REPUBLICA MOLDOVA

RAIONUL ŞOLDĂNEŞTI
CONSILIUL SĂTESC ROGOJENI

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

РЕСПУБЛИКА МОЛДОВА

РАЙОН ШОЛДЭНЕШТЬ
СЕЛЬСКИЙ СОВЕТ
РОГОЖЕНЬ

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

PROIECT

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 administraţia publică locală, Legii nr.71/2007 cu privire la register, Legii nr.133/2011 privind protecţia datelor cu caracter personal , Instrucţiunilor privind ţinerea lucrărilor de secretariat referitoare la petiţiile persoanelor fizice şi juridice, adresate organelor de stat, întreprinderilor, instituţiilor şi organizaţiilor Republicii Moldova, aprobate prin Hotărîrea Guvernului nr.208 din 31.03.1995, cerinţelor faţă de asigurarea securităţii datelor cu caracter personal, aprobate prin Hotărîrea Guvernului nr.1123 din 14.12.2010 , Consiliul sătesc Rogojeni

D E C I D E :

1. Se aprobă următoarele acte normative interne în domeniul prelucrării datelor cu caracter personal:
   1.1. Regulamentul privind prelucrarea informaţiilor ce conţin date cu caracter personal în sistemul de evidenţă al corespondenţei şi petiţiilor parvenite în adresa Primăriei satului Rogojeni.
   1.2. Regulamentul privind prelucrarea informaţiilor ce conţin date cu caracter personal în sistemul de evidenţă a resurselor umane în cadrul Primăriei satului Rogojeni.
   1.3. Regulamentul privind prelucrarea informaţiilor ce conţin date cu caracter personal în sistemul de evidenţă contabilă în cadrul Primăriei satului Rogojeni.
   1.4. Politică privind protecţia datelor cu caracter personal în cadrul Primăriei satului Rogojeni.
   1.5. Politică de confidenţialitate privind prelucrarea datelor personale ale angajaţilor şi potenţialilor angajaţi 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 informaţiilor ce conţin date cu caracter personal în sistemul de evidenţă supraveghere video.

2. Se desemnează primarul satului în calitate de persoană responsabilă de protecţia datelor cu caracter personal în cadrul Primăriei satului Rogojeni şi de implementarea politicii de securitate a sistemului de informaţii şi mijloace.
3. Prezenta decizie se publică în Registrul de stat al actelor locale, se aduce la cunoştinţa angajaţilor contrasemnătură şi se plasează pentru informare publică pe pagina oficială a Primăriei Rogojeni în reţeaua internet: WEB: www.rogojeni.sat.md .
4. Controlul executării prezentei decizii se atribuie primarului Ruslan Groza.

AU VOTAT: pentru -, contra - s-au abţinut -

Autor : Primarul s. Rogojeni Groza Ruslan
Tel : (0272 - 63) 2-36, primaria.rogojeni@apl.gov.md

Contrasemnat : Secretarul 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 şi 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 şi 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 şi 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 şi juridice, adresate organelor de stat, întreprinderilor, instituțiilor şi organizațiilor Republicii Moldova, aprobate prin Hotărîrea Guvernului nr.208 din 31.03.1995, cerințelor față de asigurarea securității datelor cu character personal, aprobate prin Hotărîrea Guvernului nr.1123 din 14.12.2010.
7. Avizarea şi consultarea publică a proiectului Anunțul despre inițierea proiectului de Decizie se publică pe site-ul official al Primăriei WEB : rogojeni.sat.md ;
8. Constatările expertizei anticorupție - Nu necesită
9. Constatările expertizei de compatibilitate - Nu necesită

Secretara consiliului Ardeleanu Viorica

Anexa nr.1
la decizia nr.1/13
din ____ 2025

REGULAMENTUL
privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență al corespondenței şi 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 şi petițiilor parvenite în adresa Primăriei satului Rogojeni (Regulamentul) este elaborat în conformitate cu prevederile Codului administrativ al Republicii Moldova, aprobat prin Legea пr. 116 din 19 iulie 2018, Legii nr. 7l-XVI din 22 martie 2007 cu privire la registre, Legii nr.133 din 8 iulie 2011 privind protectia datelor cu caracter personal,Instrucțiunilor privind ținerea lucrărilor de secretariat referitoare la petițiile persoanelor fizice şi juridice, adresa organelor de stat, întreprinderilor, instituțiilor şi organizațiilor Republicii Moldova, aprobate prin Hotărirea Guvernului nr. 208 din 31 martie 1995, Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora iп cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărirea Guvernului пr. 1123 din 14 decembrie 2010.

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

3. Noțiunile utilizate iп prezentul Regulament au semnificația prevăzută de Legea cu privire la registre, Codului administrativ al Republicii Moldova, aprobat prin Legea nr.116 din l9 iulie 2018, Legea privind protecția datelor cu caracter personal, Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora in 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 persoaпй 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 urmăreşte realizarea de către autoritatea publică a uпor acțiuni de interes public;

Registrul de evidență a corespondenței - resursa informațională specializată (totalitatea informațiilor ținute în formă automatizată şi manuală) care asigură evidența informației sistematizate, principalul obiectiv al căruia consta în asigurarea evidenței corespondenței parvenite la Centrul de Informare şi 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 iп modul stabilit de lege sau acord.

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

- Primăria satului Rogojeni, în calitate de proprietar şi deținător al Registrului;
- persoanele împuternicite de ținerea Registrului şi 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 şi vizualiza datele din Registru.

5. Angajaţii Primăriei satului Rogojeni poartă răspundere personală pentru îndeplinirea cerinţelor prezentului Regulament, asigurarea confidenţialităţii, securităţii şi păstrarea în stare corespunzătoare a informaţiei din Registru.

5.1. Petiţiile 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. Condiţii generale faţă de ţinerea sistemului de evidenţă a corespondenţei şi petiţiilor (Registrul)

6. Registrul de evidenţă a corespondenţei şi petiţiilor reprezintă un sistem mixt ce utilizează atât evidenţa în formă electronică, cît şi în formă manuală.

7. De către persoana împuternicită de ţinerea Registrului din cadrul Primăriei va fi asigurată ţinerea în formă manuală a unor componente al Registrului (ţinând cont de competenţa funcţională) prin înscrierea informaţiei, inclusiv păstrarea cărţii Registrului de către angajat împuternicit în acest sens (registratorul) din cadrul subdiviziunii respective, în conformitate cu prevederile legislaţiei în vigoare.

8. Persoana responsabilă din cadrul Primăriei va asigura suplimentar, evidenţa în formă electronică a corespondenţei şi petiţiilor parvenite la Primăria satului Rogojeni.

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

10. Registrul va ţinut în limba de stat.

11. Registratorul este obligat:

- să introducă în Registru numai informaţie veridică, colectată de la adresant sau din alte surse interzise de lege;
- să asigure evidenţa în ordine cronologică a fiecărei înscrieri în Registru;
- să nu admită modificarea neîntemeiată a datelor introduse în Registru;
- să efectueze înregistrările în Registru astfel, încît să excludă posibilitatea de a fi radiată (ştearsă, distrusă) în mod mecanic, chimic sau în orice alt mod, fără a lăsa urme vizibile ale radierii (ştergerii, distrugerii);
- să asigure accesul la informaţia din registru doar persoanelor care au dreptul de a primi informaţia respectivă, în conformitate cu legislaţia 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 şi actuală a informaţiei privind persoanele care s-au adresat la primăria satului Rogojeni.

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

- denumirea registrului;
- denumirea Primăriei satului Rogojeni ca proprietar, posesor şi deţinător al Registrului;
- numele, prenumele şi funcţia persoanei responsabile de introducerea datelor în Registru şi a administratorului acestuia;
- numele, prenumele şi funcţia persoanei care va exercita controlul asupra ţinerii Registrului;
- numărul Registrului, termenile de ţinere şi păstrare a acestora.

14. Datele cu caracter personal din Registru vor fi prelucrate în condiţiile stabilite de legislaţia privind protecţia datelor cu caracter personal. În acest sens, vor fi realizate măsuri de asigurare a gradului de executare a datelor registrului şi de protecţie a acestora contra distrugerii întâmplătoare sau neautorizate, modificării, dezvăluirii sau oricăror alte acţiuni ilegale la ţinerea registrului.

15. Prelucrarea datelor cu caracter personal în sistemul de evidenţă al corespondenţei şi petiţiilor parvenite în adresa Primăriei satului Rogojeni, se efectuează în conformitate cu prevederile art.5 alin.(5) lit.b), d), şi e) al Legii privind protecţia datelor cu caracter personal.

III. Condiţii generale privind introducerea informaţiei în Registru

16. Informaţia privind corespondenţa parvenită în adresa Primăriei satului Rogojeni va fi recepţionată şi înregistrată în aceiaşi zi de persoana responsabilă din cadrul entităţii şi după caz, în fişele de evidenţă

şi 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) şi în Sistemul informatic (formă electronică) în baza datelor furnizate prin documentele transmise atît de furnizorul datelor registrului (petiționarul agentul economic, autoritatea publică), atât pe suport de hîrtie sau în formă electronică, perfectate în modul stabilit de lege.

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

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

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

21. Modificările şi radierile făcute în Registru se efectuează în baza decizie şi 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 şi va informa despre aceasta furnizorul datelor.

23. Greşelile de ordin tehnic de către persoana împuternicită de ținerea Registrului se rectifică de către acesta. Corectarea greşelii 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 şi data radierii) şi nu reprezintă excluderea fizică a datelor despre obiect din Registru.

25. Rectificările şi radierile inscrierilor din Registru se efectuează astfel încît textul inițial să fie citibil.

IV. Condiții generale privind păstrarea şi 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 decât pe perioada stabilita de lichidatorul documentelor-tip şi a termenilor lor de păstrare pentru organele administrației publice, pentru instituțiile, organizațiile şi întreprinderile Republicii Moldova, aprobat de Serviciul de Stat de Arhivă nr.57 din 27.07.2016.

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

28. În acest sens, persoana împuternicită de ținerea şi 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 şi 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 şi alte persoane, care au dreptul de a primi informația respectivă, în conformitate cu legislația în vigoare sau care demonstrează dreptul şi 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 / peti|iilor*
- *Registrul cererilor de comunicare a informațiilor de interes public*
- *Registrul documentelor intrate*
- *Registrul documenteIor expediate*
- *Registrul evidensei declarațiilor (de cdsătorie, de paternitate, Cereri de mamă solitară)*
- *Registrul Declarațiilor de nastere a copilului*
- *Registrul de evidență a certɒcatelor de Stare Civilă eliberate de primăria Rogojeni*
- *Registrul de evidență a declarațiilor de primire in 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 tnregistrare a contractelor de arendă a terenurilor private*
- *Registru de evidență a contribuabililor la impozitele funciare și pe bunurile imobiliare*
- *Registru conturilor personaIe 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, încleierea 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 şi 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 şi păstrarea informației în acest Registru este asigurată de registratorul desemnat din cadrul Centrului de Informare şi Prestări Servicii.

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

-tipul adresării;
-data şi numărul de intrare;
-termenul de rezolvare şi 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 şi 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 şi petițiilor.

40.1. Sistemul informațional de evidență al corespondenței şi 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 Hotărîrea 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 şi petițiilor

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

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

43. Accesul fizic la mijloacele de reprezentare a informației preluate din sistemul de evidență a corespondenței şi 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 şi introducerea mijloacelor de prelucrare a informațiilor din sistemul de evidență a corespondenței şi 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 şi petițiilor, se înfăptuiesc ținând cont de necesitatea asigurării confidențialității şi integrității acestora, prin protecție în formă manuală, electronică şi externă.

47. Cerinţe speciale faţă de marcare: toate informaţiile ieşite din sistemul de evidenţă a corespondenţei şi petiţiilor, care conţin date cu caracter personal, sînt supuse marcării, cu indicarea numărului de identificare unic al operatorului de date cu caracter personal.

Model- Atenţie! Documentul conţine date cu caracter personal. Prelucrarea ulterioară a acestor date poate fi efectuată numai în condiţiile prevăzute de Legea privind protecţia datelor cu caracter personal nr.133 din 08.07.2011.

48. Accesul la biroul unde este amplasat sistemul de evidenţă a corespondenţei şi petiţiilor este restricţionat, fiind permis doar persoanele care au autorizaţia necesară şi doar în timpul orelor de program. Accesul în birou este posibil doar cu autorizarea de acces şi/sau cheia de la lacătul mecanic.

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

50. Înainte de acordarea accesului fizic la sistemul de evidenţă a corespondenţei şi petiţiilor, se verifică competenţele de acces.

51. Registrele de monitorizare se păstrează minimum un an, la expirarea termenului indicat, acesta se lichidează, iar datele şi documentele ce se conţin în registrul supus lichidării se transmit în arhivă, conform cerinţelor prevăzute în instrucţiunile cu privire la ţinerea lucrărilor de secretariat.

52. Perimetrul de securitate se consideră perimetrul biroului în care este amplasat sistemul de evidenţă a corespondenţei şi petiţiilor, fiind integru din punct de vedere fizic.

53. Zilnic se inspectează perimetrul de securitate al clădirii şi al biroului, unde este amplasat sistemul de evidenţă a corespondenţei şi petiţiilor, din punct de vedere fizic.

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

55. Uşile şi ferestrele sunt încuiate în cazul în care în încăpere lipsesc angajaţii autorizaţi de administrarea sistemului.

56. Amplasarea sistemului de evidenţă a corespondenţei şi a petiţiilor răspunde necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.

57. Securitatea electroenergetică: este asigurată securitatea echipamentului electric utilizat pentru menţinerea funcţionalităţii sistemului de evidenţă a corespondenţei şi petiţiilor, a cablurilor electrice, inclusiv protecţia acestora contra deteriorărilor şi conectărilor nesancţionate. În cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, este asigurată posibilitatea deconectării electricităţii la registru, inclusiv posibilitatea deconectării oricărui component TI.

