive de stocare în masă, cum ar fi CD-uri, DVD-uri și unități USB.

Toată hârtia de deșeu care conține informații sensibile sau confidențiale trebuie plasate în cutiile confidențiale dedicate.

Stațiile de lucru pentru calculatoare trebuie să fie blocate atunci când biroul este neocupat și închis complet la sfârșitul zilei de lucru.

## **VII.SFERA DATELOR PERSONALE. PRELUCRAREA DATELOR CU CARACTER PERSONAL, SCOPURILE ȘI TEMEIURILE PRELUCRĂRII**

Activitățile de prelucrare a datelor cu caracter personal realizate la nivelul **PRIMĂRIEI SATULUI ROGOJENI** pot consta în: colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea.

În cazurile în care **PRIMĂRIA SATULUI ROGOJENI** stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal va avea calitatea de Operator. În situațiile în care **PRIMĂRIA SATULUI ROGOJENI** împreună cu unul sau mai mulți operatori stabilesc în comun scopurile și mijloacele de prelucrare, aceștia vor avea calitatea de Operatori Asociați. Atunci când **PRIMĂRIA SATULUI ROGOJENI** nu stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal va avea calitatea de Persoană împuternicită și va prelucra datele conform instrucțiunilor definite de Operator.

**La nivelul PRIMĂRIEI SATULUI ROGOJENI sunt prelucrate următoarele categorii de date aparținând angajaților proprii, precum și candidaților la angajare, și anume:**

*A numele, prenumele;*

*A sexul;*

*A data și locul nașterii;*

*A cetățenia;*

*A IDNP;*

*A imagine;*

*A situația familială;*

*A situația militară;*

*A datele personale ale membrilor de familie;*

*A datele din permisul de conducere;*

*A datele pentru transferul pe contul bancar a plăților salariate și a altor sume datorate cu titlu de indemnizații, compensații sau alte beneficii, după caz;*

*A semnătura;*

*A datele din actele de stare civilă;*

*A numărul dosarului de pensie;*  
*A codul personal de asigurării sociale (CPAS);*  
*A codul asigurării medicale (CPAM);*  
*A numărul de telefon/fax;*  
*A numărul de telefon mobil;*  
*A adresa (domiciliului/reședinței);*  
*A adresa e-mail;*  
*A profesia și/sau locul de muncă;*  
*A formarea profesională - diplome - studii;*  
*A numele, prenumele (după caz, patronimicul) persoanelor care se află la întreținerea persoanei respective (membrii familiei, alte rude și persoane, după caz);*  
*A mărimea concretă a drepturilor salariale calculate, taxele și impozitele aferente, inclusiv contribuțiile de asigurări sociale obligatorii de asistență medicală și socială, și alte sume datorate în virtutea legii sau contractului;*  
*A datele din certificatele de concediu medical acordate, necesare pentru calcularea indemnizației corespunzătoare;*  
*A informații de recrutare (inclusiv copii ale diplomelor de studii, referințe și alte informații incluse într-un CV sau scrisoare de intenție ca parte a procesului de aplicare);*  
*A informații despre utilizarea de către angajat a sistemelor noastre de informare și comunicații;*  
*A după caz, alte date necesare îndeplinirii scopului menționat, conform legislației în vigoare.*

**La nivelul PRIMĂRIEI SATULUI ROGOJENI sunt prelucrate următoarele categorii de date aparținând cetățenilor/petiționarilor:**

*A numele, prenumele, patronimicul;*  
*A telefon mobil;*  
*A e-mail;*  
*A semnătura digitală;*  
*A telefon/fax;*  
*A adresa (domiciliului/reședinței);*  
*A alte date relevante în procesul de examinare a corespondenței, în dependență de solicitarea persoanei vizate.*

**La nivelul PRIMĂRIEI SATULUI ROGOJENI sunt prelucrate următoarele categorii de date aparținând cetățenilor/petiționarilor și alor persoane vizate prin intermediul înregistrării și difuzării audio-video a ședințelor Consiliului sătesc:**

*J imaginea persoanelor vizate;*  
*•J vocea persoanelor care vor lua cuvântul;*  
*J numele și prenumele persoanelor care vor lua cuvântul sau altor persoane vizate;*  
*A funcția deținută de persoanele care vor lua cuvântul.*

**La nivelul PRIMĂRIEI SATULUI ROGOJENI sunt prelucrate următoarele categorii de date aparținând partenerilor contractuali (persoane fizice) și reprezentanților partenerilor comerciali (persoane juridice) și anume:**

*A date de identificare: nume, prenume;*  
*A date de contact: adresă de domiciliu, număr de telefon, adresă de e-mail;*  
*J seria și numărul buletinului de identitate, IDNP;*  
*•A alte date cu caracter personal: semnătura, funcția.*

Colectarea datelor cu caracter personal. Informarea persoanelor vizate.

Acordarea Consimțământului privind prelucrarea datelor.

În momentul colectării de date de la persoane fizice, acestea trebuie informate, în scris sau oral, într-un mod inteligibil cu privire la:

*A cine este operatorul;*  
*A în ce scopuri va folosi operatorul datele cu caracter personal ale acestora;*  
*A categoriile de date cu caracter personal în cauză;*  
*A justificarea legală a prelucrării datelor;*  
*A perioada stocării datelor;*

*A destinarii datelor cu caracter personal;*

*A dacă datele cu caracter personal ale acestor persoane vor fi transferate transfrontalier;*

*A accesul la o copie a datelor (dreptul de a accesa datele cu caracter personal) și alte drepturi de bază în domeniul protecției datelor;*

*A dreptul de a depune o plângere către Autoritatea de Supraveghere a Prelucrării Datelor cu Caracter Personal (CNPDCP);*

*A dreptul de a-și retrage consimțământul în orice moment;*

*A eventuala existență a unui proces decizional automatizat și logica utilizată, inclusiv consecințele acestui fapt.*

Aceste informații sunt prezentate în scris sau oral persoanelor vizate sau prin alte mijloace, dacă a fost posibilă identificarea acestora, utilizând un limbaj clar și inteligibil.

**PRIMĂRIA SATULUI ROGOJENI** are obligația de a aduce la cunoștință persoanei vizate categoriile de date și sursa din care a obținut datele, inclusiv în situația în care acestea provin din surse disponibile public.

**PRIMĂRIA SATULUI ROGOJENI** realizează distincția dintre obligația de informare și obligația de a obține consimțământul persoanei vizate, acesta din urmă aplicându-se doar în cazuri limitativ prevăzute de legislația în vigoare și dacă prelucrarea nu se încadrează în situațiile de excepție care permit prelucrarea în baza unor temeuri legale.

Consimțământul se definește ca fiind o manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, prin intermediul unei declarații, ca datele cu caracter personal care o privesc să fie prelucrate.

Rolul obținerii consimțământului este de a asigura transparența și de a spori încrederea persoanelor vizate, oferind totodată acestora posibilitatea de a alege în mod liber și de a deține controlul asupra datelor cu caracter personal prelucrate.

### **Scopurile în care sunt prelucrate datele cu caracter personal**

La nivelul **PRIMĂRIEI SATULUI ROGOJENI** realizate prelucrări de date cu caracter personal în numeroase scopuri, iar modalitățile de colectare, baza legală de prelucrare, utilizarea, dezvăluirea, perioadele de păstrare etc., pot să difere în funcție de fiecare scop.

**PRIMĂRIA SATULUI ROGOJENI** prelucrează datele personale ale **propriilor angajați precum și candidaților la angajare** în următoarele scopuri cu caracter general:

*Managementul resurselor umane cadrul procesului de recrutare.*

*Managementul administrativ al resurselor umane.*

Scopurile specifice de prelucrare a datelor cu caracter personal ale propriilor angajați precum și candidaților la angajare, sunt prevăzute de **Politica de Confidențialitate privind prelucrarea datelor personale ale angajaților și potențialilor angajați** aprobată la nivelul entității.

**PRIMĂRIA SATULUI ROGOJENI** prelucrează datele cu caracter personal ale

cetățenilor/petiționarilor în scopul acordării serviciilor publice solicitate.

**PRIMĂRIA SATULUI ROGOJENI** prelucrează datele cu caracter personal ale

cetățenilor/petiționarilor prin difuzarea în direct pe pagina de Facebook și/sau pe alte rețele sau platforme de socializare, precum și publicarea pe pagina web a primăriei satului a ședințelor Consiliului Local, urmărind scopul de:

*J transparentizare a proceselor/deciziilor din administrația locală;*

*J informare eficientă a cetățenilor orașului;*

*J creștere a gradului de implicare a cetățenilor în problemele orașului;*

*J creștere a nivelului de încredere în administrația publică locală.*

**PRIMĂRIA SATULUI ROGOJENI** prelucrează datele cu caracter personal ale cetățenilor/petiționarilor prin înregistrarea audio-video a ședințelor Consiliului sătesc, urmărind scopul de a contribui la redactarea proceselor-verbale ale ședințelor, în sensul consemnării întocmai, în cuprinsul acestora, a tuturor problemelor dezbătute/opiniilor exprimate în cadrul ședinței.

### **Temeiul juridic și condițiile de legalitate pe care se bazează prelucrările de date**

Prelucrarea datelor cu caracter personal în cadrul **PRIMĂRIEI SATULUI ROGOJENI** se realizează respectând cel puțin una dintre următoarele condiții de legalitate:

*prelucrarea se efectuează având consimțământul persoanei vizate;*

*J prelucrarea este necesară pentru a încheia un raport juridic/contract sau pentru executarea acestuia;*

*J prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;*

*J prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță;*

*J executarea sarcinilor de interes public sau care rezultă din exercitarea prerogativelor de autoritate publică cu care este investit operatorul sau terțul căruia îi sânt dezvăluite datele cu caracter personal.*

### **VIII. DEZVĂLUIREA DATELOR CU CARACTER PERSONAL**

Angajații **PRIMĂRIEI SATULUI ROGOJENI**, prestatorii de servicii, vor putea transfera datele cu caracter personal ale persoanelor vizate numai în condițiile respectării cerințelor prevăzute de legislația în vigoare și în conformitate cu politicile și procedurile **PRIMĂRIEI SATULUI ROGOJENI**.

Datele cu caracter personal sunt destinate utilizării de către PRIMĂRIA SATULUI GROZEȘTI, dar pot fi transferate către:

■ *J parteneri contractuali;*

• *S subcontractanți;*

*J procesatori de plăți;*

*J companii ce oferă servicii IT;*

*J companii de audit;*

*J avocați, notari, executori judecătorești;*

*deținători de registre publice și/sau private;*

*autorități publice, cum ar fi, dar a nu se limita la: ASP; CNAM, CNAS, SFS, instanțe de judecată sau arbitrate, precum și autorități competente să cerceteze săvârșirea de fapte penale.*

### **Vom mai putea dezvălui datele tale personale unor terți în următoarele situații:**

• *A în cazul în care ne solicitați personal această dezvăluire sau ne dați acordul în acest sens;*

*J persoanelor care pot demonstra că dețin autoritatea legală de a acționa în numele dvs.;*

■ *A în cazul în care avem obligația de a dezvălui datele tale personale pentru a respecta o obligație legală sau o solicitare din partea autorităților;*

■ *A pentru a răspunde oricăror acțiuni juridice, pentru a proteja drepturile noastre sau ale unui terț, pentru siguranța oricărei persoane sau pentru a preveni orice fel de activitate nelegală;*

Punerea la dispoziție a datelor cu caracter personal în interiorul entității:

În derularea activității **PRIMĂRIEI SATULUI ROGOJENI**, datele cu caracter personal ale unor persoane vizate trebuie să fie prelucrate de către mai multe subdiviziuni/departamente. Procesele interne al entității sunt concepute pentru a respecta cerințele de protecție a datelor cu caracter personal, inclusiv reducerea la minim a datelor cu caracter personal folosite de diferite subdiviziuni/departamente din cadrul entității în activitățile lor.

Colectarea și prelucrarea de către o/un subdiviziune/departament specific, de alte date decât cele prevăzute de aceste procese și modele interne pot fi efectuate numai cu aprobarea corespunzătoare a Primarului.

Transferurile de date cu caracter personal către prestatorii de servicii:

Pentru a-și îndeplini activitatea, în anumite situații **PRIMĂRIA SATULUI ROGOJENI** va pune la dispoziția prestatorilor săi de servicii, datele cu caracter personal ale persoanelor vizate. Aceste

transferuri trebuie să fie efectuate întotdeauna potrivit prevederilor contractuale dintre prestatorii de servicii și **PRIMĂRIA SATULUI ROGOJENI**.

Transferurile de date cu caracter personal către Terți.

Transferul de date cu caracter personal către terți care nu sunt prestatori de servicii și cu care în general **PRIMĂRIA SATULUI ROGOJENI** nu are încheiat un contract, va putea fi efectuat în baza unor obligații legale sau pe baza interesului său legitim. De ex. conceptul de ”Terți” poate include autoritățile publice, inclusiv fiscale, instanțele de judecată, executori judecătorești, etc.

**Datele cu caracter personal sunt prelucrate numai pe teritoriul Republicii Moldova și nu sunt fi transferate în altă țară.**

## **IX. TERMENUL DE PRELUCRARE A DATELOR CU CARACTER PERSONAL**

**1. PRIMĂRIA SATULUI ROGOJENI** reține datele personale ale **angajaților** doar în măsura în care este necesar pentru îndeplinirea scopurilor pentru care le-a colectat sau pentru care au fost comunicate, în consecință, în general, datele se vor păstra cel puțin pe durata angajării.

La expirarea termenului menționat datele sunt păstrate în formă arhivată pe perioada stabilită de Indicatorul documentelor-tip și al termenelor lor de păstrare pentru organele administrației publice,

pentru instituțiile, organizațiile și întreprinderile Republicii Moldova, aprobat de Serviciul de Stat de Arhivă nr.57 din 27.07.2016).

Cu referire la termenul de păstrare a datele personale colectate în procesul de recrutare:

■ *J* Datele sunt păstrate atât timp cât este necesar pentru finalizarea cu succes a procesului de recrutare.

*J* Datele referitoare la candidații selectați vor fi incluse în dosarul personal al acestora și vor fi păstrate pe perioada activității în cadrul **PRIMĂRIEI SATULUI ROGOJENI**, iar după încetarea raporturilor de muncă, se vor păstra în formă arhivată, pe perioada stabilită de Indicatorul documentelor-tip și al termenelor lor de păstrare pentru organele administrației publice, pentru instituțiile, organizațiile și întreprinderile Republicii Moldova, aprobat de Serviciul de Stat de Arhivă nr.57 din 27.07.2016).

*J* în cazul în care CV-ul nu a fost selectat pentru ca candidatul să poată participa la proba interviului sau în urma interviului nu a fost selectat pentru angajare, datele vor fi păstrate timp de 3 luni de la încheierea procesului de recrutare pentru a putea oferi, la necesitate, explicații candidaților cu privire la motivele pentru care candidatura a fost respinsă.