58. Computerele, unde este amplasat fizic sistemul de evidenţă a corespondenţei şi petiţiilor, 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 reţea: cablurile de reţea, prin care se efectuează operaţiunile de transmitere a datelor preluate din sistemul de evidenţă a corespondenţei şi petiţiilor, sînt protejate contra conectărilor nesancţionate sau deteriorărilor. Pentru a exclude bruiajul, cablurile de tensiune sînt separate de cele comunicaţionale.

60. Securitatea antiincendiară a sistemului de evidenţă a corespondenţei şi petiţiilor: biroul unde este amplasat registrul este dotat cu echipament antiincendiar şi corespunde cerinţelor şi normelor antiincendiare în vigoare.

61. Controlul instalării şi scoaterii componentelor TI: se efectuează controlul şi evidenţa instalării şi scoaterii mijloacelor de program, mijloacelor tehnice şi celor tehnice de program, utilizate în cadrul sistemului de evidenţă a corespondenţei şi petiţiilor. La expirarea termenului de păstrare, informaţiile, care conţin date cu caracter personal şi care se conţin pe purtătorii de informaţii se distrug.

VIII. Identificarea şi autentificarea utilizatorului sistemului de evidenţă a corespondenţei şi petiţiilor

62. Este efectuată identificarea şi autentificarea utilizatorilor informaţiilor preluate din sistemul de evidenţă a corespondenţei, petiţiilor şi a proceselor executate în numele acestor utilizatori.

63. Toţi utilizatorii (inclusiv administratorii de reţea, programatorii şi administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului) care nu trebuie să conţină semnalmentele nivelului de accesibilitate al utilizatorului.

64. Pentru confirmarea ID-ului utilizatorului sînt utilizate parole. Utilizarea parolelor în procesul asigurării securității informaționale: pe lîngă 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, şi, ca urmare, noile sarcini nu necesită accesul la datele cu caracter personal, precum şi în cazul de modificare a drepturilor de acces ale utilizatorului, abuz al utilizatorului de 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 şi autentificare se revocă sau se suspendă.

67. Folosirea tehnologiilor fără fir, echipamentelor portative şi mobile se autosesizează 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 şi supusă unei analize riguroase în prealabil privind scopul şi 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 şi 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 şi că folosirea neautorizată a acestora este sancționată în conformitate cu legislația civilă, contravențională şi penală.

IX. Auditul securității în sistemul de evidență a corespondenței şi petițiilor

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

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

a) data şi numărul tentativei/ieşirii;
b) ID-ul utilizatorului.

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

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

75. Cazurile de deranjament al auditului securității în sistemul de evidență a corespondenței şi petițiilor sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, sînt aduse la cunoştința 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 şi petițiilor (operațiunile de prelucrare a informațiilor şi mijloacele de efectuare a auditului), se protejează contra accesului neautorizat prin aplicarea măsurilor de securitate adecvate şi asigurarea confidențialității şi integrității acestora.

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

X. Asigurarea integrității informațiilor din sistemul de evidență a corespondenței şi petițiilor

78. Copiile de siguranță a informațiilor din sistemul de evidență a corespondenței, petițiilor şi soft-urilor folosite pentru prelucrările automatizate a acestora vor fi efectuate în regimul automat, zilnic, reeşind din volumul prelucrărilor efectuate. Copiile de siguranță se testează în scopul verificării siguranței purtătorilor de informații şi integrității informației indicate. Procedurile de restabilire a copiilor de siguranță se actualizează şi se testează cu regularitate, în scopul asigurării eficacității acestora.

XI. Gestionarea incidentelor de securitate a sistemului de evidență a corespondenței şi petițiilor

79. Persoanele care asigură exploatarea sistemului de evidență a corespondenței şi petițiilor trec, minimum o dată în an instruirea cu privire la responsabilitățile şi obligațiile în cazul executării acțiunilor de gestionare şi reacționare la incidentele de securitate.

80. Prelucrarea incidentelor de securitate include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor şi restabilirea securității. Se monitorizează şi documentează, în mod permanent, incidentele de securitate în sistemul de evidență a corespondenței şi 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 şi 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 şi să asigure accesul la informațiile necesare relevante obiectului controlului.

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

XII. Dispoziții finale

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

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

85. Regulamentul este adus la cunoştința angajaților contra semnătură.

86. Modificarea şi 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 şi petițiilor parvenite în adresa Primăriei satului Rogojeni

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

Anaxa nr.2
la decizia nr._1/13
din 25.02.2025

REGULAMENT
Cu privire la asigurarea securității datelor cu caracter personal
în sistemul de avidență 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 stabulește 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 sudiviziunile 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 şi normele legale stabilite prin prevederile Legii nr.133 din 8 iulie 2011 privind protecția datelor cu caracter personal, Hotărîrii 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 şi 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 şi a prezentării rapoartelor trimestriale şi 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 şi locul naşterii;*
- *Cetățenia;*
- *IDNP;*
- *Imagine;*
- *Situația familiară;*
- *Situația militară;*
- *Datele personale ale membrilor de familie;*
- *Datele din permisul de conducere;*
- *Datele pentru transferul pe contul bancar a plăților salariale şi 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/reşedinţei);*
- *adresa e-mail;*
- *profesia şi/sau locul de muncă;*
- *formarea profesională - diplome - studii;*
- *numele, prenumele (după caz, patronimicul) persoanelor care se află la întreţinerea persoanei respective (membrii familiei, alte rude şi persoane, după caz);*
- *mărimea concretă a drepturilor salariale calculate, taxele şi impozitele aferente, inclusiv contribuţiile de asigurări sociale obligatorii de asistenţă medicală şi socială, şi alte sume datorate în virtutea legii sau contractului;*
- *datele din certificatele de concediu medical acordate, necesare pentru calcularea indemnizaţiei corespunzătoare;*
- *informaţii de recrutare (inclusiv copii ale diplomelor de studii, referinţe şi alte informaţii incluse într-un CV sau scrisoare de intenţie ca parte a procesului de aplicare);*
- *Informaţii despre utilizarea de către angajat a sistemelor noastre de informare şi comunicaţii;*
- *după caz, alte date necesare îndeplinirii scopului menţionat, conform legislaţiei în vigoare.*

5. Prelucrarea datelor cu caracter personal menţionate va fi efectuată pentru realizarea următoarelor scopuri:

a) prelucrarea informaţiei privind modificările survenite la prelucrarea datelor cu caracter personal ce vizează angajaţii şi care au impact asupra executării contractului individual de muncă;

b) stabilirea sistemului de salarizare a personalului în conformitate cu legislaţia în vigoare a Republicii Moldova;

c) prelucrarea certificatelor de concedii medicale ale angajaţilor în vederea stabilirii indemnizaţiilor corespunzătoare;

d) elaborarea, înregistrarea şi prelucrarea ordinelor rectorului referitor la personal;

e) prezentarea la CNAM a evidenţei nominale a noilor angajaţi şi a celor concediaţi, format hârtie şi format electronic;

f) înregistrarea şi prelucrarea dosarelor pentru concursul de suplinire a posturilor vacante;

g) întocmirea declaraţiei persoanei asigurate REV 1 pentru fiecare angajat şi transmiterea acestora Casei Teritoriale de Asigurări Sociale, Centru pe suport de hârtie;

h) asistarea procesului (prin furnizarea informaţiei necesare) pentru completarea periodică (lunară) a raportului şi dării de seamă privind venitul achitat şi impozitul pe venit reţinut din acesta;

i) completarea lunară, trimestrială şi anuală a rapoartelor statistice referitoare la personalul primăriei;

j) prelucrarea cererilor şi a documentelor necesare executării contractelor individuale de muncă;

k) eliberarea certificatelor care atestă calitatea de salariat al primăriei la cererea angajaţilor;

l) ţinerea dosarelor personale ale salariaţilor;

m) înregistrarea datelor în carnetele de muncă;

n) alte scopuri, necesare realizării activităţilor ce ţin 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/şterge, în funcţie de suportul pe care au fost efectuate. în cazul obligaţiilor 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 evidenţă a Resurselor Umane în alte scopuri decât cele menţionate mai sus este interzisă.

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

III. LOCAŢIA ŞI DESCRIEREA SISTEMULUI DE EVIDENŢĂ A RESURSELOR UMANE

9. Datele cu caracter personal conţine în sistemul de evidenţă a Resurselor Umane în cadrul entităţii se prelucrează şi se stochiază:
1) pe suport de hîrtie;
2) în format electronic:
a)Software – Sistemul de evidenţă a resurselor umane: 1C –BIT SECRETAR
b) Hardware –Nr. de inventariere 31460024.

10. Prelucrarea informaţiilor în sistemul de evidenţă resurse umane pe suport de hîrtie este structurată după criteriul „mape-dosare", fiind păstrate în dulapuri, care sânt amplasate fizic în biroul specialistului resurse umane a Primăriei satului Rogojeni, raionul Şoldăneşti, s.Rogojeni, MD-7230.

IV. DURATA DE STOCARE

11. Prelucrarea datelor cu caracter personal în sistemul de evidenţă a Resurselor Umane se efectuează pe perioada activităţii angajaţilor primăriei, la expirarea termenilor menţionate datele din sistemul de evidenţă a angajaţilor primăriei sunt păstrate în formă arhivată pe perioada stabilită în Nomenclatorul dosarelor în cadrul primăriei. Actele normative ce reglementează regimul juridic şi termenele de păstrare. Dosarele de concurs ale candidaţilor la funcţiile 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 funcţia publică şi statutul funcţionarului public, după care sunt nimicite prin proces verbal. Prelucrarea datelor cu caracter personal în sistemul de evidenţă a datelor privind gestionarea resurselor umane se efectuează pe perioada activităţii angajaţilor.

Datele cu caracter personal a potenţialilor angajaţi se preia din CV-ul transmis de către aceştia la adresa de e-mail. După primirea CV-ului prin intermediul poştei electronice, acesta se tipăreşte pe suport de hârtie, iar de pe adresa electronica se şterge. în cazul în care rezultatul în privinţa angajării persoanei a cărei date cu caracter personal au fost prelucrate, este negativ, CV-ul se distruge

12. La expirarea termenilor menţionaţi datele din sistemul de evidenţă 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 ANGAJAŢILOR SI PERSOANELOR VIZATE

13.Primăria în calitate de operator de date cu caracter personal, garantează respectarea drepturilor privind protecţia datelor cu caracter personal ce le revin angajaţilor, precum şi, după caz, altor persoane vizate.
14. In conformitate cu principiile de protecţie a datelor cu caracter personal, persoanele vizate beneficiază de următoarele drepturi: la informare, de acces la date, de intervenţie, de opoziţie asupra datelor cu caracter personal ce-i vizează, precum şi dreptul de a se adresa injustiţie.
15. Toate persoanele implicate în activitatea de administrare şi/sau prelucrare a informaţiilor din sistemul de evidenţă a Resurselor Umane vor respecta procedura de acces la datele cu caracter personal.
16. Acordarea dreptului de acces al angajaţilor la informaţiile ce-i vizează se efectuează doar prin solicitarea expresă, în formă scrisă, cu acordul nemijlocit al primarului. Informaţiile furnizate vor fi acordate astfel, încât să nu prejudicieze drepturile terţilor. Persoanele care solicită date cu caracter personal trebuie să indice scopul solicitării, precum şi perioada concretă pentru care solicită informaţiile.

17. Există posibilitatea refuzării dreptului de acces în 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 înfăptuiesc 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.22. Înainte de acordarea accesului fizic la sistemul de evidență a Resurselor Umane se verifică competențele de acces.
23. Registrele de monitorizare se păstrează minimum un an, la expirarea termenului indicat, acestea se lichidează, iar datele si 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 încăpere lipsesc angajații autorizați de administrarea sistemului.
27. Amplasarea sistemul 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 sistemul de evidentă a Resurselor Umane, a cablurilor electrice,

inclusiv protecţia acestora contra deteriorărilor şi conectărilor nesancţionate. In cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, este asigurată posibilitatea deconectării electricităţii la sistemul de evidenţă a Resurselor Umane, inclusiv posibilitatea deconectării oricărui component TI.

29. Computerele, unde este amplasat fizic sistemul de evidenţă 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 reţea: cablurile de reţea, prin care se efectuează operaţiunile de transmitere a datelor preluate din sistemul de evidenţă a Resurselor Umane, sunt protejate contra conectărilor nesancţionate sau deteriorărilor. Pentru a exclude bruiajul, cablurile de tensiune sunt separate de cele comunicaţionale.

31. Securitatea anti incendiară a sistemul de evidenţă a Resurselor Umane: biroul unde este amplasat sistemul de evidenţă a Resurselor Umane este dotat cu echipament anti incendiar şi corespunde cerinţelor şi normelor anti incendiare în vigoare.

32.Controlul instalării şi scoaterii componentelor TI: se efectuează controlul şi evidenţa instalării şi scoaterii mijloacelor de program, mijloacelor tehnice şi celor tehnice de program, utilizate în cadrul sistemul de evidenţă a Resurselor Umane. La expirarea termenului de păstrare, informaţiile, care conţin date cu caracter personal şi care s conţin pe purtătorii de informaţii, se distrug.

VI. AUDITUL SECURITĂŢII ÎN SISTEMUL DE EVIDENŢĂ A RESURSELOR UMANE

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

34. înregistrările de audit a securităţii Sistemului de Evidenţă al Resurselor Umane în care sînt prelucrate date cu caracter personal, trebuie să conţină:

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

35. Rezultatele auditului securităţii în Sistemul de Evidenţă al Resurselor Umane (operaţiunile de prelucrare a informaţiilor şi mijloacele de efectuare a auditului), se protejează contra accesului neautorizat prin aplicarea măsurilor de securitate adecvate şi asigurarea confidenţialităţii şi integrităţii acestora.