De asemenea, având în vedere interesul nostru legitim de a optimiza selecția celor mai potriviți candidați pentru posturile disponibile și pentru a informa candidații despre alte campanii de recrutare pentru posturi disponibile în cadrul **PRIMĂRIEI SATULUI ROGOJENI**, vom păstra CV-ul. **în acest caz, stocăm datele personale o perioadă de maxim 2 ani** (*perioadă care este proporțională și rezonabilă, pe termen scurt și mediu, cu scopul unei persoane de a găsi și de a ocupa un loc de muncă adecvat pregătirii sale*). Însă, în cazul în care persoana vizată nu dorește ca **PRIMĂRIA SATULUI ROGOJENI** să păstreze CV-ul în acest scop, ea are dreptul de a se opune unei astfel de prelucrări și de a solicita ștergerea datelor.

Datele referitoare la candidați pot fi păstrate într-o arhivă intermediară în scopuri probatorii, în special pentru a se proteja împotriva unor eventuale reclamații pentru discriminare, pentru o perioadă nu mai mare de 5 ani de la încheierea procesului de recrutare.

**PRIMĂRIA SATULUI ROGOJENI** păstrează datele cu caracter personal ale **cetățenilor/petiționarilor**, pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor pentru care au fost colectate, după care, se arhivează dacă legislația în vigoare nu prevede altfel.

**PRIMĂRIA SATULUI ROGOJENI** păstrează **datele obținute în rezultatul înregistrării audiovideo a ședințelor consiliului local**, până la data aprobării, de către consilierii locali, a procesului verbal aferent ședinței înregistrate.

Prin aprobarea procesului verbal al ședinței de consiliu local, consilierii locali confirmă faptul că în cuprinsul acestui proces se regăsește integral conținutul înregistrării audio al ședinței aferente.

**Difuzările audio-video ale ședințelor Consiliului Local nu se păstrează pe rețelele de socializare mai mult decât 1 zile calendaristice.**

## **X. MIJLOACE SUPUSE PRINCIPIILOR DE PROTECȚIE A DATELOR CU CARACTER PERSONAL**

Protecția datelor cu caracter personal în cadrul **PRIMĂRIEI SATULUI ROGOJENI** (în calitate de operator de date cu caracter personal) este asigurată printr-un complex de măsuri tehnice și organizatorice de preîntâmpinare a prelucrării ilicite a datelor cu caracter personal.

Sânt supuse protecției prin mijloace/procedee specifice, toate resursele informaționale ale operatorului de date cu caracter personal gestionate, care conțin date cu caracter personal, păstrate pe:

- suporturi magnetice, optice, laser sau alte suporturi ale informației electronice, masive informaționale și baze de date;
- sistemele informaționale, rețelele, sistemele operaționale, sistemele de gestionare a bazelor de date și alte aplicații, sistemele de telecomunicații, inclusiv mijloacele de confecționare și multiplicare a documentelor și alte mijloace tehnice de prelucrare a informației.

suporturi de hârtie.

## **XI. MĂSURILE DE PROTECȚIE A DATELOR CU CARACTER PERSONAL**

Măsurile de protecție a datelor cu caracter personal sunt asigurate în scopul:

*J* preîntâmpinării scurgerii informației care conține date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;

preîntâmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în rețelele telecomunicaționale și resursele informaționale;

*J* neadmiterea dezvăluirii terților a informației cu accesibilitate limitată;

■ *S* eficientizarea resurselor informaționale atât pe suport de hârtie cât și cel în format electronic.

## **XII. METODE DE PROTECȚIE A DATELOR CU CARACTER PERSONAL PRELUCRATE ÎN SISTEMELE INFORMAȚIONALE**

Protecția datelor cu caracter personal prelucrate în sistemele informaționale se efectuează prin următoarele metode:

*J* preîntâmpinarea conexiunilor neautorizate la rețelele telecomunicaționale și interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste rețele;

*J* excluderea accesului neautorizat la datele cu caracter personal prelucrate;

• *S* preîntâmpinarea acțiunilor speciale tehnice și de program, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program;

• *S* preîntâmpinarea acțiunilor intenționate și/sau neintenționate a utilizatorilor interni și/sau externi, precum și a altor membri ai operatorului/persoanelor împuternicite de către operator, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program, pe suport de hârtie;

*J* preîntâmpinarea scurgerii de informații care conțin date cu caracter personal, transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informații, precum și utilizarea canalelor VPN;

*J* preîntâmpinarea distrugerii, modificării datelor cu caracter personal sau defecțiunilor în funcționarea soft-ului destinat prelucrării datelor cu caracter personal este asigurată prin metoda folosirii mijloacelor de protecție speciale tehnice și de program, inclusiv a programelor licențiate, programelor antivirus, organizării sistemului de control al securității soft-ului și efectuarea periodică a copiilor de siguranță;

*J* preîntâmpinarea scurgerii de informații care conțin date cu caracter personal, este asigurată prin auditul intern al sistemelor informaționale, care se efectuează permanent.

stabilirea exactă a ordinii de acces la informația care conține date cu caracter personal, prelucrate în cadrul sistemelor informaționale și de evidență instituite atât pentru utilizatorii interni cât și pentru cei externi;

*J* instruirea angajaților și sensibilizarea acestora față de importanța protecției datelor cu caracter personal.

## **XIII. PROCEDURI ORGANIZATORICE ȘI TEHNICE**

Procedurile organizatorice și tehnice care urmează a fi respectate în cadrul **PRIMĂRIEI SATULUI ROGOJENI** la prelucrarea datelor cu caracter personal sunt de ordin administrativ și tehnologic precum este menționat mai jos:

Măsurile generale de administrare a securității informaționale în cazul neutilizării temporare a purtătorilor de informație pe suport de hârtie sau electronici (digitali) care conțin date cu caracter personal, aceștia se păstrează în safeuri sau dulapuri metalice care se încuie.

Computerele, terminalele de acces și imprimantele sânt deconectate la terminarea sesiunilor de lucru.

Este asigurată securitatea punctelor de primire/expediere a corespondenței, precum și securitatea contra accesului neautorizat la aparatele fax și de copiere.

Este asigurată securitatea și accesul fizic la mijloacele de reprezentare a informației care conține date cu caracter personal, în scopul împiedicării vizualizării acesteia de către persoane neautorizate.

Mijloacele de prelucrare a datelor cu caracter personal, informația care conține date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal sînt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a conducerii.

Toate programele utilizate în cadrul sistemului informatic respectă condițiile de licențiere.

Este interzisă instalarea programelor de tip Shareware sau freeware, fără aprobarea administratorului sistemului informatic.

Securitatea mediului fizic și a tehnologiilor informaționale folosite în procesul prelucrării datelor cu caracter personal.

Accesul în sediile/oficiile/birourile ori spațiile unde sînt amplasate sistemele informaționale de date cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară, conform listei sau însemnelor corespunzătoare (insigne, ecusoane, cartele de identificare). Se asigură administrarea și monitorizarea accesului fizic în toate punctele de acces la sistemele informaționale de date cu caracter personal, inclusiv se reacționează la încălcarea regimului de acces.

Perimetrul de securitate a **PRIMĂRIEI SATULUI ROGOJENI** reprezintă perimetrul sediului în care se prelucrează/stochează date cu caracter personal.

Perimetrul clădirii sau încăperilor în care sînt amplasate mijloacele de prelucrare a datelor cu caracter personal este integru din punct de vedere fizic, pereții exteriori ai încăperilor sînt rezistenți, intrările sunt echipate cu lacăte și semnalizare.

Amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespund necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.

Ușile și ferestrele se încuie în cazul în care în încăpere lipsesc membrii.

Computerele, serverele, alte terminale de acces sunt amplasate în locuri cu acces limitat pentru persoane străine.

Accesul în perimetrul de securitate a clădirii **PRIMĂRIEI SATULUI ROGOJENI** unde se prelucrează/stochează date cu caracter personal cu utilaje foto/video neautorizate este interzis, ținînd cont de necesitatea asigurării regimului de confidențialitate și securitate a prelucrării datelor cu caracter personal, prevăzut de prevederile Legii privind protecția datelor cu caracter personal nr.133 din 08.07.2011.

Identificarea și autentificarea utilizatorilor.

Este efectuată identificarea și autentificarea utilizatorilor sistemelor informaționale de date cu caracter personal și a proceselor executate în numele acestor utilizatori.

Toți utilizatorii (inclusiv personalul care asigură susținerea tehnică, administratorii de rețea, programatorii și administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu conține semnamentele nivelului de accesibilitate al utilizatorului.

Pentru confirmarea ID-ului utilizatorului sînt utilizate parole, mijloace fizice speciale de acces cu memorie (token) sau cartele cu microprocesoare, mijloace biometrice de autentificare, bazate pe caracteristici unice și individuale ale persoanei.

În cazul în care contractul de muncă/raporturile de serviciu ale utilizatorului au fost încetate, suspendate sau modificate și noile sarcini nu necesită accesul la date cu caracter personal ori drepturile de acces ale utilizatorului au fost modificate, ori utilizatorul a abuzat de codurile primite în scopul comiterii unei fapte prejudiciabile, a absentat o perioadă îndelungată, codurile de identificare și autentificare se revocă sau se suspendă de administratorul I.T.

Identificarea și autentificarea echipamentului

Este asigurată posibilitatea identificării și autentificării echipamentului folosit în operațiunile de prelucrare a datelor cu caracter personal, cu menținerea acestor informații pentru o perioadă îndelungată.

Administrarea identificatorilor utilizatorilor

Administrarea identificatorilor utilizatorilor include:

identificarea univocă a fiecărui utilizator,  
verificarea autenticității fiecărui utilizator.

Utilizarea parolilor în procesul asigurării securității informaționale

Sunt respectate regulile de asigurare a securității informaționale în cazul alegerii și folosirii parolilor care includ:

- păstrarea confidențialității parolilor,
- interzicerea înscrierii parolilor pe suport de hîrtie, în cazul în care nu se asigură securitatea păstrării acestuia,
- modificarea parolilor de fiecare dată cînd sînt prezente indiciile eventualei compromiteri a sistemului sau parolei,
- alegerea parolilor calitative cu o mărime de minimum 8 simboluri, care nu sînt legate de informația cu caracter personal a utilizatorului, nu conțin simboluri identice consecutive și nu sînt compuse integral din grupuri de cifre sau litere,
- modificarea parolilor peste intervale de 3 luni,
- dezactivarea procesului automatizat de înregistrare (cu folosirea parolilor salvate).

#### **Controlul administrării accesului**

Este efectuat controlul sistematic al acțiunilor utilizatorilor în vederea evaluării corectitudinii și conformării operațiunilor și acțiunilor efectuate prin intermediul sistemelor informaționale de date cu caracter personal.

Limitarea folosirii tehnologiilor fără fir

Accesul fără fir la sistemele informaționale de date cu caracter personal este limitat la maximum, este documentat, supus monitorizării și controlului.

Accesul fără fir la sistemele informaționale de date cu caracter personal este permis doar în cazul utilizării mijloacelor criptografice de protecție a informației.

Folosirea tehnologiilor fără fir se autorizează de persoanele responsabile ale **PRIMĂRIEI SATULUI ROGOJENI**.

#### **Securitatea electroenergetică:**

a) Echipamentul electric utilizat pentru menținerea funcționalității sistemelor informaționale de date cu caracter personal, a cablurilor electrice, este asigurat contra deteriorărilor și conectărilor nesancționate, prin montarea lor în nișe speciale.

b) în cazul apariției situațiilor excepționale, de avarie sau de forță majoră, este asigurată posibilitatea deconectării electricității la sistemele informaționale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component TI.

c) sunt implementate sisteme automatizate de depistare și semnalizare a incendiilor în birourile unde sînt amplasate sistemele informaționale de date cu caracter personal și mijloacele de prelucrare a datelor cu caracter personal.

#### **Controlul instalării și scoaterii componentelor T.L**

Este exercitat controlul și evidența instalării și scoaterii mijloacelor de program, mijloacelor tehnice și celor tehnice de program, utilizate în cadrul sistemelor informaționale de date cu caracter personal.

Informațiile, care conțin date cu caracter personal și care se conțin pe purtătorii de informații, se distrug fizic sau se transcriu și se nimicesc prin metode sigure, evitîndu-se folosirea funcțiilor standarde de nimicire.

**Dezvăluirea datelor cu caracter personal** prin rețele comunicaționale ori pe alt suport digital de stocare.

Dezvăluirea formatului electronic al datelor cu caracter personal conținute în sistemele de evidență, prin rețele comunicaționale ori pe alt suport digital de stocare și păstrare, urmează a fi asigurată criptarea acestei informații sau examinarea posibilității utilizării unei conexiuni bilaterale prin canal securizat VPN. Accesul fără fir la sistemele de evidență a datelor cu caracter personal este permis doar utilizatorilor autorizați. Fiecare caz de solicitare a dezvăluirii prin transmitere a datelor cu caracter personal pe cale electronică va fi examinat separat, reieșind din posibilitățile tehnice asigurate de destinatar și operator, precum și în corespundere cu măsurile organizatorice și tehnice implementate de părți. în cazul în care rețelele comunicaționale prezintă riscuri pentru

confidențialitatea și securitatea datelor cu caracter personal, vor fi utilizate metode tradiționale de transmitere (*expedierepoștală cu aviz recomandat, înmînareapersonală, etc.*).

Dezvăluirea prin transmitere a datelor cu caracter personal prin rețele comunicaționale ce nu corespund Cerințelor, (*spre exemplu: expedierea informației prin intermediul e-mail-urilor personale de tipul @gmail.com, @mail.ru, @yahoo.com, etc.*) sînt interzise.

Sînt interzise operațiunile de dezvăluire a datelor cu caracter personal între **PRIMĂRIA SATULUI ROGOJENI** și alte entități care sunt amplasate geografic în stînga Nistrului care refuză să se supună juridic legislației Republicii Moldova, reieșind din considerentul că la moment nu există posibilitatea exercitării unui control efectiv asupra acestei părți teritoriale, inclusiv în partea ce ține de conformitatea prelucrării datelor cu caracter personal prevederilor *Legii privind protecția datelor cu caracter personal nr.133 din 08.07.2011*.

Procedura dezvăluirii prin transmitere a datelor cu caracter personal stocate pe suport de hîrtie și/sau suport digital, peste hotarele Republicii Moldova, urmează a fi reglementată prin act normativ instituțional/acord bilateral luîndu-se în considerare necesitatea asigurării unui nivel adecvat de protecție a datelor cu caracter personal.

Transmiterea transfrontalieră a datelor cu caracter personal este efectuată în strictă corespundere cu prevederile legislației în vigoare în domeniul protecției datelor cu caracter personal, în special în cazurile cînd tratatul internațional în baza căruia se efectuează transmiterea nu conține garanții privind protecția drepturilor subiectului de date cu caracter personal.

Volumul și categoriile datelor cu caracter personal colectate în scopul ținerii evidenței **PRIMĂRIEI SATULUI ROGOJENI**, este limitat la strictul necesar pentru realizarea scopurilor declarate.

f) Acces la sistemele informaționale gestionate în cadrul **PRIMĂRIEI SATULUI ROGOJENI**, din partea Procuraturii Generale (*după caz procuraturile teritoriale/specializate*), Ministerului Afacerilor Interne, Centrului Național Anticorupție etc., va fi permis doar în cazul în care solicitarea va corespunde prevederilor art. 15 și art. 212 Cod de procedură penală. Se explică că în conformitate cu prevederile art. 157 Cod de procedură penală, documentele în orice formă (*scrisă, audio, video, electronică etc.*) care provin de la persoane oficiale fizice sau juridice dacă în ele sînt expuse ori adeverate circumstanțe care au importanță pentru cauză, (*inclusiv informația stocată în auditul sistemelor informaționale și de evidență*), pot fi solicitate printr-un demers al organului de urmărire penală în cadrul urmăririi penale sau în procesul judecării cauzei. În acest caz, însă, urmează a fi respectate prevederile art.214 Cod de procedură penală, care stipulează că în cursul procesului penal nu pot fi administrate, utilizate și răspîndite fără necesitate informație oficială cu accesibilitate limitată.