36. Durata minimă a stocării rezultatelor auditului securităţii în Sistemul de Evidenţă al Resurselor Umane constituie 2 */doi/* ani, în scopul asigurării posibilităţii de folosire a acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigaţii sau procese judiciare. în cazul în care investigările sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

V. GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMULUI DE EVIDENŢĂ A RESURSELOR UMANE

37.Persoanele care asigură exploatarea sistemul de evidenţă a Resurselor Umane trec, minim o dată în an, instruirea cu privire la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate.

38. Prelucrarea incidentelor de securitate include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii. Se monitorizează şi documentează, în mod permanent, incidentele de securitate în sistemul de evidentă a Resurselor Umane.

39. Persoanele care se fac vinovate de încălcarea normelor privind obţinerea, păstrarea, prelucrarea şi protecţia informaţiilor din sistemul de evidenţă a Resurselor Umane poartă răspundere civilă, contravenţională şi penală.

40. „In cazul producerii incidentelor de securitate, persoanele responsabile vor întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia şi va înlătura cauzele incidentului de securitate cu informarea în termen de 72 ore din momentul producerii incidentului de securitate a Centrului Naţional pentru Protecţia Datelor cu Caracter Personal al Republicii Moldova. Totodată, în cadrul controalelor efectuate de Centrul Naţional pentru Protecţia Datelor cu Caracter Personal, persoanele responsabile sânt obligate să ofere suportul necesar şi să asigure accesul la informaţiile necesare relevante obiectului controlului."

VI. DISPOZIŢII FINALE

41. Prezentul Regulament este aprobat de către organul de conducere al **PRIMĂRIEI SATULUI ROGOJENI** şi revizuit periodic, la necesitate, în cazul modificării legislaţiei în vigoare.

42. Prezentul Regulament se completează cu prevederile legislaţiei în vigoare.

43. Modificarea şi completarea prezentului Regulament se face în modul stabilit pentru aprobarea acestuia.

LISTA ANGAJAŢILOR FAMILIARIZAŢI CU PREVEDERILE REGULAMENTULUI cu privire la asigurarea securităţii datelor cu caracter personal în sistemul de evidenţă a resurselor umane în cadrul Primăriei Rogojeni raionul Şoldăneşti

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

Anexa nr.3
la Decizia nr.1/13
din 25.02.2025

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 conţin date cu caracter personal în sistemul de evidenţă 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 şi a Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărîrea Guvernului nr.l 123 din 14 decembrie 2010, precum şi întru respectarea prevederilor art. 91 - 94 ale Codului muncii al Republicii Moldova.

1.2. Prezentul Regulament reglementează condiţiile generale şi cerinţele faţă de prelucrarea datelor cu caracter personal ale angajaților **PRIMĂRIEI SATULUI ROGOJENI** în cadrul sistemului de evidenţă contabilă.

II. SCOPUL

2.1. Scopul prelucrării informaţiilor ce conţin date cu caracter personal în sistemul de evidenţă contabilă constă în asigurarea înregistrării informaţiilor contabile referitoare la calculul drepturilor salariale ale angajaţilor, inclusiv a premiilor, stimulărilor, sporurilor, indemnizaţiilor, compensaţiilor şi altor drepturi şi obligaţii cu conţinut pecuniar, precum şi a prezentării rapoartelor financiare, trimestriale şi anuale către instituţiile statului, conform legislaţiei în vigoare.

2.2. Prelucrarea datelor cu caracter personal în sistemul de evidenţă contabilă se efectuează în conformitate cu prevederile art. 5 alin. 5 lit. a), b) şi e) al Legii privind protecţia datelor cu caracter personal.

2.3. în cadrul sistemului de evidenţă contabilă sânt prelucrate următoarele categorii de date cu caracter personal:

- numele, prenumele şi patronimicul;
- sexul;
- numărul personal de identificare de stat (IDNP);
- data naşterii şi domiciliul;
- telefon mobil/fix/fax;
- semnătura/semnătura digitala;

- date din acte de stare civilă,
- profesie, funcţie
- formare profesională, diplome, studii
- cetăţenia;
- situaţie economica sau financiara;
- imagine;
- date bancare,
- date din permisul de conducere
- sancţiuni disciplinare
- codul personal de asigurări sociale (CPAS);
- codul personal de asigurări medicale (CPAM);
- adresa domiciliului,reşedinţei,
- datele privind locul de muncă,
- mărimea salariului brut şi alte premii, sporuri, stimulări,
- datele privind situaţia familială ;
- datele din certificatele de concediu medical

2.4. Prelucrarea datelor cu caracter personal menţionate va fi efectuată pentru realizarea următoarelor scopuri:

a) Prelucrarea informaţiei privind modificările survenite la prelucrarea datelor cu caracter personal ce vizează angajaţii **PRIMĂRIEI SATULUI ROGOJENI** şi care au impact asupra calculării plăţilor salariale, precum şi a persoanelor fizice şi juridice cu care **PRIMĂRIA SATULUI ROGOJENI** intră în relaţii contractuale;

b) Calcularea drepturilor salariale lunare, în conformitate cu legislaţia în vigoare a Republicii Moldova (conform contractelor individuale de muncă, contractelor civile, tabelelor de pontaj, ordinelor/dispoziţiilor conducerii, raportului de activitate lunară);

c) Prelucrarea certificatelor de concedii medicale ale angajaţilor în vederea stabilirii indemnizaţiilor de incapacitate temporară de muncă;

d) Prelucrarea copiilor ordinelor/dispoziţiilor conducerii referitoare la personal;

e) Calcularea şi reţinerea taxelor ce ţin de plăţile salariale aferente angajaţilor: primele de asigurare obligatorie de asistenţă medicală, contribuţiile la bugetul asigurărilor sociale de stat, impozitul pe venit, etc.;

f) Calcularea şi virarea primelor de asigurare obligatorie de asistenţă medicală şi a contribuţiilor la bugetul asigurărilor sociale de stat, aferente plăţilor salariale - obligaţie a angajatorului;

g) Furnizarea informaţiei necesare pentru elaborarea rapoartelor lunare privind contribuţiile de asigurare socială de stat obligatorii (forma IPC 18) şi rapoartelor trimestriale privind primele de asigurare obligatorie de asistenţă medicală (forma IPC 18);

h) întocmirea, lunară, a declaraţiei persoanei asigurate REV 5 pentru fiecare angajat şi transmiterea acestora Casei Teritoriale de Asigurări Sociale, în format electronic prin SIA E- REPORTING cu aplicarea semnăturii digitale;

i) Asistarea procesului (prin furnizarea informaţiei necesare) pentru completarea periodică (lunară) a raportului şi dării de seamă privind venitul achitat şi impozitul pe venit reţinut din acesta;

j) Completarea lunară, trimestrială şi anuală a dărilor de seamă cu prezentarea acestora Inspectoratului Fiscal de Stat, precum şi perfectarea şi eliberarea informaţiei privind veniturile

k) calculate şi achitate în folosul persoanei fizice şi impozitul pe venit reţinut din aceste venituri angajaţilor **PRIMĂRIEI SATULUI ROGOJENI;**

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

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

n) Completarea şi stocarea fişelor personale de evidenţă a veniturilor sub formă de salariu şi alte plăţi efectuate de către patron în folosul angajatului pe fiecare an, precum şi a impozitului pe venit reţinut din aceste plăţi (Anexa nr. 8 la Ordinul IFPS nr.676 din 14.12.2007);

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

p) Prezentarea documentelor financiare ce conţin date cu caracter personal către acţionari/fondatori, comisiei de cenzori, auditului intern sau extern. în cazul datelor cu caracter personal ale angajaţilor sau ale altor persoane, **PRIMĂRIA SATULUI ROGOJENI** se află în relaţie juridică, îi va înştiinţa pe aceştia atunci când datele respective vor fi transmise către terţi;

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/şterge, în funcţie de suportul pe care au fost efectuate. în cazul obligaţiilor 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 evidenţă contabilă în alte scopuri decât cele menţionate mai sus este interzisă.

III. LOCAŢIA ŞI DESCRIEREA SISTEMULUI DE EVIDENŢĂ CONTABILĂ

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

1. pe suport de hârtie;
2. în format electronic:

- Software - Sistemul de evidenţă contabilă IC- 2.098
- Hardware - Calculator cu Nr. de inventariere: nr. _____

3.2 Prelucrarea informaţiilor în sistemul de evidenţă contabilă pe suport de hârtie este structurată după criteriul "mape-dosare", fiind păstrate în dulapuri, care sînt amplasate fizic în biroul contabilităţii **PRIMĂRIEI SATULUI ROGOJENI rnl. ŞOLDĂNEŞTI, s. Rogojeni, MD-7230.**

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

Efectuarea ajustărilor în program, în baza modificărilor legislaţiei Republicii Moldova; Eliminarea erorilor în funcţionarea programului;

Consultarea în rezolvarea dificultăţilor apărute în utilizarea programului;

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

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

Examinarea şi nedivulgarea informaţiei 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 evidenţă contabilă se efectuează pe perioada valabilităţii contractelor de achiziţie publică, pe perioada activităţii angajaţilor Primăriei (din momentul semnării contractului până la finalizarea efectuării acţiunilor prevăzute de actele legislative în cazul încetării raporturilor de muncă).

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

V. DREPTURILE ANGAJAŢILOR ŞI PERSOANELOR VIZATE

5.1. PRIMĂRIA SATULUI ROGOJENI, în calitate de operator de date cu caracter personal, garantează respectarea drepturilor privind protecţia datelor cu caracter personal ce le revin angajaţilor, precum şi, după caz, altor persoane vizate.

5.2. în conformitate cu principiile de protecţie a datelor cu caracter personal, persoanele vizate beneficiază de următoarele drepturi: la informare, de acces la date, de intervenţie, de opoziţie asupra datelor cu caracter personal ce-i vizează, precum şi dreptul de a se adresa Injustiţie.

5.3. Toate persoanele implicate în activitatea de administrare şi/sau prelucrare a informaţiilor din sistemul de evidenţă contabilă vor respecta procedura de acces la datele cu caracter personal.

5.4. Acordarea dreptului de acces a angajaţilor la informaţiile ce-i vizează se efectuează doar prin solicitarea expresă, în formă scrisă, cu acordul nemijlocit al conducerii **PRIMĂRIEI SATULUI ROGOJENI.** Informaţiile furnizate vor fi acordate astfel, încât să nu prejudicieze drepturile terţilor. Persoanele care solicită date cu caracter personal trebuie să indice scopul solicitării, precum şi perioada concretă pentru care solicită informaţiile.

5.5. Există posibilitatea refuzării dreptului de acces în situaţia în care se aplică excepţiile prevăzute de lege. Necesitatea de a restricţiona accesul se poate impune în cazul în care există obligaţia de a proteja drepturile şi libertăţile unor terţe persoane, de exemplu, dacă în informaţiile solicitate apar şi alte persoane şi nu există posibilitatea de a obţine consimţământul acestora sau nu pot fi extrase, prin editare, datele cu caracter personal nerelevante.

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

6.1. Măsurile generale de administrare a securităţii informaţionale

6.1.1. în cazul neutilizării temporare a purtătorilor de informaţie pe suport de hârtie sau electronic care conţin date preluate din sistemul de evidenţă contabilă, aceştia se păstrează în safeuri care se încuie.

6.1.2. La terminarea sesiunilor de lucru, computerele şi imprimantele se deconectează de la reţeaua electrică.

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

6.1.4. Accesul fizic la mijloacele de reprezentare a informaţiei preluate din sistemul de evidenţă contabilă este blocat împotriva vizualizării de către persoane neautorizate.

6.1.5. Mijloacele de prelucrare a informaţiilor preluate din sistemul de evidenţă contabilă sau soft- urile destinate prelucrării acestora sânt scoase din perimetrul de securitate doar în baza permisiunii scrise a operatorului.

6.1.6. Scoaterea şi introducerea mijloacelor de prelucrare a informaţiilor din sistemul de evidenţă contabilă din/în perimetrul de securitate se înregistrează în registru.

6.2. Măsurile de protecţie a datelor cu caracter personal, prelucrate în sistemul de evidenţă contabilă, se înfăptuiesc ţinînd cont de necesitatea asigurării confidenţialităţii şi integrităţii acestora, prin protecţie în formă manuală, electronică.

6.3. Cerinţe speciale faţă de marcare: toate informaţiile ieşite din sistemul de evidenţă contabilă, care conţin date cu caracter personal, sânt supuse marcării, cu indicarea prescripţiilor pentru prelucrarea ulterioară şi răspândirea acestora, inclusiv cu indicarea numărului de identificare unic al operatorului de date cu caracter personal.

6.4. Accesul în biroul unde este amplasat sistemul de evidenţă contabilă este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară şi doar în timpul orelor de program. Accesul în birou este posibil doar cu autorizarea de acces şi cheia de la lacătul mecanic.

6.5. Biroul nu este lăsat niciodată fără supraveghere la ieşirea în exterior, uşa biroului se încuie cu lacătul.

6.6. înainte de acordarea accesului fizic la sistemul de evidenţă contabilă, se verifică competenţele de acces.

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

6.8. Perimetrul de securitate se consideră perimetrul biroului în care este amplasat sistemul de evidenţă contabilă, fiind integru din punct de vedere fizic.

6.9. Zilnic, se inspectează perimetrul de securitate al clădirii şi al biroului, unde este amplasat sistemul de evidenţă contabilă, din punct de vedere fizic.

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

6.11. Uşile şi ferestrele sânt încuiate în cazul în care în încăpere lipsesc angajaţii autorizaţi de administrarea sistemului.

6.12. Amplasarea sistemului de evidenţă contabilă răspunde necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.

6.13. Securitatea electroenergetică: este asigurată securitatea echipamentului electric utilizat pentru menţinerea funcţionalităţii sistemului de evidenţă contabilă, a cablurilor electrice, inclusiv protecţia acestora contra deteriorărilor şi conectărilor nesancţionate. în cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, este asigurată posibilitatea deconectării electricităţii la sistemele de evidenţă contabilă, inclusiv posibilitatea deconectării oricărui component TI.