Persoanele cărora organul de urmărire penală sau instanța le solicită să comunice sau să prezinte informație oficială cu accesibilitate limitată (*inclusiv operatorii de date cu caracter personal*) au dreptul să se convingă de faptul că aceste date se colectează pentru procesul penal respectiv, iar în caz contrar să refuze de a comunica sau de a prezenta date. Persoanele cărora organul de urmărire penală sau instanța le solicită să comunice sau să prezinte informație oficială cu accesibilitate limitată au dreptul să primească în prealabil de la persoana care solicită informații o explicație în scris care ar confirma necesitatea furnizării datelor menționate.

Urmează a ține cont de faptul că în conformitate cu prevederile art. 8 al Legii privind accesul la informație, datele cu caracter personal fac parte din categoria informației oficiale cu accesibilitate limitată, accesul la care se realizează în conformitate cu prevederile legislației privind protecția datelor cu caracter personal.

#### **XIV. EDUCAȚIA CONTINUĂ CU PRIVIRE LA PROTECȚIA DATELOR CU CARACTER PERSONAL**

Toți angajații entității vor fi instruiți în mod constant cu privire la aspectele legate de prelucrarea datelor cu caracter personal și cu modul în care ar trebui să lucreze cu aceste date.

Partenerii contractuali, prestatorii de servicii, trebuie la rândul lor, să implementeze programe de educație periodică cu privire la aspecte de protecție a datelor cu caracter personal în legătură cu activitatea lor de prelucrare a datelor pentru entitate.

Instruirile se vor efectua de către Responsabilul Pentru protecția Datelor și Managerul IT și vor consta în sesiuni de training care privesc atât aspecte generale de protecție a datelor, cât și aspecte specifice, în funcție de atribuțiile concrete de serviciu ale personalului care prelucrează date personale.

## **XV.EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR CU CARACTER PERSONAL**

În funcție de natura, contextul și scopurile prelucrării datelor, în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc sporit pentru drepturile și libertățile persoanelor, **entitatea**, efectuează, înaintea prelucrării, evaluarea impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal. O evaluare unică poate aborda un set de operațiuni de prelucrare similare care prezintă riscuri sporite similare.

La realizarea evaluării impactului asupra protecției datelor, **entitatea** solicită avizul persoanei responsabile cu protecția datelor.

Evaluarea impactului asupra protecției datelor se impune mai ales în cazul evaluării sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv pe crearea de profiluri, și care stă la baza unor decizii automatizate

care produc efecte juridice privind persoana fizică sau care o afectează, în mod similar, într-o măsură semnificativă.

Evaluarea conține cel puțin:

Descrierea sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării datelor, inclusiv, după caz, a interesului legitim urmărit de **entitate**;  
evaluarea necesității și proporționalității operațiunilor de prelucrare în legătură cu scopurile respective;

evaluarea riscurilor pentru drepturile și libertățile subiecților de date, în special originea (sursa), natura, gradul specific de probabilitate a materializării riscului sporit și gravitatea acestui risc.

Rezultatul evaluării se ia în considerare la stabilirea măsurilor adecvate care trebuie luate pentru a demonstra că prelucrarea datelor cu caracter personal respectă Legea privind protecția datelor cu caracter personal nr.133 din 08.07.2011;

măsurile de prevenire a riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea cu prevederile legale, luând în considerare drepturile și interesele legitime ale subiecților de date și ale altor persoane interesate.

**PRIMĂRIA SATULUI ROGOJENI** va solicita, după caz, avizul în formă scrisă, în formă electronică sau prin utilizarea mijloacelor electronice de comunicație al subiecților de date ori al reprezentanților acestora privind prelucrarea preconizată, fără a aduce atingere protecției intereselor comerciale sau publice ori securității operațiunilor de prelucrare.

Dacă este necesar **PRIMĂRIA SATULUI ROGOJENI** efectuează o analiză pentru a evalua dacă prelucrarea datelor are loc în conformitate cu evaluarea impactului asupra protecției datelor, cel puțin atunci când are loc o modificare a riscului reprezentat de operațiunile de prelucrare.

Lista tipurilor de operațiuni de prelucrare care fac obiectul cerinței de efectuare a unei evaluări a impactului asupra protecției datelor, se stabilește de Centrul Național pentru Protecția Datelor cu Caracter Personal.

**PRIMĂRIA SATULUI ROGOJENI** va consulta Centrul Național pentru Protecția Datelor cu Caracter Personal înainte de prelucrarea datelor dacă evaluarea impactului asupra protecției datelor, indică faptul că prelucrarea ar genera un risc sporit, iar **PRIMĂRIA SATULUI ROGOJENI** consideră că riscul nu poate fi atenuat prin mijloace rezonabile sub aspectul tehnologiilor disponibile și al costurilor implementării.

În cazul în care operatorul consultă Centrul Național pentru Protecția Datelor cu Caracter Personal, va furniza următoarea informație:

- după caz, responsabilitățile corespunzătoare ale operatorului/operatorilor și ale persoanelor împuternicite de operator implicate în activitățile de prelucrare a datelor, în special pentru prelucrarea în cadrul unui grup de întreprinderi;

- scopurile și mijloacele prelucrării preconizate;

măsurile și garanțiile prevăzute pentru protecția drepturilor și libertăților subiecților de date, în conformitate cu prezenta lege;

- după caz, datele de contact ale persoanei responsabile cu protecția datelor;  
evaluarea impactului asupra protecției datelor;

- alte informații relevante și necesare solicitate suplimentar de Centrul Național pentru Protecția Datelor cu Caracter Personal.

### **Prelucrarea prin împuterniciți**

**PRIMĂRIA SATULUI ROGOJENI** va încheia contracte cu Persoane împuternicite care oferă garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să respecte prevederile legale și să asigure protecția drepturilor și libertăților persoanelor vizate. Conținutul respectivelor contracte va face referire la obiectul și durata prelucrării, natura și scopul prelucrării, tipul de date cu caracter personal și categoriile de persoane

vizate, obligațiile și drepturile **PRIMĂRIEI SATULUI ROGOJENI**, în calitate de operator, și ale persoanei împuternicite.

## **XVI. DREPTURILE SUBIECȚILOR DE DATE CU CARACTER PERSONAL**

În situația solicitărilor venite din partea persoanelor vizate în vederea accesării datelor cu caracter personal, rectificării, ștergerii sau portabilității acestora, **PRIMĂRIEI SATULUI ROGOJENI** va verifica mai întâi dacă datele personale menționate aparțin solicitantului.

Dacă o cerere de exercitare a unui drept al persoanei vizate nu poate fi satisfăcută, în acest caz operatorul va furniza persoanei vizate o explicație completă, transmisă în scris, în termen de 30 de zile, menționând motivele refuzului, precum și dreptul persoanei vizate de a depune o plângere la CNPDCP.

Potrivit dispozițiilor legale, persoanele vizate au următoarele drepturi:

**dreptul la informare și acces;**

**dreptul la rectificare;**

**dreptul la opoziție;**

**dreptul de ștergere;**

**dreptul la restricționarea prelucrării;**

**dreptul la portabilitatea datelor.**

**dreptul de a nu fi supus unei decizii individuale.**

**Dreptul de a depune o plângere la operator și la autoritatea competentă privind protecția datelor;**

**Dreptul de a retrage consimțământul.**

## **XVII. STOCAREA, PĂSTRAREA ȘI DISTRUGEREA DATELOR CU CARACTER PERSONAL PRELUCRATE**

Accesul în spațiile/perimetrul unde sînt amplasate sistemele informaționale și de evidență a datelor cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară conform politicii de securitate instituționale /regulamentelor departamentale aprobate.

Stocarea și păstrarea formatului electronic al datelor cu caracter personal, structurate în sisteme de evidență, în computere care sînt conectate la internet, nu sînt echipate cu mijloace de protecție speciale tehnice și de program și nu au instalate programe licențiate, programe antivirus, sisteme de control al securității soft-ului, de asigurare a efectuării periodice a copiilor de siguranță și de efectuare a auditului - este interzisă.

Introducerea în perimetrul de securitate instituțional și utilizarea calculatoarelor personale ori a purtătorilor de informații în scopuri de serviciu este interzisă. Mai mult, accesul la computerele din dotare sunt protejate/restricționate prin crearea profilurilor de utilizatori, iar drepturile de administrator sînt încredințate doar persoanei responsabile pentru implementarea politicii de securitate desemnate din cadrul **PRIMĂRIEI SATULUI ROGOJENI**.

Stocarea datelor cu caracter personal pe suport magnetic, optic, laser, de hîrtie sau alt suport al informației, pe care se creează, se fixează, se transmite, se recepționează, se păstrează sau, în alt mod, se utilizează documentul și care permite reproducerea acestuia, este asigurat prin plasarea acestora în safeuri sau dulapuri metalice care se încuie. Scoaterea, fără autorizare, a purtătorilor de date cu caracter personal din perimetrul de securitate al operatorului este interzisă.

## **XVIII. AUDITUL SISTEMELOR INFORMAȚIONALE GESTIONATE**

Se efectuează înregistrarea tentativelor de intrare/ieșire a utilizatorului în sistem, conform următorilor parametri:

- data și timpul tentativei intrării/ieșirii;
- ID-ul utilizatorului;
- rezultatul tentativei de intrare/ieșire - pozitivă sau negativă.

Se efectuează înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:

- data și timpul tentativei de obținere a accesului (executate a operațiunii),
- denumirea (identificatorul) aplicației sau procesului, o ID-ul utilizatorului,
- specificațiile resursei protejate (identificator, nume logic, nume fișier, număr etc.),
- tipul operațiunii solicitate (citire, înregistrare, ștergere etc.),
- rezultatul tentativei de obținere a accesului (executare a operațiunii) — pozitivă sau negativă.

Este efectuată înregistrarea modificărilor drepturilor de acces (competențelor) utilizatorului și statutului obiectelor de acces, conform următorilor parametri:

- data și timpul modificării competențelor,
- ID-ul administratorului care a efectuat modificările,
- ID-ul utilizatorului și competențele acestuia sau specificarea obiectelor de acces și statutul nou al acestora.

Se efectuează înregistrarea ieșirii din sistem a informației care conține date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecților și statutul obiectelor de acces, conform următorilor parametri:

- data și timpul eliberării,
- denumirea informației și căile de acces la aceasta,
- specificarea echipamentului (dispozitivului) care a eliberat informația (numele logic),
- ID-ul utilizatorului, care a solicitat informația.

#### **XIX.ASIGURAREA PROTECȚIEI CONTRA PROGRAMELOR DĂUNĂTOARE (VIRUȘILOR)**

Este asigurată protecția contra infiltrării programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal, prin existența programelor licențiate anti-virus.

#### **XX. TESTAREA POSIBILITĂȚILOR FUNCȚIONALE DE ASIGURARE A SECURITĂȚII SISTEMELOR INFORMAȚIONALE DE DATE CU CARACTER PERSONAL**

Se asigură testarea funcționării corecte a funcțiilor de securitate a sistemelor informaționale de date cu caracter personal (automat la pornirea sistemului și lunar la solicitarea utilizatorului autorizat în acest scop).

#### **XXI.GESTIONAREA INCIDENTELOR DE SECURITATE**

Orice angajat/prestator de servicii care are cunoștință despre, sau suspectează producerea unui incident de încălcare a securității datelor cu caracter personal, are obligația de a raporta un asemenea incident în cel mai scurt timp posibil către conducerea **PRIMĂRIEI SATULUI ROGOJENI**.

Prelucrarea incidentelor include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor și restabilirea securității.

”În cazul producerii incidentelor de securitate în cadrul **PRIMĂRIEI SATULUI ROGOJENI** persoana responsabilă va 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.

În cadrul controalelor efectuate de Centrul Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova i se va oferi suportul necesar și asigurat accesul la informațiile necesare relevante obiectului controlului.”

## **XXII.MARCAREA DOCUMENTELOR**

Toată informația care se intenționează a fi dezvăluită, și care conține date cu caracter personal, urmează a fi marcată prin:

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

## **XXIII. RESPONSABILITATEA PENTRU ASIGURAREA SECURITĂȚII DATELOR CU CARACTER PERSONAL PRECUM ȘI A INFORMAȚIILOR CU ACCESIBILITATE LIMITATĂ.**

Operatorul de date cu caracter personal, persoana împuternicită de către operator, persoanele terțe după caz, pentru nerespectarea dispozițiilor Politicii de securitate - poartă răspundere civilă (Codul civil), contravențională (art. 74<sup>1</sup> Cod contravențional) și penală (art. art. 177, 178, 180 Cod penal).

## **LISTA ANGAJAȚILOR**

### **FAMILIARIZAȚI CU PREVEDERILE POLITICII**

### **PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL**

### **ÎN CADRUL**

### **PRIMĂRIEI SATULUI ROGOJENI**

<b>Nr.</b>	<b>Numele, prenumele</b>	<b>Funcția</b>	<b>Am luat cunoștință (semnătura)</b>	<b>Data</b>
1.	Groza Ruslan	primar		
2.	Ardeleanu Viorica	secretara consiliului		
3.	Guzun Ana	contabila - șefa		
4.	Odagiu Maria	specialistă		
5.	Iacurinscaia Olga	Muncitoare auxiliară		
6.	Iancu Dumitru	Muncitor auxiliar		
7.	Fosa Svetlana	Muncitoare auxiliară		
8.	Iacurinscaia Olga	Îngrijitoare de încăperi		

**Politica de Confidențialitate privind prelucrarea datelor personale  
ale angajaților  
și potențialilor angajați  
ai Primăriei satului Rogojeni, raionul Șoldănești**

*Dreptul dumneavoastră, în calitate de angajați, la intimitate și viață privată  
reprezintă pentru noi o prioritate și suntem în permanență angajați în  
îmbunătățirea continuă a modului în care protejăm datele dumneavoastră cu  
caracter personal*

INFORMAȚII PRELIMINARE

**PRIMĂRIA SATULUI ROGOJENI**, este conștientă de importanța protecției vieții private și a libertăților individuale și se angajează să asigure protecția acestora în conformitate cu legislația în vigoare cu privire la protecția datelor cu caracter personal.

Scopul acestei Politici de Confidențialitate privind prelucrarea datelor personale ale angajaților și potențialilor angajați (denumită în continuare „**Politică de Confidențialitate**”) este de a vă informa cu privire la prelucrarea datelor cu caracter personal efectuată în contextul *recrutării, angajării, pe perioada executării contractului individual de muncă, precum și după încetarea acestuia* și la drepturile pe care le aveți cu privire la aceste date.