6.14. Computerele, unde este amplasat fizic sistemul de evidenţă 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 reţea: cablurile de reţea, prin care se efectuează operaţiunile de transmitere a datelor preluate din sistemul de evidenţă contabilă, sânt protejate contra conectărilor nesancţionate sau deteriorărilor. Pentru a exclude bruiajul, cablurile de tensiune sânt separate de cele comunicaţionale.

6.16. Securitatea anti incendiară a sistemului de evidenţă contabilă: biroul unde este amplasat sistemul de evidenţă contabilă este dotat cu echipament anti incendiar şi corespunde cerinţelor şi normelor anti incendiare în vigoare.

6.17. Controlul instalării şi scoaterii componentelor TI: se efectuează controlul şi evidenţa instalării şi scoaterii mijloacelor de program, mijloacelor tehnice şi celor tehnice de program, utilizate în cadrul sistemului de evidenţă contabilă. La expirarea termenului de păstrare, informaţiile, care conţin date cu caracter personal şi care se conţin pe purtătorii de informaţii, se distrug.

VII. IDENTIFICAREA ŞI AUTENTIFICAREA UTILIZATORULUI SISTEMULUI DE EVIDENŢĂ CONTABILĂ

7.1. Este efectuată identificarea şi autentificarea utilizatorilor informaţiilor preluate din sistemele de evidenţă contabilă şi a proceselor executate în numele acestor utilizatori.

7.2. Toţi utilizatorii (inclusiv personalul care asigură mentenanţa tehnică, administratorii de reţea, programatorii şi administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu trebuie să conţină semnalmentele nivelului de accesibilitate al utilizatorului.

7.3. Pentru confirmarea ID-ului utilizatorului sânt utilizate parole. Utilizarea parolelor în procesul asigurării securităţii informaţionale: pe lângă cerinţele de păstrare a confidenţialităţii parolelor, este interzisă înscrierea acestora pe suport de hârtie, cu excepţia cazului de asigurare a securităţii păstrării acesteia (plasarea înscrisurilor în safeu). La momentul introducerii, parolele nu se reflectă în clar pe monitor.

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

7.5. întru asigurarea posibilităţii de stabilire a responsabilităţii fiecărui utilizator, sânt folosite identificatori şi parole individuale ale acestora. Este asigurată posibilitatea utilizatorilor de a alege şi schimba parolele individuale, inclusiv de activare a procedurii de evidenţă a introducerilor greşite ale acestora. După trei tentative greşite de autentificare, accesul este blocat, în mod automatizat.

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

7.7. în cazul în care raporturile de muncă ale utilizatorului au încetat, au fost suspendate sau modificate, şi, ca urmare, noile sarcini nu necesită accesul la datele cu caracter personal, precum şi în cazul de modificare a drepturilor de acces ale utilizatorului, abuz al utilizatorului de autorizaţii de acces primite în scopul comiterii unei fapte prejudiciabile, absenţă a utilizatorului la postul de muncă pe parcursul unei perioade îndelungate (mai mult de 3 luni), codurile de identificare şi autentificare se revocă sau se suspendă.

7.8. Se efectuează, prin mijloace automatizate de suport, administrarea conturilor de acces a utilizatorilor care prelucrează datele cu caracter personal în sistemul de evidenţă contabilă, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea şi ştergerea acestora. Acţiunea conturilor de acces a utilizatorilor temporari, care prelucrează date cu caracter personal înregistrate în sistemul de evidenţă contabilă, încetează automat la expirarea perioadei stabilite în timp (pentru

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 informaţiile din sistemul de evidenţă contabilă. Se folosesc mijloace automatizate de înregistrare şi informare despre crearea, modificarea, dezactivarea şi încetarea acţiunii conturilor de acces.

7.10. în scopul depistării şi evitării cazurilor de acordare a drepturilor de acces neautorizat, se revizuieşte cu regularitate, maximum la fiecare şase luni şi după oricare schimbare a statutului utilizatorului, drepturile de acces ale utilizatorilor la sistemul de evidenţă contabilă.

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

7.12. Se impun limite în privinţa persoanelor care au dreptul:
a) să vizualizeze informaţiile stocate în sistemul de evidenţă contabilă;
b) să copieze, să descarce, să şteargă sau să modifice orice informaţie stocată.

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

7.14. Orice activitate de dezvăluire a datelor cu caracter personal către terţi este documentată şi supusă unei analize riguroase în prealabil privind scopul şi temeiul legal a intenţiilor de dezvăluire a unui anumit volum de date cu caracter personal.

7.15. Orice încălcare a securităţii în ceea ce priveşte sistemul de evidenţă contabilă este supusă documentării, iar persoana responsabilă de realizarea politicii de securitate este informată în legătură cu acest lucru cît de urgent posibil.

7.16. înainte de acordarea accesului în sistem, utilizatorii sînt informaţi despre faptul că folosirea sistemului de evidenţă contabilă este controlată şi că folosirea neautorizată a acestora este sancţionată în conformitate cu legislaţia civilă, contravenţională şi penală.

VIII. AUDITUL SECURITĂŢII ÎN SISTEMELE DE EVIDENŢĂ CONTABILĂ

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

8.2. Se efectuează înregistrarea tentativelor de intrare/ieşi re a utilizatorului în sistem, conform următorilor parametri:
a) data şi timpul tentativei intrării/ieşirii;
b) ID-ul utilizatorului;
c) rezultatul tentativei de intrare/ieşire - pozitivă sau negativă.

8.3. Se efectuează înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative şi proceselor, destinate prelucrării informaţiilor din sistemele de evidenţă contabilă, înregistrarea modificărilor drepturilor de acces ale utilizatorilor şi statutul obiectelor de acces conform următorilor parametri:
a) data şi 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 obţinere a accesului (de executare a operaţiunilor) pentru aplicaţii şi procese destinate prelucrării informaţiilor din sistemul de evidenţă contabilă, conform următorilor parametri:

a) data şi timpul tentativei de obţinere a accesului (executare a operaţiunii);
b) denumirea (identificatorul) aplicaţiei sau a procesului;
c) ID-ul utilizatorului;
d) specificaţiile resursei protejate (identificator, nume logic, nume fişier, număr etc.);
e) tipul operaţiunii solicitate (citire, înregistrare, ştergere etc.);
f) rezultatul tentativei de obţinere a accesului (executare a operaţiunii) - pozitivă sau negativă.

8.5. Se efectuează înregistrarea modificărilor drepturilor de acces (competenţelor) utilizatorului şi statutului obiectelor de acces, conform următorilor parametri:

a) data şi timpul modificării competenţelor;
b) ID-ul administratorului care a efectuat modificările;
c) ID-ul utilizatorului şi competenţele acestuia sau specificarea obiectelor de acces şi statutul nou al acestora.

8.6. Se efectuează înregistrarea ieşirii din sistemul de evidenţă contabilă, înregistrarea modificărilor drepturilor de acces ale subiecţilor şi statutul obiectelor de acces, conform următorilor parametri:

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

8.7. Cazurile de deranjament al auditului securităţii în sistemul de evidenţă contabilă sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, sînt aduse la cunoştinţa persoanei responsabile de politica de securitate a datelor cu caracter personal, care întreprinde măsuri în vederea restabilirii capacităţii de lucru a sistemului de audit.

8.8. Rezultatele auditului securităţii în sistemul de evidenţă contabilă (operaţiunile de prelucrare a informaţiilor şi mijloacele de efectuare a auditului), se protejează contra accesului neautorizat prin aplicarea măsurilor de securitate adecvate şi asigurarea confidenţialităţii şi integrităţii acestora.

8.9. Durata minimă a stocării rezultatelor auditului securităţii în sistemul de evidenţă contabilă constituie 2 */doi/*ani, în scopul asigurării posibilităţii de folosire a acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigaţii sau procese judiciare. în cazul în care investigările sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

IX. ASIGURAREA INTEGRITĂŢII INFORMAŢIILOR DIN SISTEMUL DE EVIDENŢĂ CONTABILĂ

9.1. Se asigură identificarea, protocolarea şi înlăturarea deficienţelor de soft-uri destinate prelucrării informaţiilor din sistemul de evidenţă contabilă, inclusiv instalarea corectărilor şi pachetelor de reînnoire a acestora, protecţia contra infiltrării programelor dăunătoare în soft-uri, măsuri care asigură posibilitatea reînnoirii automate şi la timp a mijloacelor de asigurare a protecţiei contra programelor dăunătoare şi signaturilor de virus.

9.2. Se utilizează tehnologii şi mijloace de constatare a intrărilor ilegale, ce permit monitorizarea evenimentelor şi constatarea atacurilor, inclusiv asigură identificarea tentativelor folosirii neautorizate a informaţiilor din sistemul de evidenţă contabilă.

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

9.4. Copiile de siguranţă: reieşind din volumul prelucrărilor efectuate, individual, se stabileşte de către operator intervalul de timp în care se execută copiile de siguranţă a informaţiilor din sistemul de evidenţă contabilă şi soft-urilor folosite pentru prelucrările automatizate a acestora. Copiile de siguranţă se testează în scopul verificării siguranţei purtătorilor de informaţii şi integrităţii informaţiei indicate. Procedurile de restabilire a copiilor de siguranţă se actualizează şi se testează cu regularitate, în scopul asigurării eficacităţii acestora.

X. GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMULUI DE EVIDENŢĂ CONTABILĂ

10.1. Persoanele care asigură exploatarea sistemului de evidenţă contabilă trec, minimum o dată în an, instruirea cu privire la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate.

10.2. Prelucrarea incidentelor de securitate include depistarea, analiza, preîntîmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii. Se monitorizează şi documentează, în mod permanent, incidentele de securitate în sistemul de evidenţă 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 şi va înlătura cauzele incidentului de securitate cu informarea în termen de 72 ore din momentul producerii incidentului de securitate a Centrului Naţional pentru Protecţia Datelor cu Caracter Personal al Republicii Moldova. Totodată, în cadrul controalelor efectuate de Centrul Naţional pentru Protecţia Datelor cu Caracter Personal, persoanele responsabile sînt obligate să ofere suportul necesar şi să asigure accesul la informaţiile necesare relevante obiectului controlului.”

10.4. Persoanele care se fac vinovate de încălcarea normelor privind obţinerea, păstrarea, prelucrarea şi protecţia informaţiilor din sistemul de evidenţă contabilă poartă răspundere civilă, contravenţională şi penală.

XI. DISPOZIŢII FINALE

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

11.2. Prezentul Regulament se completează cu prevederile legislaţiei în vigoare.

11.3. Regulamentul este adus la cunoştinţa angajaţilor contra semnăturii.

11.4. Modificarea şi 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	Funcţia	Am luat cunoştinţă (semnătura)	Data
1	Groza Ruslan	primar		
2	Guzun Ana	contabila - şefa		
3	Ardeleanu Viorica	Secretara		
5				
6				
7				

Anexa nr. 4
la Decizia nr.1-13
din 25.02.2025

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

PREAMBUL

La prelucrarea datelor cu caracter personal în cadrul entității 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 Politica 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. NOŢIUNI 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 persoana 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, ţinându-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 operaţiune sau set de operaţiuni 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 dispoziţie în orice alt mod în orice alt mod, alinierea sau combinarea, restricţionarea, ştergerea sau distrugerea;

Restricţionarea prelucrării - reprezintă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;
Sistent de evidenţă a datelor cu caracter personal - orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie că este centralizată, descentralizate ori repartizată după criterii funcţionale sau geografice;
Consimţământ - manifestare de voinţă liberă, specifică, informată şi lipsită de ambiguitate a subiectului de date prin care acesta acceptă, printr-o declaraţie sau printr-o acţiune 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 informaţii suplimentare, cu condiţia ca aceste informaţii suplimentare să fie stocate separat şi să facă obiectul unor măsuri de natură tehnică şi organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;

încălcarea securităţii datelor cu caracter personal - reprezintă o încălcare a securităţii 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, agenţia sau alt organism căreia îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terţă. Cu toate acestea, autorităţile 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 autorităţile publice respective respectă normele aplicabile în materie de protecţie a datelor, în conformitate cu scopurile prelucrării.

III. OBIECTIVELE POLITICII PRIVIND PROTECŢIA DATELOR

Obiectivele principale ale Politicii sunt disponibilitatea, integritatea şi confidenţialitatea tuturor informaţiilor, inclusiv datelor cu caracter personal prelucrate de **PRIMĂRIA SATULUI ROGOJENI** atât în cadrul prelucrării manuale, cât şi în cadrul sistemelor şi proceselor de tehnologie informaţională.

Securitatea informaţională reprezintă o componentă esenţială a derulării optime a proceselor bazate pe IT în cadrul **PRIMĂRIEI SATULUI ROGOJENI.** Baza unei securităţi IT adecvate o constituie respectarea prezentei Politici şi a altor acte normative interne în acest sens. Aceasta cuprinde cerinţe şi reguli pentru protecţia tuturor informaţiilor, inclusiv datele cu caracter personal, sistemelor şi proceselor IT împotriva influenţelor naturale, erorilor umane şi tehnice, precum şi împotriva acţiunilor deliberate care pot provoca pagube materiale, respectiv imateriale, sau care pot duce la încălcări ale legislaţiei.

Având în vedere că siguranţa IT nu poate fi garantată exclusiv cu ajutorul unor sisteme tehnice, prezenta Politică vizează, de asemenea, aspecte de ordin organizatorico- juridic şi de altă natură.
PRIMĂRIA SATULUI ROGOJENI va proteja datele cu caracter personal atât a cetăţenilor/petiţionarilor, a angajaţilor săi, cât şi a altor persoane vizate.

Reglementările prezentei Politici reprezintă un standard minim pentru **PRIMĂRIA SATULUI ROGOJENI,** inclusiv şi pentru toţi angajaţii Societăţii. Pornind de la această reglementare, toţi

angajaţii **PRIMĂRIEI SATULUI ROGOJENI** urmează să respecte strict prevederile Politicii şi regulilor interne ale **entităţii** privind protecţia datelor cu caracter personal şi sistemelor IT.