Prezenta politică de confidențialitate se referă la activitățile de prelucrare a datelor cu caracter personal care sunt de natură să conducă la identificarea, în mod direct sau indirect, a unei persoane fizice care participă într-un proces de recrutare - denumită în cele ce urmează „*persoana vizată*”. Prezenta politică de confidențialitate pune în aplicare principiul transparenței și descrie modalitățile prin care se realizează operațiunile de colectare, utilizare, diseminare, stocare și eliminare a datelor dumneavoastră (denumită persoană vizată) cu caracter personal de către **PRIMĂRIA SATULUI ROGOJENI** (denumită în continuare „**Primăria**” sau „**entitatea**”), în calitate de operator de date cu caracter personal.

Această Politică de confidențialitate descrie categoriile de informații care vă privesc, pe care **PRIMĂRIA SATULUI ROGOJENI** le colectează, motivele pentru care aceste informații sunt colectate, principiile de bază pe care ne bazăm tratarea acestora și modul în care **PRIMĂRIA SATULUI ROGOJENI** vă gestionează datele personale, precum și are drept scop de a ne îndeplini obligația legală de a vă informa cu privire la prelucrarea datelor cu caracter personal pe care o desfășurăm în calitate de operator de date.

**PRIMĂRIA SATULUI ROGOJENI** colectează și utilizează datele cu caracter personal pe care le furnizați în timpul procesului de recrutare, precum și alte date cu caracter personal care sunt colectate în timpul angajării și pe perioada executării contractului individual de muncă. Avem nevoie de datele dumneavoastră cu caracter personal pentru a iniția și petrece procesul de recrutare, de a executa și înceta contractul individual de muncă încheiat cu dumneavoastră, precum

și pentru a ne conforma cu obligațiile contractuale și de reglementare aferente acestuia. **Fără aceste date, nu vom putea să vă recrutăm și/sau să vă angajăm, sau să ne conformăm obligațiilor noastre în baza unui astfel de contract.**

Potrivit prezentei Politici de confidențialitate, ne-am stabilit regula respectării obligațiilor prevăzute de legislația în vigoare privind protecția datelor cu caracter personal, dar trebuie să fiți conștienți de faptul că și dvs trebuie să fiți vigilenți cu cine partajați datele personale și cum vă protejați comunicațiile și dispozitivele.

### **DESCRIEREA DATELOR CU CARACTER PERSONAL PE CARE LE PRELUCRĂM, SCOPURILE ȘI TEMEIURILE LEGALE ALE PRELUCRĂRII**

Date cu caracter personal” înseamnă informații referitoare la o persoană fizică identificată sau identificabilă. Datele dumneavoastră de contact și data nașterii sunt, de exemplu, sunt date personale.

**PRIMĂRIA SATULUI ROGOJENI** asigură prelucrarea datelor dumneavoastră cu caracter personal. În acest context, „prelucrare” înseamnă, printre altele, colectarea, utilizarea datelor dumneavoastră personale, dezvăluirea sau distrugerea lor în orice mod.

Categoriile de date cu caracter personal pe care le procesăm variază în funcție de etapă (recrutare/angajare/executare contract/ etc.), în funcție de poziția/funția dvs în cadrul **PRIMĂRIA SATULUI ROGOJENI** și de condițiile de angajare.

### **CE DATE CU CARACTER PERSONAL PUTEM PRELUCRA:**

*numele, prenumele;*

*sexul;*

*data și locul nașterii;*

*cetățenia;*

*IDNP;*

*imagine;*

*situația familială;*

*situația militară;*

*datele personale ale membrilor de familie;*

*datele din permisul de conducere;*

*datele pentru transferul pe contul bancar a plăților salariale și a altor sume datorate cu titlu de indemnizații, compensații sau alte beneficii, după caz;*

*semnătura;*

*datele din actele de stare civilă;*

*numărul dosarului de pensie;*

*codul personal de asigurării sociale (CPAS);*

*codul asigurării medicale (CPAM);*

*numărul de telefon/fax;*

*numărul de telefon mobil;*

*adresa (domiciliului/reședinței);*

*adresa e-mail;*

*•profesia și/sau locul de muncă;*

*•formarea profesională - diplome - studii;*

*numele, prenumele (după caz, patronimicul) persoanelor care se află la întreținerea persoanei respective (membrii familiei, alte rude și persoane, după caz);*

*mărimea concretă a drepturilor salariale calculate, taxele și impozitele aferente, inclusiv contribuțiile de asigurări sociale obligatorii de asistență medicală și socială, și alte sume datorate în virtutea legii sau contractului;*

*datele din certificatele de concediu medical acordate, necesare pentru calcularea indemnizației corespunzătoare;*

*informații de recrutare (inclusiv copii ale diplomelor de studii, referințe și alte informații incluse într-un CV sau scrisoare de intenție ca parte a procesului de aplicare);*

*Informații despre utilizarea de către angajat a sistemelor noastre de informare și comunicații; după caz, alte date necesare îndeplinirii scopului menționat, conform legislației în vigoare.*

## **SURSE DE PROVENIENȚĂ A DATELOR PERSONALE**

**PRIMĂRIA SATULUI ROGOJENI** colectează datele cu caracter personal din următoarele surse:

*direct de la dumneavoastră;*

*de la alți angajați ai noștri cu care ați colaborat, spre exemplu informații privind performanța dvs. la locul de muncă;*

*de la angajații responsabili de domeniul resurse umane, din cadrul departamentului financiar, ale fostului angajator;*

*de la diverși colaboratori sau parteneri contractuali, informații ce reies din interacțiunea dumneavoastră cu aceștia.*

Vă vom ține la curent în momentul colectării datelor, care tip de date trebuie în mod imperativ să ne fie comunicate. Nefurnizarea informațiilor solicitate în mod imperativ ne poate împiedica să finalizăm anumite procese ale resurselor umane. De exemplu, dacă nu ne furnizați anumite informații înseamnă că nu vom putea continua procesul de recrutare sau de angajare, deoarece **PRIMĂRIA SATULUI ROGOJENI** nu va deține datele personale pe care le consideră necesare pentru administrarea și gestionarea eficace a relației noastre cu dumneavoastră.

Pe lângă datele personale care vă privesc, vi se va cere să ne furnizați și date cu caracter personal referitoare la terți, în special persoanele aflate la întreținere sau membrii familiei dumneavoastră, în scopuri de administrare, gestionare a resurselor umane. Înainte de a ne furniza date personale ale terților, trebuie mai întâi să informați acești terți că ne veți furniza aceste date și să îi informați că prelucrarea datelor este efectuată de **PRIMĂRIA SATULUI ROGOJENI**, așa cum este detaliat în prezenta Politică.

### **SCOPURILE PRELUCRĂRII**

Colectăm și prelucrăm datele dumneavoastră cu caracter personal în diverse scopuri, în conformitate cu reglementările legale aplicabile și contractul individual de muncă. Datele cu caracter personal pot fi utilizate ocazional în scopuri care nu vi se par evidente, dar ale căror circumstanțe justifică utilizarea (de exemplu: pentru o investigație internă sau pentru proceduri disciplinare).

În general bazăm prelucrarea datelor dumneavoastră cu caracter personal pe una dintre următoarele baze legale:

**v-ați dat consimțământul pentru unul sau mai multe scopuri specifice;**

**PRIMĂRIA SATULUI ROGOJENI are un interes legitim, cu excepția cazului în care acesta este depășit de interesele dumneavoastră sau de drepturile și libertățile dumneavoastră fundamentale care necesită protecția datelor cu caracter personal;**

**prelucrarea este necesară pentru respectarea unei obligații legale de către PRIMĂRIA SATULUI ROGOJENI;**

prelucrarea este necesară pentru executarea unui contract la care sunteți parte sau pentru îndeplinirea măsurilor precontractuale luate la cererea dumneavoastră.

Ocazional, putem prelucra datele dumneavoastră cu caracter personal în scopul satisfacerii intereselor legitime ale unei terțe părți, cu excepția cazului în care aceste interese prevalează asupra intereselor sau drepturilor și libertăților dumneavoastră fundamentale care necesită protecție. În acest caz, dacă nu este menționat în această Politică, scopul vă va fi comunicat înainte de implementarea prelucrării, într-un mod corespunzător.

**Prelucrăm datele dumneavoastră cu caracter personal pentru a lua decizii privind recrutarea, angajarea, executarea contractului de muncă și pentru a înceta raportul de muncă. Aceste scopuri sunt toate legate de o bază de legalitate a prelucrării, și anume:**

<b>SCOP</b>	<b>TEMEI LEGAL</b>
<b>Recrutare și recomandări</b>	<b>PRIMĂRIA SATULUI ROGOJENI</b> are un interes legitim să efectueze o analiză a cererilor de angajare și să decidă ce măsuri să ia, pentru a se asigura că numai cei mai calificați și relevanți candidați sunt evaluați și selectați. <b>PRIMĂRIA SATULUI ROGOJENI</b> consideră că este în interesul legitim al unui nou angajator să primească confirmarea angajării sau detaliile angajării de la <b>PRIMĂRIA SATULUI ROGOJENI</b> pentru a confirma istoricul profesional al fostului angajat sau istoricul angajării, activitatea profesională.
<b>Managementul resurselor umane cadrul procesului de recrutare și anume:</b> participarea dvs. la prima etapă a procesului de recrutare - analiza CV-ului; contactarea dvs. pentru a fi informat despre rezultatul primei etape de recrutare și, după caz, programarea dvs. la proba interviului; contactarea dvs. pentru a fi informat despre rezultatul probei interviului și după caz, programarea dvs. pentru îndeplinirea formalităților legale privind întocmirea/semnarea Contractului individual de muncă; prelucrarea cererilor de exercitare a drepturilor conform prevederilor Legii privind protecția datelor cu caracter personal, în vigoare; înregistrarea și procesarea sesizărilor și	Pentru procesul de recrutare prelucrăm datele personale în baza Codului Muncii precum și în baza Legii privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date în vigoare, pentru <i>executarea unui contract la care subiectul datelor cu caracter personal este parte sau pentru luarea unor măsuri înaintea încheierii contractului, la cererea acestuia</i> , precum și pentru <i>"îndeplinirea unei obligații care îi revine operatorului conform legii"</i> . Dacă nu ați fost angajat în urma procesului de recrutare, <b>PRIMĂRIA SATULUI ROGOJENI</b> are un interes legitim de a

reclamațiilor dvs; anexarea CV-ului la dosarul personal în cazul în care ați fost selectat pentru postul la care ați candidat; arhivare în condițiile legii.	păstra CV-ul pentru a Vă informa despre alte campanii de recrutare pentru posturi disponibile în cadrul, doar în cazul în care nu vă opuneți acestui fapt.
<b>Managementul administrativ al resurselor umane, inclusiv gestionarea dosarelor angajaților și a salarizării.</b>	Această prelucrare este necesară pentru executarea contractului individual de muncă și respectarea obligațiilor legale de către <b>PRIMĂRIA SATULUI ROGOJENI</b>
<b>Realizarea unor studii/sondaje de satisfacție a angajaților</b>	Interesul nostru legitim de a identifica nivelul de satisfacție al angajaților.
<b>Realizarea de testimoniale și articole, interviuri, inclusiv prin procesarea imaginilor / fotografiilor angajaților.</b>	Acest tip de prelucrare este justificată doar de obținerea Consimțământului
<b>Publicarea fotografiilor și filmulețelor video în cazul în care angajatul poate fi identificat, cu scopul publicării materialelor informative, promovare evenimente și manifestări pe website-ul oficial, canalul Youtube, Facebook, Instagram sau alte platforme online de către PRIMĂRIA SATULUI ROGOJENI sau orice terțe persoane afiliate sau împuternicite de entitate, care pot realiza orice fel de materiale audio/video și orice fel de imagini, capturi sau materiale fotografice</b>	Acest tip de prelucrare este justificată doar de obținerea Consimțământului
<b>Organizarea unor evenimente și seminare în scopul dezvoltării competențelor tehnice și dezvoltare personală și profesională</b>	Interesul nostru legitim de a dezvolta competențele angajaților <b>PRIMĂRIA SATULUI ROGOJENI.</b>
<b>Evaluarea performanței și a talentelor, precum și analize statistice legate de managementul resurselor umane</b>	Această prelucrare este justificată de interesul legitim al <b>PRIMĂRIA SATULUI ROGOJENI</b> de a putea optimiza cariera angajaților săi pentru a asigura un management optim al resurselor umane.
<b>Asigurarea sănătății și securității în muncă („SSM”): efectuarea unor instructaje pentru protecția muncii și a controalelor medicale în caz de necesitate</b>	Obligația legală pentru prelucrarea datelor ce țin de SSM (pentru toate prelucrările care sunt prevăzute de legislația incidentă)
<b>Organizarea timpului de lucru, inclusiv prezența la locul de muncă, absențe, concedii plătite și concedii medicale.</b>	Această prelucrare este necesară pentru îndeplinirea contractului individual de muncă și respectarea obligațiilor legale de către <b>PRIMĂRIA SATULUI ROGOJENI.</b>

<b>Gestionarea deplasărilor în interes de serviciu, a costurilor de cazare și a oricăror cheltuieli aferente.</b>	Această prelucrare este necesară pentru îndeplinirea contractului de muncă.
<b>Acordarea și gestionarea de beneficii personale către angajați (neincluse în contractul individual de muncă)</b>	Interesul legitim al <b>PRIMĂRIEI SATULUI ROGOJENI</b> de a menține o buna relație de munca cu angajații.
<b>Desfășurarea de investigații, aspecte de disciplina muncii și oferirea de suport în situații conflictuale sau de neperformanță legate de angajați</b>	Interesul nostru legitim în asigurarea unui mediu de lucru propice și a unei bune relații cu angajații, de a respecta obligațiile legale și contractuale ale <b>PRIMĂRIEI SATULUI ROGOJENI</b> și de a proteja drepturile de care beneficiază entitatea
<b>Managementul instruirii</b>	Această prelucrare este necesară pentru îndeplinirea contractului de muncă și respectarea obligațiilor sale legale de către <b>PRIMĂRIA SATULUI ROGOJENI</b> .
<b>Păstrarea datelor personale ale angajaților</b>	Această prelucrare este necesară pentru a respecta obligația legală a <b>PRIMĂRIEI SATULUI ROGOJENI</b> de a respecta termenele legale de păstrare a datelor personale și de a răspunde solicitărilor și reclamațiilor angajaților.

#### Modificarea scopului

Vom folosi informațiile dumneavoastră personale numai în scopurile pentru care le-am colectat, cu excepția cazului în care considerăm în mod rezonabil că trebuie să-l folosim din alt motiv și că acest motiv este compatibil cu scopul inițial. Dacă trebuie să folosim informațiile dvs. personale pentru o situație care nu are legătură cu scopul inițial, vă vom anunța și vă vom explica temeiul legal care ne permite să facem acest lucru.

Vă rugăm să rețineți că este posibil să vă procesăm informațiile personale fără știrea sau consimțământul dvs, în conformitate cu regulile de mai sus, acolo unde acest lucru este cerut sau permis de lege.

Vă putem cere acordul pentru anumite operațiuni de prelucrare, inclusiv a datelor cu caracter special, care nu sunt justificate de unul dintre motivele menționate mai sus. Dacă este necesar consimțământul pentru prelucrarea în cauză, vi se va solicita separat pentru a vă asigura că consimțământul este liber, informat și explicit. Informațiile referitoare la această prelucrare precum și consecințele care decurg din refuzul de a consimți la prelucrare vă vor fi furnizate în momentul în care este solicitat consimțământul. Dorim să vă reamintim că contractul individual de muncă încheiat cu dumneavoastră nu vă obligă să acceptați nicio solicitare de consimțământ din partea **PRIMĂRIA SATULUI ROGOJENI**.

Date referitoare la condamnări penale și infracțiuni

Acolo unde este permis sau necesar din punct de vedere legal, vom solicita o copie a cazierului dumneavoastră judiciar pentru a permite verificările antecedentelor și pentru a îndeplini cerințele

noastre de reglementare. Vom prelucra și acest tip de date cu caracter personal în cazul în care are loc o infracțiune la locul de muncă.

Prelucrăm aceste date cu caracter personal pe baza intereselor noastre legitime, care includ asigurarea faptului că angajăm numai personal adecvat și asigurarea securității și protecției **PRIMĂRIEI SATULUI ROGOJENI** și a bunurilor noastre.

## **TERMENUL DE PĂSTRARE A DATELOR CU CARACTER PERSONAL**

Reținem datele personale ale angajaților noștri doar în măsura în care este necesar pentru îndeplinirea scopurilor pentru care le-am colectat sau pentru care au fost comunicate. În consecință, în general, vom păstra datele dumneavoastră cu caracter personal cel puțin pe durata angajării dumneavoastră în cadrul entității.

La expirarea termenului menționat datele din sistemul de evidență a angajaților sunt păstrate în formă arhivată pe perioada stabilită de Indicatorul documentelor-tip și al termenelor lor de păstrare pentru organele administrației publice, pentru instituțiile, organizațiile și întreprinderile Republicii Moldova, aprobat de Serviciul de Stat de Arhivă nr.57 din 27.07.2016).

Cu referire la termenul de păstrare a datele personale colectate în procesul de recrutare:

Datele sunt păstrate atât timp cât este necesar pentru finalizarea cu succes a procesului de recrutare. Datele referitoare la candidații selectați vor fi incluse în dosarul personal al acestora și vor fi păstrate pe perioada activității în cadrul **PRIMĂRIEI SATULUI ROGOJENI**, iar după încetarea raporturilor de muncă, se vor păstra în formă arhivată, pe perioada stabilită de Indicatorul documentelor-tip și al termenelor lor de păstrare pentru organele administrației publice, pentru instituțiile, organizațiile și întreprinderile Republicii Moldova, aprobat de Serviciul de Stat de Arhivă nr.57 din 27.07.2016).

În cazul în care CV-ul nu a fost selectat pentru ca dvs să puteți participa la proba interviului sau în urma interviului nu ați fost selectat pentru angajare, datele dvs. vor fi păstrate timp de 3 luni de la încheierea procesului de recrutare pentru a putea oferi, la necesitate, explicații candidaților cu privire la motivele pentru care candidatura a fost respinsă.

De asemenea, având în vedere interesul nostru legitim de a optimiza selecția celor mai potriviți candidați pentru posturile disponibile și pentru a vă informa despre alte campanii de recrutare pentru posturi disponibile în cadrul **PRIMĂRIEI SATULUI ROGOJENI**, vom păstra CV-ul dvs. **în acest caz, stocăm datele personale o perioadă de maxim 2 ani** (*perioadă care este proporțională și rezonabilă, pe termen scurt și mediu, cu scopul unei persoane de a găsi și de a ocupa un loc de muncă adecvat pregătirii sale*). Însă, în cazul în care nu doriți să păstrăm CV-ul dvs în acest scop, aveți dreptul să Vă opuneți și să solicitați ștergerea datelor.

Datele referitoare la candidați pot fi păstrate într-o arhivă intermediară în scopuri probatorii, în special pentru a se proteja împotriva unor eventuale reclamații pentru discriminare, pentru o perioadă nu mai mare de 5 ani de la încheierea procesului de recrutare.

## **DESTINATARIILE DATELOR DUMNEAVOASTRĂ:**

Accesul la datele tale personale este limitat doar la acele persoane care au nevoie să cunoască aceste informații în scopuri profesionale. Acestea pot fi departamentul / subdiviziunea și persoanele lor desemnate pentru a îndeplini anumite funcții, cum ar fi angajații din echipa de resurse umane, IT, etc.

Vom dezvălui datele tale cu caracter personal, doar în măsura în care este necesar, următoarelor categorii de terți:

alte entități, cum ar fi autorități publice, contabili, auditori, avocați și alți experți externi, acolo unde activitățile lor necesită aceste informații;

și societăți care ne furnizează produse și servicii, cum ar fi: servicii de resurse umane; agenții de recrutare; furnizori de sisteme de tehnologie a informației și de mentenanță a acestor sisteme, inclusiv arhivarea email-urilor, recuperări ale datelor în caz de atacuri cibernetice, servicii de securitate cibernetică.

Altele: CNAM, CNAS, SFS.

**Vom mai putea dezvălui datele tale personale unor terți în următoarele situații:**

- în cazul în care ne solicitați personal această dezvăluire sau ne dați acordul în acest sens;
- persoanelor care pot demonstra că dețin autoritatea legală de a acționa în numele dvs.;
- în cazul în care avem obligația de a dezvălui datele tale personale pentru a respecta o obligație legală sau o solicitare din partea autorităților;
- pentru a răspunde oricăror acțiuni juridice, pentru a proteja drepturile noastre sau ale unui terți;
- pentru siguranța oricărei persoane sau pentru a preveni orice fel de activitate nelegală.

Anumite date de identificare și profesionale, cum ar fi numele dvs., locul de muncă, titlul postului, detaliile de contact și orice informații publicate despre abilitățile și experiența dvs. pot fi, de asemenea, accesibile altor angajați sau prestatori de servicii.

**PRIMĂRIEI SATULUI ROGOJENI** se așteaptă ca acești terți să trateze orice date care le-au fost dezvăluite în conformitate cu legea aplicabilă, inclusiv în ceea ce privește confidențialitatea și securitatea datelor în cazul în care aceștia acționează ca „procesatori” (de exemplu, un furnizor de servicii de mentenanță IC) și își îndeplinesc sarcinile în numele nostru și conform instrucțiunilor noastre în scopurile de mai sus. În acest caz, datele dumneavoastră cu caracter personal vor fi dezvăluite acestor părți numai în măsura în care este necesar pentru furnizarea serviciilor solicitate.

#### **TRANSFERURI TRANSFRONTALIERE DE DATE CU CARACTER PERSONAL:**

Datele cu caracter personal pe care ni le-ați furnizat sunt prelucrate numai pe teritoriul Republicii Moldova și nu vor fi transferate în altă țară.

Dorim să Vă asigurăm că datele personale colectate și procesate de către noi NU sunt transmise terților în alte scopuri diferite de acela pentru care au fost colectate.

#### **PRELUCRAREA AUTOMATĂ A DATELOR CU CARACTER PERSONAL**

Datele dumneavoastră cu caracter personal nu vor fi prelucrate în vederea generării unor decizii bazate exclusiv pe prelucrarea automată care ar urma să producă efecte juridice asupra dumneavoastră sau să vă afecteze într-o măsură semnificativă.

#### **DREPTURILE DUMNEAVOASTRĂ**

- **dreptul de informare și acces la datele cu caracter personal:** puteți solicita informații privind existența activităților de prelucrare a datelor dumneavoastră personale și accesul la acele informații, dacă există.
- **dreptul la rectificarea datelor personale incorecte:** puteți rectifica datele personale inclusiv atunci când acestea sunt inexacte sau incomplete.
- **dreptul la ștergerea datelor (“dreptul de a fi uitat”):** puteți obține din partea operatorului ștergerea datelor cu caracter personal atunci când nu mai sunt necesare pentru îndeplinirea scopurilor în care au fost colectate sau când vă retrageți consimțământul în cazul în care acesta există;
- **dreptul la restricționarea prelucrării:** puteți solicita și obține restricționarea prelucrării datelor cu caracter personal care vă privesc în cazul în care contestați exactitatea datelor, legitimitatea deținerii lor sau în alte cazuri prevăzute de lege.
- **dreptul la portabilitatea datelor dumneavoastră cu caracter personal:** aveți dreptul de a primi datele dvs într-un format structurat, utilizat în mod curent și care poate fi citit automat

și dreptul de a le transmite aceste date altui operator, tară obstacole din partea operatorului căruia i-au fost furnizate datele cu caracter personal.

- **dreptul de a nu fi supus unei decizii individuale:** aveți dreptul de a cere anularea, în totalitate sau parțială, a oricărei decizii individuale care produce efecte juridice asupra drepturilor și libertăților sale, fiind întemeiată exclusiv pe prelucrarea automatizată a datelor cu caracter personal destinată să evalueze unele aspecte ale personalității sale, precum competența profesională, credibilitatea, comportamentul și altele asemenea.
- **dreptul la opoziție:** puteți să vă opuneți, în special, prelucrărilor de date care se întemeiază pe interesul nostru legitim;
- **dreptul de a vă retrage consimțământul:** în cazurile în care prelucrarea se întemeiază pe consimțământul dumneavoastră, îl puteți retrage oricând. Retragerea consimțământului va avea efecte doar pentru viitor, prelucrarea efectuată anterior retragerii rămânând în continuare legitimă.
- **dreptul de a depune o plângere la operator și la autoritatea competentă privind protecția datelor** (CNPDCP - <https://datepersonale.md/>).

## **EXERCITAREA DREPTURILOR DVS.:**

În situația în care doriți să vă exercitați drepturile prezentate anterior sau considerați că prelucrarea datelor dvs se realizează fără respectarea prevederilor Legii privind protecția datelor cu caracter personal nr.133 din 08.07.2011, puteți formula o cerere scrisă, datată și semnată către operatorul **PRIMĂRIA SATULUI ROGOJENI**, la adresa **rnl. Șoldănești, s. Rogojeni, MD-7230**, ori către Responsabilul cu protecția datelor, la adresa de e-mail: [\\_primaria.rogojeni@apl.gov.md](mailto:_primaria.rogojeni@apl.gov.md)

Dacă doriți să vă exercitați dreptul de a formula plângere la autoritatea de stat competentă, vă informăm că aceasta este Centrul Național Pentru Protecția Datelor cu Caracter Personal (CNPDCP -<https://datepersonale.md/>) sau instanțelor de judecată.

## **NOTIFICARE PRIVIND MODIFICĂRILE ADUSE ACESTEI POLITICI**

Putem modifica sau actualiza această Politică în orice moment.

În cazul în care modificăm gestionarea protecției datelor cu caracter personal, vă vom anunța cu privire la modificările sau actualizarea acestei Politici, astfel încât să știți ce date procesăm și cum le utilizăm.

**LISTA ANGAJAȚILOR**  
**familiarizați cu**  
**Politica de Confidențialitate privind prelucrarea datelor personale**  
**ale angajaților și potențialilor angajați**  
**ai Primăriei satului Rogojeni, raionul Șoldănești**

<b>Nr.</b>	<b>Numele, prenumele</b>	<b>Funcția</b>	<b>Am luat cunoștință (semnătura)</b>	<b>Data</b>
1.	Groza Ruslan	primar		
2.	Ardeleanu Viorica	secretara consiliului		
3.	Guzun Ana	contabila - șefa		
4.	Odagiu Maria	specialistă		
5.	Iacicurinscaia Olga	Muncitoare auxiliară		
6.	Ianciu Dumitru	Muncitor auxiliar		
7.	Fosa Svetlana	Muncitoare auxiliară		
8.	Iacicurinscaia Olga	Îngrijitoare de încăperi		

**Anexa nr.6**  
**la Decizia nr.1/13**  
**din 25.02.2025**

**POLITICA ANTI - SPAM**  
**ÎN CADRUL PRIMĂRIEI SATULUI ROGOJENI**

## DEFINIȚII

**„date cu caracter personal”** - orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată”); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

**„prelucrare”** - înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;

**„operator”** - reprezintă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin actele normative, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în actele normative;

**„persoană împuternicită de operator”** - înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

**„destinatar”** - înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Cu toate acestea, autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autoritățile publice respective respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării;

**„parte terță”** - înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;

**„consimțământ”** - al persoanei vizate înseamnă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;

**„încălcarea securității datelor cu caracter personal”** - înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea;

CADRUL GENERAL:

**Scop.** Prezenta politică are ca scop asigurarea unui nivel adecvat de securitate a sistemelor informaționale ale **PRIMĂRIEI SATULUI ROGOJENI** (în continuare **”Operator”** sau **”entitatea”**) împotriva SPAM-ului, în principal cu privire la mesajele publicitare nesolicitate și/sau la mesajele ce urmăresc realizarea unei fraude prin obținerea de date confidențiale.

## DOMENIUL DE APLICARE

Prezența politică se aplică tuturor structurilor organizatorice/departamentelor ale Operatorului **PRIMĂRIA SATULUI ROGOJENI.**

### PREVEDERI GENERALE

#### Utilizarea Internetului

Accesul utilizatorilor la Internet este permis pentru îndeplinirea sarcinilor de serviciu. Utilizatorii nu trebuie să își instaleze niciun produs software pe stațiile de lucru ale Operatorului indiferent de sursa de proveniență a respectivului produs software (Internet sau altă sursă).

Documentele atașate mesajelor e-mail vor putea fi deschise doar dacă acestea sunt primite dintr-o sursă sigură. Înainte de a fi deschise, documentele atașate trebuie scanate cu un program antivirus.

Este interzisă folosirea calculatoarelor Operatorului pentru distribuirea e-mail-urilor nesolicitate ori susținerea oricărui tip de campanie publicitară care ar putea avea ca efect exprimarea unor plângeri din partea destinatarilor.

Mesajele de tip „**SPAM**” includ o varietate de promoții și solicitări precum cele de tipul mesajelor trimise în masă, sistemele piramidale și promovarea directă de produse. Atunci când angajații Operatorului primesc astfel de mesaje vor trebui să le trimită Responsabilului IT fără a le deschide sau a le răspunde. Departamentul IT va adopta măsuri corespunzătoare pentru stoparea primirii acestor mesaje.

-în cadrul comunicației electronice se interzice înlocuirea, înlăturarea sau denaturarea identității unui utilizator.

-în formularea mesajelor electronice, utilizatorul este obligat să-și precizeze datele de identificare, care trebuie să conțină:

- numele acestuia;
- numărul de telefon;
- adresa de e-mail sau apartenența la o anumită organizație/entitate.

De asemenea, se recomandă atașarea unei semnături electronice în cadrul mesajelor care să conțină informații despre expeditor precum poziția ocupată în cadrul Operatorului, apartenența la aceasta, adresa etc.

Se recomandă confirmarea identității terțelor părți înainte ca angajații Operatorului să poată trimite orice informație de uz intern să încheie orice fel de contract sau să comande produse prin intermediul rețelelor publice. Atunci când este posibil, confirmarea identității trebuie făcută prin intermediul semnăturilor digitale, altfel pot fi utilizate mijloace de identificare complementare: discuții telefonice, scrisoare de împuternicire sau referințe din partea terților.