În consecinţă, prin prezenta Politică se stabilesc acţiuni şi măsuri pentru implementarea şi respectarea de către **PRIMĂRIA SATULUI ROGOJENI** a prevederilor legale în vigoare privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi pentru:

J prelucrarea datelor cu caracter personal conform dispoziţiilor legale;
J respectarea drepturilor persoanelor vizate;

■*S* evidenţa operaţiunilor de prelucrare a datelor cu caracter personal în conformitate cu termenii legali;
adoptarea măsurilor necesare pentru a se evita încălcarea securităţii datelor cu caracter personal;
J asigurarea condiţiilor necesare accesării şi utilizării datelor cu caracter personal, exclusiv de către persoanele autorizate (angajaţii), potrivit atribuţiilor menţionate în Fişa postului.

IV. PRINCIPIILE PRELUCRĂRII DATELOR CU CARACTER PERSONAL

J Legalitate, echitate şi transparenţă: datele sunt prelucrate în mod legal, echitabil şi transparent faţă de persoana vizată;
J Limitări legate de scop: datele sunt colectate în scopuri determinate, explicite şi legitime şi nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri;
J Reducerea la minimum a datelor: datele sunt adecvate, relevante şi limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate;
J Exactitate: datele sunt exacte şi pot fi actualizate;

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

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

V. DISPOZIŢII PRIVIND IERARHIA ŞI RESPONSABILITATEA PERSOANEI RESPONSABILE DE POLITICA DE SECURITATE

Organul ierarhic superior al entităţii - PRIMĂRIA SATULUI ROGOJENI, conform competenţei:
J aprobă politicile, procedurile şi alte documente care reglementează prelucrarea datelor cu caracter personal;

Numeşte prin decizie internă angajaţii care primesc atribuţii de prelucrare a datelor cu caracter personal şi dispune măsuri de instruire şi responsabilizare a lor în acord cu cerinţele specifice din Fişa postului;

J dispune măsuri tehnice şi organizatorice menite să asigure protejarea intereselor legitime ale angajaţilor cu privire la confidenţialitatea şi securitatea datelor cu caracter personal care le aparţin, respectiv prelucrarea acestora cu respectarea prevederilor legale în domeniu în scopuri determinate, explicite şi legitime, în baza drepturilor şi obligaţiilor ce revin operatorului, în calitate de angajator;

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

J dispune măsuri tehnice şi organizatorice eficiente, în acord cu specificul de activitate al operatorului, capabile să implementeze conformitatea cu prevederile legislaţiei aferente în vigoare a activităţilor de prelucrare a datelor cu caracter personal, respectiv a celor cu caracter special, realizate în cadrul proceselor operaţionale şi de suport şi implementează în acest sens proceduri de lucru şi responsabilităţi clar definite.

Responsabilul IT:

Stabileşte măsuri tehnice în vederea securizării datelor personale;

J asigură securizarea tuturor sistemelor, serviciilor şi a echipamentelor informatice care sunt folosite pentru stocarea datelor cu caracter personal şi care aparţin entităţii;

S efectuează controale regulate pentru a se asigura că sistemele hardware şi software de securitate funcţionează 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 conţinute în sistemele IT, aplicaţii şi bazele de date ale operatorului.

Angajaţii şi prestatorii de servicii:

Toţi angajaţii şi prestatorii de servicii ai entităţii vor opera datele cu caracter personal în conformitate cu termenii menţionaţi în Politică şi în cele ce urmează:

J datele cu caracter personal sunt prelucrate conform legilor şi reglementărilor aplicabile privind confidenţialitatea şi protecţia datelor;

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

datele cu caracter personal sunt accesate, utilizate şi dezvăluite de către angajaţi şi de prestatorii de servicii, numai pe baza „necesităţii de a cunoaşte", cu aprobările corespunzătoare ale organului de conducere şi doar după ce se li se va asigura o protecţie adecvată.

Conform celor menţionate anterior, angajaţii şi prestatorii de servicii se obligă şi se asigură că:

J prelucrează date cu caracter personal doar dacă aceste atribuţii sunt înscrise în Fişa postului /obligaţiilor contractuale şi doar potrivit instrucţiunilor în vigoare aplicabile, stabilite la nivelul entităţii, respectiv în scopurile şi folosind mijloacele comunicate/puse la dispoziţia acestora de către entitate;

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

J respectă caracterul confidenţial şi măsurile tehnice, organizatorice şi de securitate impuse la nivelul entităţii cu privire la şi în sensul protejării datelor cu caracter personal şi protecţiei drepturilor şi libertăţilor persoanelor vizate; nu vor copia, dezvălui şi/sau transmite, total sau parţial, datele cu caracter personal nici unei persoane, în niciun mod, şi nici nu vor utiliza astfel de informaţii pentru sine sau pentru interesele altor persoane, în afara instrucţiunilor primite de la operator;

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

J notifică toţi terţii cu care intră în contact în timpul exercitării atribuţiilor de serviciu, atât celor cu care colaborează în prezent, cât şi celor care vor fi contactaţi în viitor, informându-i că

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

J solicită consimţământul terţilor, atât celor cu care colaborează în prezent, cât şi celor ce vor fi contactaţi 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 situaţie pentru care legile privind protecţia datelor impun acordarea consimţământului;

Interzic accesul neautorizat la date cu caracter personal;

informează organul de conducere despre situaţiile în care are loc o încălcare a securităţii 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 cunoştinţă de aceasta;

Cel mai târziu la data încetării contractului individual de muncă/contractului de prestări servicii vor preda operatorului bunurile utilizate în desfăşurarea activităţii care conţin date cu caracter personal, indiferent de modul în care au intrat în posesia acestora. Semnarea de către ambele părţi a fişei de lichidare nu instituie o prezumţie absolută în sensul îndeplinirii acestei obligaţii de către salariat/prestator;

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

J respectă măsurile tehnice şi 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 şi 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 şi că persoanele de la care sunt colectate au primit o notificare necesară în mod legal şi au fost informate cu privire la drepturile lor;

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

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

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

Operatorul de date cu caracter personal reieşind din specificul activităţii, prin prezenta Politică, transpune procedurile şi măsurile necesare în vederea asigurării nivelului adecvat de protecţie la prelucrarea datelor cu caracter personal în cadrul sistemelor de evidenţă gestionate.

Politica se va revizui cel puţin o dată în an ca rezultat al modificărilor sau reevaluării competenţelor entităţii, 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 cunoştinţă, sub semnătură, tuturor angajaţilor /prestatorilor de servicii responsabili de prelucrarea datelor cu caracter personal, înaintea acordării accesului la prelucrarea datelor cu caracter personal, inclusiv şi la operarea modificărilor odată cu necesitatea asigurării nivelului adecvat de protecţie a datelor cu caracter personal.

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

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

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

Persoana responsabilă de prezenta politică va defini clar responsabilităţile şi procesele de management al securităţii datelor cu caracter personal, cu integrarea lor corespunzătoare în structura organizaţională şi de funcţionare generală, va asigura măsuri tehnice şi organizaţionale necesare organizării procesului de management al securităţii datelor cu caracter personal, va elabora procedurile de clasificare a informaţiei care conţine date cu caracter personal astfel încât să fie posibil de întocmit un nomenclator şi 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 atribuţiilor funcţionale şi asumării responsabilităţilor de securitate a datelor cu caracter personal, inclusiv asupra confidenţialităţii acestora.

VI. REGULI „CLEAN DESK"

Pentru a îmbunătăţi securitatea şi confidenţialitatea informaţiilor **PRIMĂRIEI SATULUI ROGOJENI** a adoptat reguli **„Clean Desk"** pentru staţiile de lucru pentru computere şi imprimante.

Acest lucru asigură că toate informaţiile sensibile şi confidenţiale, 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 staţie de lucru nu este utilizată.

Aceste reguli vor reduce riscul accesului neautorizat, pierderii şi deteriorării informaţiilor în timpul şi în afara orelor normale de funcţionare sau atunci când staţiile de lucru sunt lăsate nesupravegheate.

Regulile reprezintă un control important al securităţii şi confidenţialităţii şi sunt necesare pentru respectarea legislaţiei cu privire la protecţia datelor.

Aceste reguli se aplică tuturor angajaţilor **PRIMĂRIEI SATULUI ROGOJENI** care activează atât pe perioadă determinată, cât şi nedeterminată sau prin cumul, precum şi 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 şi confidenţiale trebuie să fie scoase de pe birou şi blocate într-un sertar sau dulap de depozitare. Acestea includ dispozitive de stocare în masă, cum ar fi CD-uri, DVD-uri şi unităţi USB.

Toată hârtia de deşeuri care conţine informaţii sensibile sau confidenţiale trebuie plasate în cutiile confidenţiale dedicate.

Staţiile de lucru pentru calculatoare trebuie să fie blocate atunci când biroul este neocupat şi închis complet la sfârşitul zilei de lucru.

VII.SFERA DATELOR PERSONALE. PRELUCRAREA DATELOR CU CARACTER PERSONAL, SCOPURILE ŞI TEMEIURILE PRELUCRĂRII

Activităţile 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 dispoziţie în orice alt mod, alinierea sau combinarea, restricţionarea, ştergerea sau distrugerea.

În cazurile în care **PRIMĂRIA SATULUI ROGOJENI** stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal va avea calitatea de Operator. în situaţiile în care **PRIMĂRIA SATULUI ROGOJENI** împreună cu unul sau mai mulţi operatori stabilesc în comun scopurile şi mijloacele de prelucrare, aceştia vor avea calitatea de Operatori Asociaţi. Atunci când **PRIMĂRIA SATULUI ROGOJENI** nu stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal va avea calitatea de Persoană împuternicită şi va prelucra datele conform instrucţiunilor definite de Operator.

La nivelul PRIMĂRIEI SATULUI ROGOJENI sunt prelucrate următoarele categorii de date aparţinând angajaţilor proprii, precum şi candidaţilor la angajare, şi anume:

A numele, prenumele;

A sexul;

A data şi locul naşterii;
A cetăţenia;
A IDNP;
A imagine;
A situaţia familială;
A situaţia militară;
A datele personale ale membrilor de familie;
A datele din permisul de conducere;
A datele pentru transferul pe contul bancar a plăţilor salariate şi a altor sume datorate cu titlu de indemnizaţii, compensaţii 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/reşedinţei);
A adresa e-mail;
A profesia şi/sau locul de muncă;
A formarea profesională - diplome - studii;
A numele, prenumele (după caz, patronimicul) persoanelor care se află la întreţinerea persoanei respective (membrii familiei, alte rude şi persoane, după caz);
A mărimea concretă a drepturilor salariate calculate, taxele şi impozitele aferente, inclusiv contribuţiile de asigurări sociale obligatorii de asistenţă medicală şi socială, şi alte sume datorate în virtutea legii sau contractului;
A datele din certificatele de concediu medical acordate, necesare pentru calcularea indemnizaţiei corespunzătoare;
A informaţii de recrutare (inclusiv copii ale diplomelor de studii, referinţe şi alte informaţii incluse într-un CV sau scrisoare de intenţie ca parte a procesului de aplicare);
A informaţii despre utilizarea de către angajat a sistemelor noastre de informare şi comunicaţii;
A după caz, alte date necesare îndeplinirii scopului menţionat, conform legislaţiei în vigoare.

La nivelul PRIMĂRIEI SATULUI ROGOJENI sunt prelucrate următoarele categorii de date aparţinând cetăţenilor/petiţionarilor:

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

La nivelul PRIMĂRIEI SATULUI ROGOJENI sunt prelucrate următoarele categorii de date aparţinând cetăţenilor/petiţionarilor şi alor persoane vizate prin intermediul înregistrării şi difuzării audio-video a şedinţelor Consiliului sătesc:

J imaginea persoanelor vizate;
•J vocea persoanelor care vor lua cuvântul;
J numele şi prenumele persoanelor care vor lua cuvântul sau altor persoane vizate;
A funcţia deţinută de persoanele care vor lua cuvântul.

La nivelul PRIMĂRIEI SATULUI ROGOJENI sunt prelucrate următoarele categorii de date aparţinând partenerilor contractuali (persoane fizice) şi reprezentanţilor partenerilor comerciali (persoane juridice) şi anume:

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

Colectarea datelor cu caracter personal. Informarea persoanelor vizate.

Acordarea Consimţământului 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 destinatarii 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) şi alte drepturi de bază în domeniul protecţiei datelor;
A dreptul de a depune o plângere către Autoritatea de Supraveghere a Prelucrării Datelor cu Caracter Personal (CNPDCP);
A dreptul de a-şi retrage consimţământul în orice moment;
A eventuala existenţă a unui proces decizional automatizat şi logica utilizată, inclusiv consecinţele acestui fapt.

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

PRIMĂRIA SATULUI ROGOJENI are obligaţia de a aduce la cunoştinţă persoanei vizate categoriile de date şi sursa din care a obţinut datele, inclusiv în situaţia în care acestea provin din surse disponibile public.

PRIMĂRIA SATULUI ROGOJENI realizează distincţia dintre obligaţia de informare şi obligaţia de a obţine consimţământul persoanei vizate, acesta din urmă aplicându-se doar în cazuri limitativ prevăzute de legislaţia în vigoare şi dacă prelucrarea nu se încadrează în situaţiile de excepţie care permit prelucrarea în baza unor temeiuri legale.

Consimţământul se defineşte ca fiind o manifestare de voinţă liberă, specifică, informată şi lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, prin intermediul unei declaraţii, ca datele cu caracter personal care o privesc să fie prelucrate.
Rolul obţinerii consimţământului este de a asigura transparenţa şi de a spori încrederea persoanelor vizate, oferind totodată acestora posibilitatea de a alege în mod liber şi de a deţine controlul asupra datelor cu caracter personal prelucrate.