Nu se permite accesul angajaților în modulul de administrare al site-ului web al Operatorului decât dacă au aprobarea Conducerii de a efectua modificări în conținutul de informații. Adăugarea de legături către alte resurse, actualizarea informațiilor sau schimbarea design-ului intră, de asemenea, sub incidența acestor aprobări.

Acordarea drepturilor de acces din Internet la rețeaua internă a Operatorului se va aproba colaboratorilor numai pe baza unei solicitări exprimate de către managerul de sistem. Din rândul prestatorilor de servicii fac parte: producătorii de software, contractorii, consultații, personalul temporar, personalul companiilor prestatoare de servicii, etc.

Accesul va fi acordat în mod individual și doar pentru perioada desfășurării sarcinilor aprobate.

Angajații pot folosi alte surse de furnizare a conexiunii la Internet utilizând calculatoarele Operatorului, doar cu acordul Conducerii, întrucât controalele de acces și metodele de asigurare a securității datelor nu pot fi aplicate corespunzător decât dacă întregul flux de activități

referitoare la Internet trece prin echipamentele de tip firewall ale Operatorului. În aceeași manieră, angajații sunt obligați să utilizeze numai căsuța de e-mail oferită de către Operator. În acest context, folosirea adresei de e-mail personale nu este permisă.

Este interzisă folosirea în scopul afacerilor personale sau încredințarea către alte persoane a resurselor informatice ale Operatorului.

Operatorul nu se declară răspunzător pentru conținutul paginilor de Internet accesate de angajați. În cazul accesării întâmplătoare a unui site cu conținut informațional imoral (caracter sexual explicit, rasist, misogin, violent sau de natură ofensatoare), angajații în cauză sunt obligați să aleagă o altă pagină sau să încheie procesul curent.

Operatorul poate înregistra paginile accesate, fișierele desemnate, timpul petrecut pe o pagină anume și alte informații conexe.

Conducerea Operatorului poate primi rapoarte ce conțin astfel de informații și pe baza lor să decidă tipul accesului la Internet în cadrul fiecărui departament al Operatorului.

Conducerea Operatorului are dreptul de a revizui e-mail-urile, fișierele aflate pe stațiile de lucru, fișierele temporare ale browser-elor de Internet (Internet Explorer, Mozilla Firefox, Google Chrome etc.), paginile marcate, istoricul site-urilor web necesare și alte informații stocate sau care tranzitează stațiile de lucru ale Operatorului în orice moment și fără necesitatea unui anumit prealabil.

Se interzice angajaților stabilirea unor legături la Internet sau la alte rețele externe care ar putea favoriza terțe părți să pătrundă în rețeaua Operatorului și să aibă acces la sistemele și informațiile acestora, decât dacă acest lucru este aprobat de către Conducere. Aceste conexiuni presupun legături de tip file-sharing (partajare de fișiere), sisteme de comerț prin intermediul Internetului sau servere FTP.

#### Utilizarea e-mail-ului

Operatorul pune la dispoziția angajaților săi sau, după caz, prestatorilor de servicii atunci când aceștia utilizează sistemele IT ale Operatorului, căsuțe de poștă electronică. Conturile de poștă electronică individuale nu trebuie utilizate în comun.

Utilizarea sistemului de mesagerie electronică al Operatorului trebuie realizată ca parte a activității profesionale, ce are ca scop îmbunătățirea activităților de zi cu zi prin înlesnirea comunicării interne în cadrul Operatorului, respectiv în exterior prin menținerea legăturilor cu clienții, partenerii de afaceri ai Operatorului sau cu autoritățile locale.

Comunicarea electronică se va limita la materialele care au legătură cu activitățile profesionale și sarcinile de serviciu ale angajaților și nu va fi folosită ca suport pentru campanii caritabile de strângere de fonduri, campanii de susținere politică/religioasă sau pentru activități ce țin de afaceri personale, amuzament sau distracție.

Se interzice folosirea de către un utilizator a unei adrese de e-mail ce aparține altei persoane. Periodic, angajații vor fi informați și instruiți să folosească în mod adecvat resursele sistemului informatic al Operatorului.

În cadrul comunicației electronice se interzice înlocuirea, înlăturarea sau denaturarea identității unui utilizator.

Fiecare utilizator al sistemului de e-mail al Operatorului (administrator sau utilizator final) trebuie să se preocupe de luarea tuturor măsurilor necesare în vederea asigurării protecției împotriva e-mail-urilor nesolicitate (mesaje de tip „hoax”, mesaje înlănțuite chain letter, spam

etc.) și scheme de mesaje electronice cu caracter fraudulos (phishing și alte tipuri de mesaje de tip fraudulos).

Fiecare utilizator al sistemului de e-mail al Operatorului (administrator sau utilizator final) trebuie să se preocupe de luarea tuturor măsurilor necesare în vederea asigurării protecției împotriva infectării cu produse software cu potențial distructiv (virusi, troieni, worm etc.) în cazul în care primesc sau detectează orice e-mail suspicios, angajații sunt obligați să informeze Departamentul IT.

#### Utilizarea echipamentelor mobile

Toate echipamentele mobile care au fost achiziționate în numele Operatorului sunt considerate a fi proprietatea Operatorului și vor fi utilizate ca atare.

Atribuirea unui dispozitiv mobil către un angajat implică responsabilitatea acestuia de a asigura securitatea dispozitivului atât în sediul Operatorului, cât și în locuința personală sau oricare altă locație.

Accesul la dispozitivele de tip mobile computing trebuie să fie securizat prin sistem de autentificare cu parolă sau cod PIN. Pentru o eficiență sporită nu vor fi folosite parole și coduri PIN ușor de identificat.

Accesul la rețeaua Operatorului din exterior nu este permisă decât printr-o conexiune securizată de tip VPN.

Utilizarea dispozitivelor mobile în spații publice trebuie făcută cu prudență pentru a elimina riscul ca informațiile afișate pe ecran să poată fi văzute de persoane neautorizate. În situația în care se poate asigura o minimă intimitate, utilizarea dispozitivelor mobile în locațiile publice trebuie restrânsă.

Pentru stocarea informațiilor cu caracter sensibil se recomandă folosirea serverelor de rețea și mai puțin a echipamentelor de tip mobil computing. Pentru a se asigura siguranța informației, discul fix al dispozitivului mobil și părțile aferente pe care se va face stocarea trebuie să fie criptate.

În funcție de arhitectura hardware și software, dispozitivele de tip mobil computing trebuie să aibă configurate soluții corespunzătoare de protecție împotriva aplicațiilor software cu potențial distructiv (virusi, spyware, malware etc.). Utilizatorul unui dispozitiv mobil trebuie să-și actualizeze permanent programele de protecție și să se asigure că folosește ultima versiune dată de producător.

Toate echipamentele mobile vor avea configurată o aplicație „screen-saver” care se va activa automat după un timp determinat de inactivitate.

Cazurile de pierdere sau furt a unui dispozitiv mobil trebuie raportate în cel mai scurt timp către managerul de departament.

Echipamentele mobile de calcul (laptop, notebook, balckberry etc.) pot conține informații cu caracter sensibil din cadrul Primăriei. În aceste condiții, utilizatorul unui astfel de dispozitiv devine responsabil pentru disponibilitatea, integritatea și confidențialitatea datelor referitoare la Primărie, pe care le are la dispoziție. Utilizarea calculatorului portabil în exteriorul Primăriei se permite doar cu acordul conducătorului și impune respectarea unor reguli:

Utilizatorul este responsabil de supravegherea permanentă a dispozitivului.

Utilizatorul trebuie să asigure din punct de vedere fizice securitatea echipamentului prin folosirea unor dispozitive de împiedicare a furtului (de exemplu: cablul de securitate).

Utilizatorii trebuie să-și salveze periodic documentele pe care le dezvoltă pentru a preveni pierderea accidentală a informațiilor nesalvate.

Pentru orice perioadă de inactivitate, dispozitivul va fi blocat, iar deblocarea se va face pe baza de parolă.

Dispozitivele trebuie să aibă configurat un mecanism de autentificare adecvat pentru securizarea accesului.

Este interzisă folosirea programelor software nelicențiate și instalarea aplicațiilor de către utilizatori.

Folosirea telefoanelor mobile ale Operatorului este permisă numai pentru desfășurarea convorbirilor telefonice. De asemenea, se recomandă supravegherea telefoanelor mobile, întrucât acestea ar putea conține informații din cadrul Operatorului (de exemplu, e-mail etc.).

#### Protecția împotriva virușilor

Operatorul are implementate măsuri de protecție ale sistemelor telefonice informatice, aplicațiilor și rețelelor și de detectare a tuturor tipurilor de viruși și a altor produse software dăunătoare.

Pe toate sistemele informatice ale Operatorului există instalate programe antivirus.

Utilizatorii au responsabilitatea de a nu modifica setările programului antivirus. Totodată, sunt responsabili de raportarea către Departamentul IT a tuturor incidentelor datorate virușilor.

Departamentul IT are următoarele responsabilități:

-să se asigure că programul antivirus este instalat pe toate stațiile utilizatorilor și pe toate serverele;

să actualizeze definițiile virușilor;

-să înregistreze și să investigheze toate incidentele raportate de către utilizatori.

#### Salvarea și restaurarea datelor

Operatorul realizează salvări (backup) periodice ale sistemelor și datelor, conform procedurilor interne. Salvările sunt menținute conform prevederilor acestei norme, iar periodic sunt efectuate teste ale mediilor de stocare pentru a se verifica posibilitatea recuperării datelor în cazul unei urgențe.

### **LISTA ANGAJAȚILOR FAMILIARIZAȚI CU PREVEDERILE POLITICII ANTI-SPAM ÎN CADRUL PRIMĂRIEI SATULUI ROGOJENI**

<b>Nr.</b>	<b>Numele, prenumele</b>	<b>Funcția</b>	<b>Am luat cunoștință (semnătura)</b>	<b>Data</b>
1.	Groza Ruslan	primar		
2.	Ardeleanu Viorica	secretara consiliului		
3.	Guzun Ana	contabila - șefa		
4.	Odagiu Maria	specialistă		
5.	Iacurinscaia Olga	Muncitoare auxiliară		
6.	Ianciu Dumitru	Muncitor auxiliar		

7.	Fosa Svetlana	Muncitoare auxiliară		
8.	Iacicurinscaia Olga	Îngrijitoare de încăperi		

Anexa nr.7  
la Decizia nr.1/13  
din 25.02.2025

**POLITICA PRIVIND RESURSELE INFORMATICE ÎN CADRUL  
PRIMĂRIEI SATULUIROGOJENI**

## 1. DEFINIȚII

**„date cu caracter personal”** - orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată”); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

**„prelucrare”** - înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;

**„operator”** - reprezintă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin actele normative, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în actele normative;

**„persoană împuternicită de operator”** - înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

**„destinatar”** - înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Cu toate acestea, autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autoritățile publice respective respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării;

**„parte terță”** - înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;

**„consimțământ”** - al persoanei vizate înseamnă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;

**„încălcarea securității datelor cu caracter personal”** - înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea;

## 2. CADRUL GENERAL

**Scop.** Prezenta politică are ca scop asigurarea securității resurselor informaționale ale **PRIMĂRIEI SATULUI ROGOJENI**.

(în continuare ”Operator” sau ”entitatea”). Se va urmări protecția resurselor informaționale împotriva modificărilor neautorizate sau accidentale, asigurând acuratețea și completitudinea acestora, precum și protecția resurselor informaționale împotriva divulgării neautorizate.

### **3. DOMENIUL DE APLICARE**

Prezenta politică se aplică tuturor structurilor organizatorice/departamentelor Operatorului de date **PRIMĂRIA SATULUI ROGOJENI**.

Prezenta politică va fi considerată ca având caracter general și se va aplica tuturor prelucrărilor efectuate de Operator. În cazul în care se constată existența anumitor aspecte legate de gestionare datelor cu caracter general pentru care prezenta politică nu oferă directive corespunzătoare, angajații trebuie să solicite imediat consiliere din partea Responsabilului pentru Protecția Datelor (DPO), dacă a fost numit, sau reprezentantului legal al Operatorului.

### **4. PREVEDERI GENERALE**

**4.1. Principii.** Toți angajații și prestatorii de servicii care utilizează resursele informaționale ale Operatorului de date **PRIMĂRIA SATULUI ROGOJENI** au responsabilitatea de a proteja activele informaționale ale Operatorului, folosind prezenta politică drept un instrument principal și aderând la standardele, procedurile și îndrumările incluse în acesta.

Rețelele, aplicațiile și sistemele informatice ale Operatorului sunt disponibile în momentul în care este nevoie de ele. Acestea nu pot fi accesate decât de către utilizatorii autorizați și conțin informații corecte și complete.

Prin implementarea unor măsuri atât tehnice, cât și operaționale, Operatorul va proteja toate programele, echipamentele și activele informaționale aflate în patrimoniul ei.

**4.2. Informarea utilizatorilor.** Fiecare angajat/prestator de servicii care utilizează resursele informaționale ale Operatorului de date **PRIMĂRIA SATULUI ROGOJENI**, va participa în momentul angajării și ulterior, anual, la cursuri de securitate a informațiilor organizate de conducerea Operatorului. De asemenea, fiecărui angajat/prestator de servicii îi vor fi puse la dispoziție, în momentul angajării/semnării contractului de colaborare, copii ale prezentei politici, precum și ale tuturor normelor și procedurilor operaționale IT, pe care va trebui să le respecte. Aceștia își vor exprima acordul cu privire la respectarea acestor norme prin semnarea formulărilor din **Anexa 1** a acestui document.

De asemenea, prezenta politică precum și celelalte norme și proceduri operaționale IT vor fi postate pe Intranetul Operatorului într-o locație disponibilă tuturor angajaților. Angajații vor fi informați cu privire la această locație. Prezenta politică precum și celelalte proceduri operaționale se adresează deopotrivă și prestatorilor de servicii ai Operatorului, care vor folosi sau vor avea acces la resursele fizice și informaționale ale Operatorului. Pentru a dovedi luarea la cunoștință a prevederilor incluse în aceste norme, colaboratorii vor semna formularul din **Anexa 1**.

**4.3. Evaluarea riscurilor.** Operatorul realizează în mod continuu evaluarea riscurilor pentru toate sistemele informatice, aplicațiile și rețele care sunt utilizate în cadrul tuturor proceselor

Operatorului. Totodată, se vor identifica măsurile necesare pentru protecția împotriva breșelor de confidențialitate, integritate și disponibilitate.

**4.4. Utilizarea informațiilor.** Fiecare angajator/ prestator de servicii care utilizează resursele informaționale ale Operatorului de date **PRIMĂRIA SATULUI ROGOJENI** trebuie să aibă acces doar la informația necesară pentru a-și îndeplini sarcinile. Informațiile sensibile trebuie accesate doar de către angajații / prestatorilor de servicii cărora proprietarul aplicației respective le-a acordat drept de acces.

Informațiile Operatorului nu trebuie folosite în alte scopuri decât cele de afaceri aprobate în mod oficial de către Conducere. Folosirea neaprobata a informațiilor Operatorului este interzisă.

Utilizatorilor nu le este permis să efectueze nicio activitate în sistemele informatice ale Operatorului ce ar putea conduce la deteriorarea imaginii Operatorului.

Folosirea în scop personal a informațiilor Operatorului, cum ar fi listele de distribuție a e-mail-urilor, este interzisă.

Nu este permisă utilizarea de programe licențiate de către Operator pe calculatoare personale, cu excepția cazului în care sistemul a fost desemnat să proceseze informații ale Operatorului.

Toate activitățile utilizatorilor sunt înregistrate și analizate ulterior. O conduită nepotrivită poate duce la acțiuni disciplinare inclusiv revocarea drepturilor de acces. Operatorul permite utilizarea ocazională a sistemelor informatice în scop personal, inclusiv a telefonului, atât timp cât nu implică costuri semnificative, nu interferează cu performanța la locul de muncă, și nu limitează accesul altor utilizatori la resursele sistemului.

#### **4.5. Politica pentru parole**

Accesul la sistemul informatic al Operatorului trebuie să fie restricționat pe bază de nume de utilizator și parolă.

Parolele asociate conturilor de utilizatori nu trebuie folosite pentru autentificarea în sisteme externe (de ex. Conturi personale de e-mail, conturi pe site-uri comerciale etc.). Parolele trebuie să difere de la o aplicație accesată la alta. Alegeți parole diferite pentru aplicații față de cele pentru accesul în rețea.

Utilizatorii nu trebuie să dezvăluie nimănui parolele utilizate în cadrul sistemelor informatice ale Operatorului, nici măcar celorlalți angajați. Toate parolele sunt calificate ca informații confidențiale.

Nu este permisă stocarea parolelor în sistemele informatice. Nu este permisă scrierea parolelor în clar pe hârtie sau pe un alt suport.

Pentru protejarea parolelor, utilizatorii trebuie să:

- NU destăinuie sub nicio circumstanță nicio parolă NIMĂNUI;
- NU împărtășească parolele cu membrii familiei;
- NU dezvăluie parola colegilor de serviciu pe perioada concediului;
- NU ofere NIMĂNUI detalii cu privire la parolă („numărul meu de la mașină”);
- NU scrie în clar parola pe hârtie sau în mesaje electronice;
- NU păstreze parolele scrise;
- NU stocheze parolele sub formă de fișiere pe NICIUN sistem de calcul (nici pe echipamentele mobile) fără ca acele fișiere să fie criptate.

Este necesar ca utilizatorii să schimbe parola cel puțin o dată la 90 de zile. Dacă un utilizator suspectează că o persoană a aflat un cont de utilizator sau o parolă ce nu îi este atribuită, trebuie să raporteze departamentului IT și să-și schimbe imediat parola în cazul în care aceasta este la cauză.

**Parolele adecvate au următoarele caracteristici:**

- conțin atât majuscule, cât și litere mici (A-Z, a-z);
- conțin cifre și cel puțin un caracter alfanumeric (0-9,!@#\$%^&\*()\_+?:;.);
- nu se bazează pe informații personale precum nume, numere de telefon etc.;
- nu coincid și nu conțin numele de utilizator;
- au lungimea minimă de opt caractere.

Parolele neadecvate reprezintă parole cu grad scăzut de complexitate ce sunt deseori caracterizate de una dintre următoarele specificații:

- reprezintă un cuvânt folosit în mod uzual, cum ar fi:
- numele de familie al utilizatorului, numele copiilor, colegilor de serviciu, animalelor de Operator etc.;
- zilele de naștere, adrese, numere de telefon, numărul de la mașină sau alte informații personale;
- cuvinte sau succesiuni de litere sau cifre de genul: abcdef,123456,zyxwvuts, 123321 etc.;
- oricare dintre cuvintele de mai sus scrise în ordinul invers;
- coincid sau conțin numele de utilizator;
- au lungimea mai mică de opt caractere.

#### **4.6. Accesul la distanță**

Accesul la distanță se va face folosind un mecanism de autentificare cu parolă valabilă o singură dată sau prin chei publice/private protejate cu parole corespunzătoare. Accesul la distanță se acordă după aprobarea Departamentului IT și conducătorului Operatorului.

Accesul de la distanță în sistemele Operatorului impune respectarea următoarelor reguli:

- Remote control - descriere proces de acces sistem (se identifică partea care încearcă să acceseze, se comunică parola de acces prin telefon, nu e-mail: parola de acces este regenerată la fiecare logare).
- Înainte de a iniția conexiunea la rețeaua Operatorului, angajații trebuie să se asigure că echipamentul de calcul pe care îl folosesc nu este conectat în același timp la o altă rețea.
- Orice altă configurație hardware sau software de acces de la distanță în afara celor aprobate de Operator trebuie aprobată de Departamentul IT.
- Conectarea de la distanță la rețeaua Operatorului implică folosirea unui software antivirus aprobat și actualizat zilnic la ultimele semnături de virusuri.
- Angajații vor accesa sistemele Operatorului de la distanță numai folosind echipamentele Operatorului, configurate și protejate corespunzător (PC-uri, Laptopuri, PDA-uri, tablete

- etc.), sau după caz, în cazuri excepționale folosind echipamentele personale, doar cu autorizarea conducătorului.

#### **4.7. Raportarea incidentelor**

Angajații trebuie să raporteze toate incidentele cu privire la sistemele informatice ale Operatorului, iar cele referitoare la securitatea informației trebuie să fie raportate Departamentului IT.

Angajații vor raporta incidentele întâlnite către responsabilii din cadrul Operatorului prin trimiterea unui mesaj electronice în care vor specifica condițiile de apariție ale incidentului, alături de toate detaliile observate la momentul procedurii.

Procesul de raportare a incidentelor de securitate a informației folosește aceleași căi de raportare ca și în cazul incidentelor obișnuite.

### **5. ROLURI ȘI RESPONSABILITĂȚI**

#### **5.1. Angajații**

Toți angajații care activează în cadrul Operatorului au următoarele responsabilități:

- să respecte Politica privind resursele informatice;
- să asiste în sesiuni de informare și la cursuri de securitatea informației;
- să se familiarizeze și să acționeze în concordanță cu toate cerințele Operatorului ;
- să solicite șefului lor direct acces la resursele informaționale care le sunt necesare;
- să raporteze toate activitățile suspecte și problemele de securitate;
- să raporteze orice suspiciune de breșă de securitate sau breșă de securitate ca atare;
- să prevină introducerea în sistemele informaționale din cadrul Operatorului de produse software cu potențial distructiv;
- să păstreze în bună stare resursele informaționale, produsele software și echipamentele hardware ale Operatorului.

#### **5.2. Conducerea Operatorului**

Are următoarele responsabilități:

- să asigure securitatea bunurilor organizației (informație, echipamente hardware, produse software folosite de către angajați și de către terțe părți);
- să asigure aplicarea politicii de securitate a Informației;
- să se asigure că toți angajații sunt conștienți de responsabilitățile de securitate pe care le au;
- să se asigure raportarea și înregistrarea tuturor incidentelor de securitate;
- să asigure că orice încălcare a securității informației de către angajați este investigată în mod corespunzător;
- să asigure faptul că angajații au fost instruiți corespunzător cu privire la securitatea informației;
- să emită decizii prin care este dispusă cercetarea faptelor angajaților care au încălcat prevederile prezentei proceduri.

## 6. Dispoziții finale

### Răspunderea în cazul încălcării procedurii

Încălcarea prevederilor acestei proceduri poate determina aplicarea unor măsuri disciplinare, inclusiv desfacerea contractului de muncă din motive care țin de persoana angajatului sau chiar răspunderea penală a persoanei care se face vinovată de încălcarea prevederilor prezentei Proceduri, atunci când legile în vigoare o impun.

Prestatorii de servicii care utilizează resursele informaționale ale Operatorului de date **PRIMĂRIA SATULUI ROGOJENI**, de asemenea poartă răspundere deplină în conformitate cu legislația în vigoare, în cazul în care se face vinovată de încălcarea prevederilor prezentei Proceduri.

În condițiile menționate, lipsa de înțelegere în cazul în care procedura va fi încălcată nu va putea fi invocată de către utilizatorii cărora le este adresată această procedură.

### LISTA ANGAJAȚILOR FAMILIARIZAȚI CU PREVEDERILE POLITICII PRIVIND RESURSELE INFORMATICE ÎN CADRUL PRIMĂRIEI SATULUI ROGOJENI

Nr.	Numele, prenumele	Funcția	Am luat cunoștință (semnătura)	Data
1.	Groza Ruslan	primar		
2.	Ardeleanu Viorica	secretara consiliului		
3.	Guzun Ana	contabila - șefa		
4.	Odagiu Maria	specialistă		
5.	Iacurinscaia Olga	Muncitoare auxiliară		
6.	Iancu Dumitru	Muncitor auxiliar		
7.	Fosa Svetlana	Muncitoare auxiliară		
8.	Iacurinscaia Olga	Îngrijitoare de încăperi		

## **Anexa 1 - Acord de respectare a Politicii de Securitate a Informațiilor în cadrul PRIMĂRIEI SATULUI ROGOJENI**

Numele complet al utilizatorului: \_\_\_\_\_

Datele de contact: \_\_\_\_\_

Subsemnatul identificat mai sus, am luat la cunoștință prevederile Procedurii privind resursele informatice și îmi exprim prin semnarea prezentului formular acordul cu privire la următoarele:

- Să respect toate prevederile politicilor și procedurilor existente în cadrul Operatorului, precum și în Politica privind resursele informatice. În acest sens, am luat la cunoștință conținutul tuturor acestor documente.
- Să adopt toate măsurile de precauție necesare în vederea eliminării riscurilor de dezvăluire către persoane neautorizate a informațiilor interne ale Operatorului sau a informațiilor care mi-au fost încredințate de către Operator.
- Să returnez odată cu finalizarea activității mele pentru Operator, toate materialele la care am primit acces ca rezultat al activității mele în cadrul acesteia. Înțeleg faptul că îmi este interzisă folosirea acestor informații în scopuri personale și nici nu am autorizarea de a dezvălui aceste materiale terților fără aprobarea explicită în scris a managerului desemnat pentru relația cu angajatorul meu din interiorul Operatorului.
- Să informez prompt șeful direct despre orice situație de încălcare sau posibilă încălcare a Politicilor din cadrul Operatorului.
- Sunt de acord cu faptul că încălcarea Politicii privind resursele informatice poate duce la aplicarea de măsuri disciplinare, la revocarea drepturilor, la desfacerea contractului de muncă și eventual la răspunderea legală pe cale civilă sau penală.

**Data**

**Semnătura**

Anexa nr.8  
la Decizia nr.1/13  
din 25.02.2025

REGULAMENTUL  
PRIVIND SUPRAVEGHEREA PRIN MIJLOACE VIDEO  
ÎN CADRUL PRIMĂRIEI SATULUI ROGOJENI

## 1. Dispoziții generale

În contextul actual securitatea obiectivelor nu poate fi asigurată fără o supraveghere video eficientă, care să permită, atât monitorizarea în timp real a evenimentelor și persoanelor suspecte, cât și înregistrarea imaginilor video.

Aceste sisteme de supraveghere prin mijloace video se adresează, în principal, spațiilor în care se desfășoară activități de vânzare, spații comerciale dar și birourilor de acces public.

Totodată utilizarea unui astfel de sistem include anumite responsabilități și garanții din partea proprietarului de sistem, referitor la prelucrarea și protecția datelor cu caracter personal ce se înregistrează în sistem, atribuții și reglementări descrise în legea nr. 133 din 18.07.2011 privind protecția datelor cu caracter personal.

Din acest motiv este necesară stabilirea unui regulament de securitate privind supravegherea prin mijloace video și prelucrarea datelor cu caracter personal preluate și înregistrate în sistemul de supraveghere prin mijloace video.

**Mijloacele de supraveghere video se instalează și utilizează cu respectarea principiului:**

- legalității;
- proporționalității;
- transparenței;
- securității.

**2. Regulamentul privind supravegherea prin mijloace video în cadrul PRIMĂRIEI SATULUI ROGOJENI are drept scop:**

- Stabilirea unui set unitar de reguli care reglementează implementarea și utilizarea sistemului de supraveghere prin mijloace video, în scopul asigurării securității persoanelor și bunurilor, pazei și protecției bunurilor, imobilelor, valorilor și a materialelor cu regim special, respectând în același timp obligațiile ce revin entității, în calitate de operator de date, conform Legii nr. 133 din 18.07.2011 și măsurile de securitate adoptate pentru protecția datelor cu caracter personal, protejarea vieții private, a intereselor legitime și garantarea drepturilor fundamentale ale persoanelor vizate.
- Stabilirea responsabilităților privind administrarea și exploatarea sistemului de supraveghere prin mijloace video, precum și cele privind întocmirea, avizarea și aprobarea documentelor aferente acestor activități.
- Scopul utilizării sistemului de supraveghere prin mijloace video este de a asigura buna administrare și funcționare a entității, în special în vederea controlului de securitate și pază. De asemenea, sistemul de supraveghere prin mijloace video este necesar pentru a sprijini politicile de securitate instituite de actele normative care reglementează protecția datelor cu caracter personal și contribuie la îndeplinirea atribuțiilor structurii de securitate.
- Prezentul Regulament descrie măsurile care necesită a fi luate de **PRIMĂRIA SATULUI ROGOJENI** pentru a proteja datele cu caracter personal care sânt prelucrate prin metoda supravegherii video, vieții private și alte drepturi fundamentale și interese legitime ale subiecților.

## 3. Zonele supravegheate

- Camerele de supraveghere video sânt amplasate în locuri vizibile. Orice utilizare ascunsă a acestora este strict interzisă, cu excepția cazurilor expres reglementate de legislație.
- Camerele de supraveghere video sânt amplasate conform anexelor nr. 1 și 2 al prezentului Regulament.
- 
- Nu sânt monitorizate zonele în care persoanele pot conta, în mod rezonabil, pe intimitate, precum birourile de serviciu și toaletele. Instalarea mijloacelor de supraveghere video se poate realiza numai în condițiile în care echipamentele sânt orientate exclusiv asupra căilor de acces și perimetrului

acestor bunuri, fără ca în raza lor de acoperire să fie vizualizate alte spații publice, ori bunurile terților.

#### 4. Datele cu caracter personal colectate prin intermediul sistemului de supraveghere prin mijloace video

- Sistemul de supraveghere prin mijloace video este dotat cu detector de mișcare. Toate camerele funcționează în regim 24/24 ore și sânt fixate.
- La darea în exploatare a sistemului de supraveghere video, persoana împuternicită va primi instructajul referitor la setările sistemului de supraveghere prin mijloace video, respectarea regimului de confidențialitate și dreptul de acces la informația prelucrată în sistemul de evidență.
- 

#### 5. Limitarea scopului

- Sistemul de supraveghere prin mijloace video va fi utilizat numai în scop legal, fără a se urmări în special obținerea unor informații pentru anchetele interne sau procedurile disciplinare, cu excepția situațiilor în care se produce un incident de securitate sau se observă un comportament infracțional (în circumstanțe excepționale imaginile pot fi transmise organelor competente în cadrul unor investigații disciplinare sau penale).
- în vederea protejării vieții private a altor subiecți decât cei vizați nemijlocit, sistemul de supraveghere prin mijloace video este dotat cu mecanisme care prevăd estomparea imaginii (în caz de necesitate) pentru a face ca întreaga imagine sau o parte a ei, după caz, să fie anonimată.
- Persoana responsabilă va gestiona accesul la sistemul de supraveghere prin mijloace video numai cu acordul scris al conducerii **PRIMĂRIEI SATULUI ROGOJENI**.