<u>Scopurile în care sunt prelucrate datele cu caracter personal</u>

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 angajaţi precum şi candidaţilor 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 angajaţi precum şi candidaţilor la angajare, sunt prevăzute de **Politica de Confidenţialitate privind prelucrarea datelor personale ale angajaţilor şi potenţialilor angajaţi** 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 şi/sau pe alte rețele sau platforme de socializare, precum şi publicarea pe pagina web a primăriei satului a şedinţelor Consiliului Local, urmărind scopul de:

J transparentizare a proceselor/deciziilor din administrația locală;
J informare eficientă a cetățenilor oraşului;
J creştere a gradului de implicare a cetățenilor în problemele oraşului;
J creştere a nivelului de încredere în administrația publică locală.

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

<u>Temeiul juridic şi condițiile de legalitate pe care se bazează prelucrările de date</u>

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 consimţământul persoanei vizate;
J prelucrarea este necesară pentru a încheia un raport juridic/contract sau pentru executarea acestuia;
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 învestit 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 cerinţelor prevăzute de legislația în vigoare şi în conformitate cu politicile şi procedurile **PRIMĂRIEI SATULUI ROGOJENI.**

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

■*J parteneri contractuali;*
•S subcontractanţi;
J procesatori de plăţi;
J companii ce oferă servicii IT;
J companii de audit;
J avocaţi, notari, executori judecătoreşti;
deţinători de registre publice şi/sau private;
autorităţi publice, cum ar fi, dar a nu se limita la: ASP; CNAM, CNAS, SFS, instanţe de judecată sau arbitrate, precum şi autorităţi competente să cerceteze săvârşirea de fapte penale.

Vom mai putea dezvălui datele tale personale unor terţi în următoarele situaţii:

•A în cazul în care ne solicitaţi personal această dezvăluire sau ne daţi acordul în acest sens;
J persoanelor care pot demonstra că deţin autoritatea legală de a acţiona în numele dvs.;
■*A în cazul în care avem obligaţia de a dezvălui datele tale personale pentru a respecta o obligaţie legală sau o solicitare din partea autorităţilor;*
■*A pentru a răspunde oricăror acţiuni juridice, pentru a proteja drepturile noastre sau ale unui terţ, pentru siguranţa oricărei persoane sau pentru a preveni orice fel de activitate nelegală;*
Punerea la dispoziţie a datelor cu caracter personal în interiorul entităţii:

În derularea activităţii **PRIMĂRIEI SATULUI ROGOJENI,** datele cu caracter personal ale unor persoane vizate trebuie să fie prelucrate de către mai multe subdiviziuni/departamente. Procesele interne al entităţii sunt concepute pentru a respecta cerinţele de protecţie a datelor cu caracter personal, inclusiv reducerea la minim a datelor cu caracter personal folosite de diferite subdiviziuni/departamente din cadrul entităţii în activităţile lor.
Colectarea şi prelucrarea de către o/un subdiviziune/departament specific, de alte date decât cele prevăzute de aceste procese şi modele interne pot fi efectuate numai cu aprobarea corespunzătoare a Primarului.

Transferurile de date cu caracter personal către prestatorii de servicii:
Pentru a-şi îndeplini activitatea, în anumite situaţii **PRIMĂRIA SATULUI ROGOJENI** va pune la dispoziţia 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 şi **PRIMĂRIA SATULUI ROGOJENI.**

Transferurile de date cu caracter personal către Terţi.

Transferul de date cu caracter personal către terţi care nu sunt prestatori de servicii şi cu care în general **PRIMĂRIA SATULUI ROGOJENI** nu are încheiat un contract, va putea fi efectuat în baza unor obligaţii legale sau pe baza interesului său legitim. De ex. conceptul de ’’Terţi” poate include autorităţile publice, inclusiv fiscale, instanţele de judecată, executori judecătoreşti, etc.
Datele cu caracter personal sunt prelucrate numai pe teritoriul Republicii Moldova şi nu sunt fi transferate în altă ţară.

IX. TERMENUL DE PRELUCRARE A DATELOR CU CARACTER PERSONAL

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

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

pentru instituţiile, organizaţiile şi 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 <u>în procesul de recrutare</u>:

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

J Datele referitoare la candidaţii selectaţi vor fi incluse în dosarul personal al acestora şi vor fi păstrate pe perioada activităţii în cadrul **PRIMĂRIEI SATULUI ROGOJENI,** iar după încetarea raporturilor de muncă, se vor păstra în formă arhivată, pe perioada stabilită de Indicatorul documentelor-tip şi al termenelor lor de păstrare pentru organele administraţiei publice, pentru instituţiile, organizaţiile şi 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, explicaţii candidaţilor cu privire la motivele pentru care candidatura a fost respinsă.

De asemenea, având în vedere interesul nostru legitim de a optimiza selecţia celor mai potriviţi candidaţi pentru posturile disponibile şi pentru a informa candidaţii 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 proporţională şi rezonabilă, pe termen scurt şi mediu, cu scopul unei persoane de a găsi şi de a ocupa un loc de muncă adecvat pregătirii sale).* însă, în cazul în care persoana vizată nu doreşte ca **PRIMĂRIA SATULUI ROGOJENI** să păstreze CV-ul în acest scop, ea are dreptul de a se opune unei astfel de prelucrări şi de a solicita ștergerea datelor.

Datele referitoare la candidaţi pot fi păstrate într-o arhivă intermediară în scopuri probatorii, în special pentru a se proteja împotriva unor eventuale reclamaţii 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 **<u>cetăţenilor/petiţionarilor</u>,** pe o perioadă care nu depăşeşte perioada necesară îndeplinirii scopurilor pentru care au fost colectate, după care, se arhivează daca legislaţia în vigoare nu prevede altfel.

PRIMĂRIA SATULUI ROGOJENI păstrează **<u>datele obţinute în rezultatul înregistrării audio-video a şedinţelor consiliului local</u>,** până la data aprobării, de către consilierii locali, a procesului verbal aferent şedinţei înregistrate.

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

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

X. MIJLOACE SUPUSE PRINCIPIILOR DE PROTECŢIE A DATELOR CU CARACTER PERSONAL

Protecţia 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 şi organizatorice de preîntâmpinare a prelucrării ilicite a datelor cu caracter personal.

Sânt supuse protecţiei prin mijloace/procedee specifice, toate resursele informaţionale ale operatorului de date cu caracter personal gestionate, care conţin 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 securităţii informaţionale

în cazul neutilizării temporare a purtătorilor de informaţie pe suport de hârtie sau electronici (digitali) care conţin date cu caracter personal, aceştia se păstrează în safeuri sau dulapuri metalice care se încuie.

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

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

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

Mijloacele de prelucrare a datelor cu caracter personal, informaţia care conţine 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 condiţiile de licenţiere.

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

Securitatea mediului fizic şi a tehnologiilor informaţionale folosite în procesul prelucrării datelor cu caracter personal.

Accesul în sediile/oficiile/birourile ori spaţiile unde sînt amplasate sistemele informaţionale de date cu caracter personal este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară, conform listei sau însemnelor corespunzătoare (insigne, ecusoane, cartele de identificare). Se asigură administrarea şi monitorizarea accesului fizic în toate punctele de acces la sistemele informaţionale de date cu caracter personal, inclusiv se reacţionează 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, pereţii exteriori ai încăperilor sînt rezistenţi, intrările sunt echipate cu lacăte şi semnalizare.

Amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespund necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.

Uşile şi 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, ţinînd cont de necesitatea asigurării regimului de confidenţialitate şi securitate a prelucrării datelor cu caracter personal, prevăzut de prevederile Legii privind protecţia datelor cu caracter personal nr.133 din 08.07.2011.

Identificarea şi autentificarea utilizatorilor.

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

Toţi utilizatorii (inclusiv personalul care asigură susţinerea tehnică, administratorii de reţea, programatorii şi administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu conţine semnalmentele 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 şi individuale ale persoanei.

În cazul în care contractul de muncă/raporturile de serviciu ale utilizatorului au fost încetate, suspendate sau modificate şi 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 şi autentificare se revocă sau se suspendă de administratorul I.T.

Identificarea şi autentificarea echipamentului

Este asigurată posibilitatea identificării şi autentificării echipamentului folosit în operaţiunile de prelucrare a datelor cu caracter personal, cu menţinerea acestor informaţii pentru o perioadă îndelungată.

Administrarea identificatorilor utilizatorilor

Administrarea identificatorilor utilizatorilor include:
identificarea univocă a fiecărui utilizator,
verificarea autenticităţii fiecărui utilizator.

Utilizarea parolelor în procesul asigurării securităţii informaţionale

Sunt respectate regulile de asigurare a securităţii informaţionale în cazul alegerii şi folosirii parolelor care includ:

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

Controlul administrării accesului

Este efectuat controlul sistematic al acţiunilor utilizatorilor în vederea evaluării corectitudinii şi conformării operaţiunilor şi acţiunilor efectuate prin intermediul sistemelor informaţionale de date cu caracter personal.

Limitarea folosirii tehnologiilor fără fir

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

Accesul fără fir la sistemele informaţionale de date cu caracter personal este permis doar în cazul utilizării mijloacelor criptografice de protecţie a informaţiei.

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

Securitatea electroenergetică:

a) Echipamentul electric utilizat pentru menţinerea funcţionalităţii sistemelor informaţionale de date cu caracter personal, a cablurilor electrice, este asigurat contra deteriorărilor şi conectărilor nesancţionate, prin montarea lor în nişe speciale.

b) în cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, este asigurată posibilitatea deconectării electricităţii la sistemele informaţionale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component TI.

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

Controlul instalării şi scoaterii componentelor T.L

Este exercitat controlul şi evidenţa instalării şi scoaterii mijloacelor de program, mijloacelor tehnice şi celor tehnice de program, utilizate în cadrul sistemelor informaţionale de date cu caracter personal.

Informaţiile, care conţin date cu caracter personal şi care se conţin pe purtătorii de informaţii, se distrug fizic sau se transcriu şi se nimicesc prin metode sigure, evitîndu-se folosirea funcţiilor standarde de nimicire.

Dezvăluirea datelor cu caracter personal prin reţele comunicaţionale ori pe alt suport digital de stocare.

Dezvăluirea formatului electronic al datelor cu caracter personal conţinute în sistemele de evidenţă, prin reţele comunicaţionale ori pe alt suport digital de stocare şi păstrare, urmează a fi asigurată criptarea acestei informaţii sau examinarea posibilităţii utilizării unei conexiuni bilaterale prin canal securizat VPN. Accesul fără fir la sistemele de evidenţă a datelor cu caracter personal este permis doar utilizatorilor autorizaţi. Fiecare caz de solicitare a dezvăluirii prin transmitere a datelor cu caracter personal pe cale electronică va fi examinat separat, reieşind din posibilităţile tehnice asigurate de destinatar şi operator, precum şi în corespundere cu măsurile organizatorice şi tehnice implementate de părţi. în cazul în care reţelele comunicaţionale prezintă riscuri pentru confidenţialitatea şi securitatea datelor cu caracter personal, vor fi utilizate metode tradiţionale de transmitere *(expediereрoştală cu aviz recomandat, înmînareapersonală, etc.).*

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

Sînt interzise operaţiunile de dezvăluire a datelor cu caracter personal între **PRIMĂRIA SATULUI ROGOJENI** şi alte entităţi care sunt amplasate geografic în stînga Nistrului care refuză să se supună juridic legislaţiei Republicii Moldova, reieşind din considerentul că la moment nu există posibilitatea exercitării unui control efectiv asupra acestei părţi teritoriale, inclusiv în partea ce ţine de conformitatea prelucrării datelor cu caracter personal prevederilor *Legii privind protecţia datelor cu caracter personal nr.133 din 08.07.2011.*

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

Transmiterea transfrontalieră a datelor cu caracter personal este efectuată în strictă corespundere cu prevederile legislaţiei în vigoare în domeniul protecţiei datelor cu caracter personal, în special în cazurile cînd tratatul internaţional în baza căruia se efectuează transmiterea nu conţine garanţii privind protecţia drepturilor subiectului de date cu caracter personal.

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

f) Acces la sistemele informaţionale gestionate în cadrul **PRIMĂRIEI SATULUI ROGOJENI,** din partea Procuraturii Generale *(după caz procuraturile teritoriale/specializate),* Ministerului Afacerilor Interne, Centrului Naţional Anticorupţie etc., va fi permis doar în cazul în care solicitarea va corespunde prevederilor art. 15 şi 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 adeverite circumstanţe care au importanţă pentru cauză, *(inclusiv informaţia stocată în auditul sistemelor informaţionale şi de evidenţă),* pot fi solicitate printr-un demers al organului de urmărire penală în cadrul urmăririi penale sau în procesul judecării cauzei. In 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 şi răspîndite fără necesitate informaţie 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 conţine cel puţin:

Descrierea sistematică a operaţiunilor de prelucrare preconizate şi a scopurilor prelucrării datelor, inclusiv, după caz, a interesului legitim urmărit de **entitate;**

evaluarea necesităţii şi proporţionalităţii operaţiunilor de prelucrare în legătură cu scopurile respective;

evaluarea riscurilor pentru drepturile şi libertăţile subiecţilor de date, în special originea (sursa), natura, gradul specific de probabilitate a materializării riscului sporit şi 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 protecţia datelor cu caracter personal nr.133 din 08.07.2011;

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

PRIMĂRIA SATULUI ROGOJENI va solicita, după caz, avizul în formă scrisă, în formă electronică sau prin utilizarea mijloacelor electronice de comunicaţie al subiecţilor de date ori al reprezentanţilor acestora privind prelucrarea preconizată, fără a aduce atingere protecţiei intereselor comerciale sau publice ori securităţii operaţiunilor 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 protecţiei datelor, cel puţin atunci când are loc o modificare a riscului reprezentat de operaţiunile de prelucrare.

Lista tipurilor de operaţiuni de prelucrare care fac obiectul cerinţei de efectuare a unei evaluări a impactului asupra protecţiei datelor, se stabileşte de Centrul Naţional pentru Protecţia Datelor cu Caracter Personal.

PRIMĂRIA SATULUI ROGOJENI va consulta Centrul Naţional pentru Protecţia Datelor cu Caracter Personal înainte de prelucrarea datelor dacă evaluarea impactului asupra protecţiei 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 şi al costurilor implementării.

În cazul în care operatorul consultă Centrul Naţional pentru Protecţia Datelor cu Caracter Personal, va furniza următoarea informaţie:

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

- scopurile şi mijloacele prelucrării preconizate;

măsurile şi garanţiile prevăzute pentru protecţia drepturilor şi libertăţilor subiecţilor de date, în conformitate cu prezenta lege;

- după caz, datele de contact ale persoanei responsabile cu protecţia datelor;

evaluarea impactului asupra protecţiei datelor;

- alte informaţii relevante şi necesare solicitate suplimentar de Centrul Naţional pentru Protecţia Datelor cu Caracter Personal.

Prelucrarea prin împuterniciţi

PRIMĂRIA SATULUI ROGOJENI va încheia contracte cu Persoane împuternicite care oferă garanţii suficiente pentru punerea în aplicare a unor măsuri tehnice şi organizatorice adecvate, astfel încât prelucrarea să respecte prevederile legale şi să asigure protecţia drepturilor şi libertăţilor persoanelor vizate. Conţinutul respectivelor contracte va face referire la obiectul şi durata prelucrării, natura şi scopul prelucrării, tipul de date cu caracter personal şi categoriile de persoane vizate, obligaţiile şi drepturile **PRIMĂRIEI SATULUI ROGOJENI ,** în calitate de operator, şi ale persoanei împuternicite.

XVI. DREPTURILE SUBIECŢILOR DE DATE CU CARACTER PERSONAL

În situaţia solicitărilor venite din partea persoanelor vizate în vederea accesării datelor cu caracter personal, rectificării, ştergerii sau portabilităţii acestora, **PRIMĂRIEI SATULUI ROGOJENI** va verifica mai întâi dacă datele personale menţionate aparţin 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 explicaţie completă, transmisă în scris, în termen de 30 de zile, menţionând motivele refuzului, precum şi dreptul persoanei vizate de a depune o plângere la CNPDCP.
Potrivit dispoziţiilor legale, persoanele vizate au următoarele drepturi:
dreptul la informare şi acces;
dreptul la rectificare;
dreptul la opoziţie;
dreptul de ştergere;
dreptul la restricţionarea prelucrării;
dreptul la portabilitatea datelor.
dreptul de a nu fi supus unei decizii individuale.
Dreptul de a depune o plângere Ia operator şi la autoritatea competentă privind protecţia datelor;
Dreptul de a retrage consimţământul.

XVII. STOCAREA, PĂSTRAREA ŞI DISTRUGEREA DATELOR CU CARACTER PERSONAL PRELUCRATE

Accesul în spaţiile/perimetrul unde sînt amplasate sistemele informaţionale şi de evidenţă a datelor cu caracter personal este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară conform politicii de securitate instituţionale /regulamentelor departamentale aprobate.
Stocarea şi păstrarea formatului electronic al datelor cu caracter personal, structurate în sisteme de evidenţă, în computere care sînt conectate la internet, nu sînt echipate cu mijloace de protecţie speciale tehnice şi de program şi nu au instalate programe licenţiate, programe antivirus, sisteme de control al securităţii sofît-ului, de asigurare a efectuării periodice a copiilor de siguranţă şi de efectuare a auditului - este interzisă.

Introducerea în perimetrul de securitate instituţional şi utilizarea calculatoarelor personale ori a purtătorilor de informaţii în scopuri de serviciu este interzisă. Mai mult, accesul la computerele din dotare sunt protejate/restricţionate prin crearea profilurilor de utilizatori, iar drepturile de administrator sînt încredinţate 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 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, 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/ieşire a utilizatorului în sistem, conform următorilor parametri:

- data şi timpul tentativei intrării/ieşirii;
- ID-ul utilizatorului;
- rezultatul tentativei de intrare/ieşire - pozitivă sau negativă.

Se efectuează înregistrarea tentativelor de obţinere a accesului (de executare a operaţiunilor) pentru aplicaţii şi procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:

- data şi timpul tentativei de obţinere a accesului (executate a operaţiunii),
- denumirea (identificatorul) aplicaţiei sau procesului, o ID-ul utilizatorului,
- specificaţiile resursei protejate (identificator, nume logic, nume fişier, număr etc.),
- tipul operaţiunii solicitate (citire, înregistrare, ştergere etc.),
- rezultatul tentativei de obţinere a accesului (executare a operaţiunii) — pozitivă sau negativă.

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

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

Se efectuează înregistrarea ieşirii din sistem a informaţiei care conţine date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecţilor şi statutul obiectelor de acces, conform următorilor parametri:

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

XIX.ASIGURAREA PROTECȚIEI CONTRA PROGRAMELOR DĂUNĂTOARE (VIRUȘILOR)

Este asigurată protecţia contra infiltrării programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal, prin existenţa programelor licenţiate anti-virus.

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

Se asigură testarea funcţionării corecte a funcţiilor de securitate a sistemelor informaţionale de date cu caracter personal (automat la pornirea sistemului şi lunar la solicitarea utilizatorului autorizat în acest scop).

XXI.GESTIONAREA INCIDENTELOR DE SECURITATE

Orice angajat/prestator de servicii care are cunoştinţă despre, sau suspectează producerea unui incident de încălcare a securităţii datelor cu caracter personal, are obligaţia 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 şi restabilirea securităţii.

”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 şi va înlătura cauzele incidentului de securitate cu

informarea, în termen de 72 ore din momentul producerii incidentului de securitate, a Centrului Naţional pentru Protecţia Datelor cu Caracter Personal al Republicii Moldova.
în cadrul controalelor efectuate de Centrul Naţional pentru Protecţia Datelor cu Caracter Personal al Republicii Moldova i se va oferi suportul necesar şi asigurat accesul la informaţiile necesare relevante obiectului controlului."

XXII.MARCAREA DOCUMENTELOR

Toată informaţia care se intenţionează a fi dezvăluită, şi care conţine date cu caracter personal, urmează a fi marcată prin:

Model - Atenţie! Documentul conţine date cu caracter personal. Prelucrarea ulterioară a acestor date poate fi efectuată numai în condiţiile prevăzute de Legea privind protecţia datelor cu caracter personal nr.133 din 08.07.2011.

XXIII. RESPONSABILITATEA PENTRU ASIGURAREA SECURITĂŢII DATELOR CU CARACTER PERSONAL PRECUM ŞI A INFORMAŢIILOR CU ACCESIBILITATE LIMITATĂ.

Operatorul de date cu caracter personal, persoana împuternicită de către operator, persoanele terţe după caz, pentru nerespectarea dispoziţiilor Politicii de securitate - poartă răspundere civilă (Codul civil), contravenţională (art. 74^1 Cod contravenţional) şi penală (art. art. 177, 178, 180 Cod penal).

LISTA ANGAJAŢILOR

FAMILIARIZAŢI CU PREVEDERILE POLITICII

PRIVIND PROTECŢIA DATELOR CU CARACTER PERSONAL

ÎN CADRUL

PRIMĂRIEI SATULUI ROGOJENI

Nr.	Numele, prenumele	Funcţia	Am luat cunoştinţă (semnătura)	Data
1.	Groza Ruslan	primar		
2.	Ardeleanu Viorica	secretara consiliului		
3.	Guzun Ana	contabila - şefa		
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.5
la Decizia nr.1/13
din 25.02.2025

Politica de Confidenţialitate privind prelucrarea datelor personale
ale angajaţilor
şi potenţialilor angajaţi
ai Primăriei satului Rogojeni, raionul Şoldăneşti

Dreptul dumneavoastră, în calitate de angajaţi, la intimitate şi viaţă privată reprezintă pentru noi o prioritate şi suntem în permanenţă angajaţi în îmbunătăţirea continuă a modului în care protejăm datele dumneavoastră cu caracter personal

INFORMAȚII PRELIMINARE

PRIMĂRIA SATULUI ROGOJENI, este conştientă de importanţa protecţiei vieţii private şi a libertăţilor individuale şi se angajează să asigure protecţia acestora în conformitate cu legislaţia în vigoare cu privire la protecţia datelor cu caracter personal.

Scopul acestei Politici de Confidenţialitate privind prelucrarea datelor personale ale angajaţilor şi potenţialilor angajaţi (denumită în continuare **„Politică de Confidenţialitate")** 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 şi după încetarea acestuia* şi la drepturile pe care le aveţi cu privire la aceste date.

Prezenta politică de confidenţialitate se referă la activităţile 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 confidenţialitate pune în aplicare principiul transparenţei şi descrie modalităţile prin care se realizează operaţiunile de colectare, utilizare, diseminare, stocare şi 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 confidenţialitate descrie categoriile de informaţii care vă privesc, pe care **PRIMĂRIA SATULUI ROGOJENI** le colectează, motivele pentru care aceste informaţii sunt colectate, principiile de bază pe care ne bazăm tratarea acestora şi modul în care **PRIMĂRIA SATULUI ROGOJENI** vă gestionează datele personale, precum şi are drept scop de a ne îndeplini obligaţia legală de a vă informa cu privire la prelucrarea datelor cu caracter personal pe care o desfăşurăm în calitate de operator de date.

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

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

Potrivit prezentei Politici de confidenţialitate, ne-am stabilit regula respectării obligaţiilor prevăzute de legislaţia în vigoare privind protecţia datelor cu caracter personal, dar trebuie să fiţi conştienţi de faptul că şi dvs trebuie să fiţi vigilenţi cu cine partajaţi datele personale şi cum vă protejaţi comunicaţiile şi dispozitivele.

DESCRIEREA DATELOR CU CARACTER PERSONAL PE CARE LE PRELUCRĂM, SCOPURILE ŞI TEMEIURILE LEGALE ALE PRELUCRĂRII"

Date cu caracter personal" înseamnă informaţii referitoare la o persoană fizică identificată sau identificabilă. Datele dumneavoastră de contact şi data naşterii 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 funcţie de etapă (recrutare/angajare/executare contract/ etc.), în funcţie de poziţia/funcţia dvs în cadrul **PRIMĂRIA SATULUI ROGOJENI** şi de condiţiile de angajare.

CE DATE CU CARACTER PERSONAL PUTEM PRELUCRA:

numele, prenumele;
sexul;
data şi locul naşterii;
cetăţenia;
IDNP;
imagine;
situaţia familială;
situaţia militară;
datele personale ale membrilor de familie;
datele din permisul de conducere;
datele pentru transferul pe contul bancar a plăţilor salariate şi a altor sume datorate cu titlu de indemnizaţii, compensaţii 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/reşedinţei);
adresa e-mail;
•profesia şi/sau locul de muncă;
•formarea profesională - diplome - studii;
numele, prenumele (după caz, patronimicul) persoanelor care se află la întreţinerea persoanei respective (membrii familiei, alte rude şi persoane, după caz);

mărimea concretă a drepturilor salariale calculate, taxele şi impozitele aferente, inclusiv contribuţiile de asigurări sociale obligatorii de asistenţă medicală şi socială, şi alte sume datorate în virtutea legii sau contractului;
datele din certificatele de concediu medical acordate, necesare pentru calcularea indemnizaţiei corespunzătoare;
informaţii de recrutare (inclusiv copii ale diplomelor de studii, referinţe şi alte informaţii incluse într-un CV sau scrisoare de intenţie ca parte a procesului de aplicare);
Informaţii despre utilizarea de către angajat a sistemelor noastre de informare şi comunicaţii;
după caz, alte date necesare îndeplinirii scopului menţionat, 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 diverşi colaboratori sau parteneri contractuali, informaţii ce reies din interacţiunea dumneavoastră cu aceştia.

Vă vom ține la curent în momentul colectării datelor, care tip de date trebuie în mod imperativ să ne fie comunicate. Nefumizarea 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 sunteţi 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 terţe părţi, cu excepţia cazului în care aceste interese prevalează asupra intereselor sau drepturilor şi libertăţilor dumneavoastră fundamentale care necesită protecţie. In acest caz, dacă nu este menţionat 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 şi pentru a înceta raportul de muncă. Aceste scopuri sunt toate legate de o bază de legalitate a prelucrării, şi anume:

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

reclamaţiilor dvs; anexarea CV-ului la dosarul personal în cazul în care aţi fost selectat pentru postul la care aţi 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.
Managementul administrativ al resurselor umane, inclusiv gestionarea dosarelor angajaţilor şi a salarizării.	Această prelucrare este necesară pentru executarea contractului individual de muncă și respectarea obligațiilor legale de către **PRIMĂRIA SATULUI ROGOJENI**
Realizarea unor studii/sondaje de satisfacţie a angajaţilor	Interesul nostru legitim de a identifica nivelul de satisfacție al angajaților.
Realizarea de testimoniale şi articole, interviuri, inclusiv prin procesarea imaginilor / fotografiilor angajaţilor.	Acest tip de prelucrare este justificată doar de obținerea Consimțământului
Publicarea fotografiilor şi filmuleţelor video în cazul în care angajatul poate fi identificat, cu scopul publicării materialelor informative, promovare evenimente şi manifestări pe website-ul oficial, canalul Youtube, Facebook, Instagram sau alte platforme online de către PRIMĂRIA SATULUI ROGOJENI sau orice terţe persoane afiliate sau împuternicite de entitate, care pot realiza orice fel de materiale audio/video şi orice fel de imagini, capturi sau materiale fotografice	Acest tip de prelucrare este justificată doar de obținerea Consimțământului
Organizarea unor evenimente şi seminare în scopul dezvoltării competenţelor tehnice şi dezvoltare personală şi profesională	Interesul nostru legitim de a dezvolta competențele angajaților **PRIMĂRIA SATULUI ROGOJENI.**
Evaluarea performanţei şi a talentelor, precum şi analize statistice legate de managementul resurselor umane	Această prelucrare este justificată de interesul legitim al **PRIMĂRIA SATULUI ROGOJENI** de a putea optimiza cariera angajaților săi pentru a asigura un management optim al resurselor umane.
Asigurarea sănătăţii şi securităţii în muncă („SSM"): efectuarea unor instructaje pentru protecţia muncii şi a controalelor medicale în caz de necesitate	Obligația legală pentru prelucrarea datelor ce țin de SSM (pentru toate prelucrările care sunt prevăzute de legislația incidență)
Organizarea timpului de lucru, inclusiv prezenţa la locul de muncă, absenţe, concedii plătite şi concedii medicale.	Această prelucrare este necesară pentru îndeplinirea contractului individual de muncă și respectarea obligațiilor legale de către **PRIMĂRIA SATULUI ROGOJENI.**

Gestionarea deplasărilor în interes de serviciu, a costurilor de cazare şi a oricăror cheltuieli aferente.	Această prelucrare este necesară pentru îndeplinirea contractului de muncă.
Acordarea şi gestionarea de beneficii personale către angajaţi (neincluse în contractul individual de muncă)	Interesul legitim al **PRIMĂRIEI SATULUI ROGOJENI** de a menține o buna relație de munca cu angajații.
Desfăşurarea de investigaţii, aspecte de disciplina muncii şi oferirea de suport în situaţii conflictuale sau de neperformanţă legate de angajaţi	Interesul nostru legitim în asigurarea unui mediu de lucru propice şi a unei bune relaţii cu angajații, de a respecta obligațiile legale si contractuale ale **PRIMĂRIEI SATULUI ROGOJENI** si de a proteja drepturile de care beneficiază entitatea
Managementul instruirii	Această prelucrare este necesară pentru îndeplinirea contractului de muncă şi respectarea obligaţiilor sale legale de către **PRIMĂRIA SATULUI ROGOJENI.**
Păstrarea datelor personale ale angajaţilor	Această prelucrare este necesară pentru a respecta obligaţia legală a **PRIMĂRIEI SATULUI ROGOJENI** de a respecta termenele legale de păstrare a datelor personale şi de a răspunde solicitărilor şi reclamaţiilor angajaţilor.