#### 6. Categoriile speciale de date cu caracter personal

- Sistemul de supraveghere prin mijloace video al **PRIMĂRIEI SATULUI ROGOJENI** nu are ca scop captarea (spre exemplu prin focalizare sau orientare selectivă) sau prelucrarea imaginilor (spre exemplu indexare, creare de profiluri) care constituie categoria specială de date cu caracter personal.
- 

#### 7. Accesul la datele cu caracter personal și dezvoltarea acestora

- Accesul la imaginile video înregistrate în timp real este limitat la un număr redus de angajați ai **PRIMĂRIEI SATULUI ROGOJENI**, care pot fi identificați individual, în conformitate cu lista aprobată de către conducerea entității.
- Accesul la imaginile video și/ sau la arhiva în care sânt stocate imaginile înregistrate este permis numai persoanei responsabile în conformitate cu Politica de securitate a **PRIMĂRIEI SATULUI ROGOJENI** și numai cu acordul scris al conducerii.
- Vizualizarea și/sau efectuarea copiilor din fișierele temporare în care sânt stocate imaginile video, este permis numai cu acordul scris al conducerii.
- în cazul solicitării de către organele de drept ale Republicii Moldova, care își exercită atribuțiile conform legii, a unor copii din fișierele temporare în care sânt stocate imaginile video, este permis numai cu acordul scris al conducerii **PRIMĂRIEI SATULUI ROGOJENI**.

#### 8. Protecția sistemului informațional de date cu caracter personal în care sânt stocate (prelucrate) imaginile video

- în vederea securizării sistemului informațional de date cu caracter personal în care sânt stocate (prelucrate) imaginile video, se aplică următoarele măsuri tehnice și organizatorice:

- sistemul informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video se păstrează în camera special amenajată (amplasarea se indică în Anexa 2);
- responsabilul de protecție a datelor cu caracter personal și responsabilii de securitate din cadrul entității vor fi consultați înainte de achiziționarea sau instalarea oricărui nou sistem de supraveghere prin mijloace video.
- toate sistemele trebuie să corespundă cerințelor de securitate descrise în legislație (HG nr. 1123 privind aprobarea cerințelor față de asigurarea securității datelor cu caracter personal).
- accesul fizic la sistemul informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video are numai persoana responsabilă desemnată și conducerea **PRIMĂRIEI SATULUI ROGOJENI**;
- accesul la înregistrările video prelucrate este restricționat prin introducerea unui șir de parole;
- în cazul deconectării energiei electrice, sistemul informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video este dotat cu sursă autonomă de alimentare cu energie electrică (UPS);
- sistemul informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video este dotat cu firewall care asigură protecția în rețea;
- Echipamentele sînt astfel instalate încît să se afle sub supraveghere doar acele spații identificate în analiza de risc ca avînd nevoie de protecție suplimentară.
- Utilizatorii sistemului de supraveghere prin mijloace video sunt instruiți să nu monitorizeze astfel de zone.
- **PRIMĂRIA SATULUI ROGOJENI** actualizează în permanență listă persoanelor care au acces la sistemul informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video, care descrie în detaliu drepturile de acces ale acestora.

## 9. Control Acces

- Imaginile captate de sistemul de supraveghere prin mijloace video sînt vizualizate în timp real pe monitoarele din camera de control acces, care reprezintă o încăpere securizată, iar monitoarele nu pot fi văzute din exterior.
- Camera de control acces este amplasată în sediul central al entității.
- Accesul neautorizat în Camera de control este interzis. Accesul este strict limitat la angajații autorizați: personalul cu funcții de asigurare al securității fizice și control acces, administratorul de sistem, responsabilii cu securitatea informației și conducerea entității.
- De la caz la caz, se poate acorda accesul în Camera de control și altor persoane, în afara celor menționate mai sus, doar pe bază de autorizare din partea responsabilului de securitate din cadrul entității. Aceste persoane nu vor avea acces la datele personale prelucrate în activitatea de supraveghere video, accesul acestora fiind permis strict pentru executarea lucrărilor menționate în autorizarea din partea responsabilului de securitate din cadrul entității.

## 10. Măsuri tehnice și organizatorice

Pentru a proteja securitatea sistemului de supraveghere prin mijloace video și pentru a spori gradul de protecție a vieții private, au fost introduse următoarele măsuri tehnice și organizatorice:

- limitarea timpului de stocare a materialului filmat, în conformitate cu cerințele de securitate și legislația în vigoare privind conservarea datelor.

- mediile de stocare (serverele pe care se stochează imaginile înregistrate) se află în spații securizate și protejate de măsuri de securitate fizică.
- toți utilizatorii cu drept de acces la sistemul de supraveghere prin mijloace video au semnat acorduri de confidențialitate, prin care se obligă să respecte prevederile legale în domeniu.
- utilizatorilor se acordă dreptul de acces doar pentru acele resurse care sînt strict necesare pentru îndeplinirea atribuțiilor de serviciu.
- doar administratorii de sistem numiți în acest sens de către operator, și responsabilul de securitate, au dreptul de a accesa fișierele înregistrate în sistem, la cererea conducerii unității.

I 4 1\_

## 11. Drepturi de acces

11.1. Accesul la imaginile stocate și/sau la arhitectura tehnică a sistemului de supraveghere prin mijloace video este limitat la un număr redus de persoane și este determinat prin atribuțiile specificate în fișa postului, în care este indicat în ce scop și ce tip de acces este acordat.

**11.2. PRIMĂRIA SATULUI ROGOJENI** impune limite stricte în privința persoanelor care au dreptul:

- să vizioneze materialul filmat în timp real: imaginile care se derulează în timp real sunt accesibile responsabililor de securitate și agenților de pază desemnați să desfășoare activitatea de supraveghere;
- să vizioneze înregistrarea materialului filmat: vizionarea imaginilor înregistrate se va face în cazuri justificate, cum ar fi cazurile prevăzute expres de lege și incidentele de securitate, de către persoanele special desemnate;
- să copieze, să descarce, să șteargă sau să modifice orice material filmat de sistemul de supraveghere prin mijloace video.

## 12. Instructaj

- Toți membrii personalului cu drepturi de acces beneficiază de o instruire inițială în domeniul protecției datelor.
- Această procedură va fi integrată în programul de instruire și îndrumare, pentru toți utilizatorii cu drept de acces și atribuții în operarea sistemului de supraveghere prin mijloace video.
- Șeful subdiviziunii va asigura că întregul personal din subordine, implicat în operarea sistemului de supraveghere prin mijloace video, este instruit și informat cu privire la toate aspectele funcționale, operaționale și administrative ale acestei activități.

## 13. Măsuri de păstrare a confidențialității

- Imediat după instructaj, fiecare participant cu drept de acces la sistemul de supraveghere prin mijloace video semnează un acord de confidențialitate.

## 14. Dezvăluirea datelor cu caracter personal

- Orice activitate de dezvăluire a datelor personale către terți va fi documentată și supusă unei analize riguroase privind pe de-o parte necesitatea comunicării, și pe de altă parte compatibilitatea dintre scopul în care se face comunicarea și scopul în care aceste date au fost colectate inițial pentru prelucrare.
- Orice situație de dezvăluire va fi consemnată de administratorul sistemului într-un Registru de evidență a cazurilor de dezvăluire.
- **PRIMĂRIA SATULUI ROGOJENI** are obligația punerii la dispoziția organelor judiciare, la

solicitarea scrisă a acestora, înregistrările video în care este surprinsă săvârșirea unor fapte de natură contravențională/penală.

- Sistemul de supraveghere prin mijloace video nu este utilizat pentru verificarea prezenței la program sau evaluarea performanței la locul de muncă.
- În cazuri excepționale, dar cu respectarea garanțiilor descrise mai sus, se poate acorda acces altor servicii din cadrul entității (Protecție Antiincendiară, Resurse Umane, Riscuri), în cadrul unei anchete disciplinare, de accidentare sau de securitate, cu condiția ca informațiile să ajute la investigarea unei infracțiuni, accident de muncă sau a unei abateri disciplinare de natură să prejudicieze drepturile și libertățile unei persoane fizice sau juridice.

## 15. Durata păstrării înregistrărilor video

- Durata păstrării înregistrărilor video este de 30 zile calendaristice, după care acestea se nimicesc automat în ordinea în care au fost înregistrate.
- În cazul producerii unui incident de securitate, durata de păstrare a înregistrărilor video poate depăși limitele admisibile de program, în funcție de timpul necesar investigării suplimentare a incidentului de securitate.

## 16. Informarea publicului referitor la supravegherea video

- Informarea publicului referitor la supravegherea video din cadrul **RIMĂRIEI SATULUI ROGOJENI** se efectuează prin pictograme.
- **PRIMĂRIA SATULUI ROGOJENI** garantează că asigură respectarea drepturilor ce revin persoanelor vizate, în conformitate cu legislația Republicii Moldova. Toate persoanele implicate în activitatea de supraveghere video și cele responsabile de administrarea imaginilor filmate, vor respecta procedurile și regulamentele de acces la date cu caracter personal ale entității.

## 17. Informarea persoanelor vizate

- Informarea primară a persoanelor vizate se realizează în mod clar și permanent, prin intermediul unui semn adecvat, cu vizibilitate suficientă și localizat în zona supravegheată, astfel încât să semnaleze existența camerelor de supraveghere, dar și pentru a comunica informațiile esențiale privind prelucrarea datelor cu caracter personal.
- Persoanele vizate sunt atenționate asupra existenței sistemului de supraveghere prin mijloace video și a proprietarului prin note de informare corespunzătoare, care cuprind scopul prelucrării și identifică **PRIMĂRIA SATULUI ROGOJENI** ca operator al datelor colectate prin intermediul supravegherii video.

## 18. Exercițarea drepturilor de acces, intervenție și opoziție

- Pe întreaga perioadă de stocare a datelor cu caracter personal, persoanele vizate au dreptul de acces la datele personale care le privesc deținute de **PRIMĂRIA SATULUI ROGOJENI**, de a solicita intervenția (ștergere/ actualizare/ rectificare/ anonimizare) sau de a se opune prelucrărilor, conform legii.
- Orice cerere de a accesa, rectifica, bloca și/sau șterge date cu caracter personal ca urmare a utilizării camerelor video ar trebui să fie adresată direct **PRIMĂRIEI SATULUI ROGOJENI**.
- În cazul în care persoana vizată are alte întrebări privind prelucrarea de către **PRIMĂRIA SATULUI ROGOJENI** a datelor personale care o privesc, se poate adresa conducerii **PRIMĂRIEI SATULUI ROGOJENI**.
- Răspunsul la solicitarea de acces, intervenție sau opoziție se dă în termen de 15 zile calendaristice. Dacă nu se poate respecta acest termen, persoana vizată va fi informată asupra motivului de amânare a

răspunsului, de asemenea i se va comunica și procedura care va urma pentru soluționarea cererii.

- Dacă există solicitarea expresă a persoanei vizate, se poate acorda dreptul de a vizualiza imaginile înregistrate care o privesc sau i se poate trimite o copie a acestora. Imaginile furnizate vor fi clare, în măsura posibilității, cu condiția de a nu prejudicia drepturile terților (persoana vizată va putea vizualiza doar propria imagine, imaginile altor persoanelor care pot apărea în înregistrare vor fi editate astfel încât să nu fie posibilă recunoașterea/identificarea lor). În cazul unei asemenea solicitări, persoana vizată este obligată:

a) să se identifice dincolo de orice suspiciune (să prezinte actul de identitate când participă la vizionare), să menționeze data, ora, locația și împrejurările în care a fost înregistrată de camerele de supraveghere.

b) De asemenea, persoana vizată va prezenta și o fotografie recentă astfel încât utilizatorii desemnați să o poată identifica mai ușor în imaginile filmate.

c) Persoana va putea vizualiza doar propria imagine, imaginile persoanelor care pot apărea în înregistrare vor fi editate astfel încât să nu fie posibilă recunoașterea/identificarea lor.

- Există posibilitatea refuzării dreptului de acces în situația în care se aplică excepțiile prevăzute de lege. Necesitatea de a restricționa accesul se poate impune și în cazul în care există obligația de a proteja drepturile și libertățile unor terțe persoane, de exemplu dacă în imagini apar și alte persoane și nu există posibilitatea de a obține consimțământul lor sau nu se pot extrage, prin editarea imaginilor, datele personale nerelevante.

## **19. Auditul securității sistemului de supraveghere prin mijloace video**

- Auditul securității sistemului de supraveghere prin mijloace video menține înscrisi de sistem despre evenimentele produse în activitatea sistemului sau a aplicației, precum și despre activitatea utilizatorului.
- În conjuncție cu instrumentele și procedurile respective, auditul securității sistemului de supraveghere prin mijloace video permite de a promova mijloace de ajutor pentru a atinge obiective de securitate: evidența acțiunilor utilizatorului, definirea și stabilirea responsabilității individuale, reconstrucția evenimentelor, detectarea intrușilor și problemelor de identificare a evenimentelor.
- Auditul securității sistemului de supraveghere prin mijloace video este menit să acorde suport la:
  - stabilirea consecutivității acțiunilor utilizatorului sau proceselor;
  - stabilirea când, cine sau ce a stopat funcționarea normală a sistemului;
  - soluționarea problemei de detectare a intrușilor;
  - detectarea problemelor de funcționare a sistemului informatic în regim On-Line;

### **Anexa 1**

#### **REGULAMENTUL PRIVIND SUPRAVEGHEREA PRIN MIJLOACE VIDEO ÎN CADRUL PRIMĂRIEI SATULUI ROGOJENI LISTA CU LOCAȚIILE PENTRU AMPLASAREA CAMERELOR DE SUPRAVEGHERE ÎN CADRUL PRIMĂRIEI SATULUI ROGOJENI**

Locațiile și spațiile de acces, destinate publicului de la parterul clădirilor;

1. 2 - camere video.

Locațiile din împrejurimile clădirilor pentru a proteja spațiile exterioare;

1. 3 - camere video exterioare.

Locațiile critice de amplasare a echipamentelor și sistemelor IT și de telecomunicații cu descrierea parametrilor tehnici cum ar fi:

Tipul camerei - IP

Rezoluția camerelor - conform tabelului

Nr. d/o	Denumirea	cant.	Poziția	Rezoluția
1.				
2.				
3.				
4.				
5.				
6.				
7.				

Tipul mediului de stocare (registrator sau cloud) - Registrator

**LISTA ANGAJAȚILOR FAMILIARIZAȚI CU PREVEDERILE  
REGULAMENTULUI PRIVIND SUPRAVEGHEREA  
PRIN MIJLOACE VIDEO ÎN CADRUL  
PRIMĂRIEI SATULUI ROGOJENI**

Numele, prenumele	Funcția	Am luat cunoștință (semnătura)	Data
Groza Ruslan	primar		
Ardeleanu Viorica	secretara consiliului		
Guzun Ana	contabila - șefa		
Odagiu Maria	specialistă		
Iacurinscaia Olga	Muncitoare auxiliară		
Ianciu Dumitru	Muncitor auxiliar		
Fosa Svetlana	Muncitoare auxiliară		
Iacurinscaia Olga	Îngrijitoare de încăperi		