Modificarea scopului

Vom folosi informaţiile 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 şi că acest motiv este compatibil cu scopul inițial. Dacă trebuie să folosim informaţiile dvs. personale pentru o situaţie care nu are legătură cu scopul inițial, vă vom anunța şi vă vom explica temeiul legal care ne permite să facem acest lucru.

Vă rugăm să reţineţi că este posibil să vă procesăm informaţiile personale fără ştirea sau consimţământul dvs, în conformitate cu regulile de mai sus, acolo unde acest lucru este cerut sau permis de lege.

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

Date referitoare la condamnări penale şi infracţiuni

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

noastre de reglementare. Vom prelucra şi acest tip de date cu caracter personal în cazul în care are loc o infracţiune la locul de muncă.
Prelucrăm aceste date cu caracter personal pe baza intereselor noastre legitime, care includ asigurarea faptului că angajăm numai personal adecvat şi asigurarea securităţii şi protecţiei **PRIMĂRIEI SATULUI ROGOJENI** şi a bunurilor noastre.

TERMENUL DE PĂSTRARE A DATELOR CU CARACTER PERSONAL

Reţinem datele personale ale angajaţilor noştri doar în măsura în care este necesar pentru îndeplinirea scopurilor pentru care le-am colectat sau pentru care au fost comunicate. în consecinţă, în general, vom păstra datele dumneavoastră cu caracter personal cel puţin pe durata angajării dumneavoastră în cadrul entităţii.

La expirarea termenului menţionat datele din sistemul de evidenţă a angajaţilor sunt păstrate în formă arhivată pe perioada stabilită de Indicatorul documentelor-tip şi al termenelor lor de păstrare pentru organele administraţiei publice, pentru instituţiile, organizaţiile şi 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 candidaţii selectaţi vor fi incluse în dosarul personal al acestora şi vor fi păstrate pe perioada activităţii în cadrul **PRIMĂRIEI SATULUI ROGOJENI,** iar după încetarea raporturilor de muncă, se vor păstra în formă arhivată, pe perioada stabilită de Indicatorul documentelor-tip şi al termenelor lor de păstrare pentru organele administraţiei publice, pentru instituţiile, organizaţiile şi 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 puteţi participa la proba interviului sau în urma interviului nu aţi 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, explicaţii candidaţilor cu privire la motivele pentru care candidatura a fost respinsă.

De asemenea, având în vedere interesul nostru legitim de a optimiza selecţia celor mai potriviţi candidaţi pentru posturile disponibile şi 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 proporţională şi rezonabilă, pe termen scurt şi mediu, cu scopul unei persoane de a găsi şi de a ocupa un loc de muncă adecvat pregătirii sale).* însă, în cazul în care nu doriţi să păstrăm CV-ul dvs în acest scop, aveţi dreptul să Vă opuneţi şi să solicitaţi ştergerea datelor.

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

DESTINATARII DATELOR DUMNEAVOASTRĂ:

Accesul la datele tale personale este limitat doar la acele persoane care au nevoie să cunoască aceste informaţii în scopuri profesionale. Acestea pot fi departamentul / subdiviziunea şi persoanele lor desemnate pentru a îndeplini anumite funcţii, cum ar fi angajaţii 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 Ia ştergerea datelor ("dreptul de a fi uitat"):** puteţi obţine din partea operatorului ştergerea datelor cu caracter personal atunci când nu mai sunt necesare pentru îndeplinirea scopurilor în care au fost colectate sau când vă retrageţi consimţământul în cazul în care acesta există;
- **dreptul la restricţionarea prelucrării:** puteţi solicita şi obţine restricţionarea prelucrării datelor cu caracter personal care vă privesc în cazul în care contestaţi exactitatea datelor, legitimitatea deţinerii lor sau în alte cazuri prevăzute de lege.
- **reptul la portabilitatea datelor dumneavoastră cu caracter personal:** aveţi dreptul de a primi datele dvs într-un format structurat, utilizat în mod curent şi care poate fi citit automat şi 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:** aveţi dreptul de a cere anularea, în totalitate sau parţială, a oricărei decizii individuale care produce efecte juridice asupra drepturilor şi libertăţilor sale, fiind întemeiată exclusiv pe prelucrarea automatizată a datelor cu caracter personal destinată să evalueze unele aspecte ale personalităţii sale, precum competenţa profesională, credibilitatea, comportamentul şi altele asemenea.
- **dreptul la opoziţie:** puteţi să vă opuneţi, în special, prelucrărilor de date care se întemeiază pe interesul nostru legitim;
- **dreptul de a vă retrage consimţământul:** în cazurile în care prelucrarea se întemeiază pe consimţământul dumneavoastră, îl puteţi retrage oricând. Retragerea consimţământului va avea efecte doar pentru viitor, prelucrarea efectuată anterior retragerii rămânând în continuare legitimă.
- **dreptul de a depune o plângere la operator şi la autoritatea competentă privind protecţia datelor** (CNPDCP - https://datepersonale.md/).

EXERCITAREA DREPTURILOR DVS.:

în situaţia în care doriţi să vă exercitaţi drepturile prezentate anterior sau consideraţi că prelucrarea datelor dvs se realizează fără respectarea prevederilor Legii privind protecţia datelor cu caracter personal nr.133 din 08.07.2011, puteţi formula o cerere scrisă, datată şi semnată către operatorul **PRIMĂRIA SATULUI ROGOJENI,** la adresa **rnl. Şoldăneşti, s. Rogojeni, MD-7230,** ori către Responsabilul cu protecţia datelor, la adresa de e-mail: **primaria.rogojeni@apl.gov.md**

Dacă doriţi să vă exercitaţi dreptul de a formula plângere la autoritatea de stat competentă, vă informăm că aceasta este Centrul Naţional Pentru Protecţia Datelor cu Caracter Personal (CNPDCP -https://datepersonale.md/) sau instanţelor de judecată.

NOTIFICARE PRIVIND MODIFICĂRILE ADUSE ACESTEI POLITICI

Putem modifica sau actualiza această Politică în orice moment.
In cazul în care modificăm gestionarea protecţiei datelor cu caracter personal, vă vom anunţa cu privire la modificările sau actualizarea acestei Politici, astfel încât să ştiţi ce date procesăm şi cum le utilizăm.

LISTA ANGAJAȚILOR
familiarizaţi cu
Politica de Confidenţialitate privind prelucrarea datelor personale
ale angajaţilor şi potenţialilor angajaţi
ai Primăriei satului Rogojeni, raionul Şoldăneşti

Nr.	**Numele, prenumele**	**Funcţia**	**Am luat cunoştinţă (semnătura)**	**Data**
1.	Groza Ruslan	primar		
2.	Ardeleanu Viorica	secretara consiliului		
3.	Guzun Ana	contabila - şefa		
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 informaţii 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 identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;**

„prelucrare” - înseamnă orice operaţiune sau set de operaţiuni 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 dispoziţie în orice alt mod, alinierea sau combinarea, restricţionarea, ștergerea sau distrugerea;

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

„destinatar” - înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terţă. Cu toate acestea, autorităţile 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 autorităţile publice respective respectă normele aplicabile în materie de protecţie a datelor, în conformitate cu scopurile prelucrării;

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

„consimţământ” - al persoanei vizate înseamnă orice manifestare de voinţă liberă, specifică, informată şi lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declaraţie sau printr-o acţiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;

„încălcarea securităţii datelor cu caracter personal” - înseamnă o încălcare a securităţii 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

Prezenta 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 terților 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 angajaţilor în modulul de administrare al site-ului web al Operatorului decât dacă au aprobarea Conducerii de a efectua modificări în conţinutul de informaţii. Adăugarea de legături către alte resurse, actualizarea informaţiilor sau schimbarea design-ului intră, de asemenea, sub incidenţa acestor aprobări.

Acordarea drepturilor de acces din Internet la reţeaua 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, consultaţii, personalul temporar, personalul companiilor prestatoare de servicii, etc.
Accesul va fi acordat în mod individual şi doar pentru perioada desfăşurării sarcinilor aprobate.

Angajaţii pot folosi alte surse de furnizare a conexiunii la Internet utilizând calculatoarele Operatorului, doar cu acordul Conducerii, întrucât controalele de acces şi metodele de asigurare a securităţii datelor nu pot fi aplicate corespunzător decât dacă întregul flux de activităţi referitoare la Internet trece prin echipamentele de tip firewall ale Operatorului. în aceeaşi manieră, angajaţii sunt obligaţi să utilizeze numai căsuţa 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 încredinţarea către alte persoane a resurselor informatice ale Operatorului.

Operatorul nu se declară răspunzător pentru conţinutul paginilor de Internet accesate de angajaţi. în cazul accesării întâmplătoare a unui site cu conţinut informaţional imoral (caracter sexual explicit, rasist, misogin, violent sau de natură ofensatoare), angajaţii în cauză sunt obligaţi să aleagă o altă pagină sau să încheie procesul curent.

Operatorul poate înregistra paginile accesate, fişierele desemnate, timpul petrecut pe o pagină anume şi alte informaţii conexe.

Conducerea Operatorului poate primi rapoarte ce conţin astfel de informaţii şi 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, fişierele aflate pe staţiile de lucru, fişierele temporare ale browser-elor de Internet (Internet Explorer, Mozilla Firefoc, Google Chrome etc.), paginile marcate, istoricul site-urilor web necesare şi alte informaţii stocate sau care tranzitează staţiile de lucru ale Operatorului în orice moment şi fără necesitatea unui anumit prealabil.

Se interzice angajaţilor stabilirea unor legături la Internet sau la alte reţele externe care ar putea favoriza terţe părţi să pătrundă în reţeaua Operatorului şi să aibă acces la sistemele şi informaţiile acesteia, decât dacă acest lucru este aprobat de către Conducere. Aceste conexiuni presupun legături de tip file-sharing (partajare de fişiere), sisteme de comerţ prin intermediul Intemetului sau servere FTP.

Utilizarea e-mail-ului

Operatorul pune la dispoziţia angajaţilor săi sau, după caz, prestatorilor de servicii atunci când aceştia utilizează sistemele IT ale Operatorului, căsuţe de poştă electronică. Conturile de poştă electronică individuale nu trebuie utilizate în comun.

Utilizarea sistemului de mesagerie electronică al Operatorului trebuie realizată ca parte a activităţii profesionale, ce are ca scop îmbunătăţirea activităţilor de zi cu zi prin înlesnirea comunicării interne în cadrul Operatorului, respectiv în exterior prin menţinerea legăturilor cu clienţii, partenerii de afaceri ai Operatorului sau cu autorităţile locale.

Comunicarea electronică se va limita la materialele care au legătură cu activităţile profesionale şi sarcinile de serviciu ale angajaţilor şi nu va fi folosită ca suport pentru campanii caritabile de strângere de fonduri, campanii de susţinere politică/religioasă sau pentru activităţi ce ţin de afaceri personale, amuzament sau distracţie.

Se interzice folosirea de către un utilizator a unei adrese de e-mail ce aparţine altei persoane. Periodic, angajaţii vor fi informaţi şi instruiţi să folosească în mod adecvat resursele sistemului informatic al Operatorului.
în cadrul comunicaţiei electronice se interzice înlocuirea, înlăturarea sau denaturarea identităţii 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 protecţiei împotriva e-mail-urilor nesolicitate (mesaje de tip „hoax", mesaje înlănţuite chain letter, spam etc.) şi scheme de mesaje electonice cu caracter fraudulos (phishing şi 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 protecţiei împotriva infectării cu produse software cu potenţial distructiv (viruşi, troieni, worm etc.)
în cazul în care primesc sau detectează orice e-mail suspicios, angajaţii sunt obligaţi să informeze Departamentul IT.

Utilizarea echipamentelor mobile
Toate echipamentele mobile care au fost achiziţionate în numele Operatorului sunt considerate a fi proprietatea Operatorului şi 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 şi în locuinţa personală sau oricare altă locaţie.

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

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

Utilizarea dispozitivelor mobile în spaţii publice trebuie făcută cu prudenţă pentru a elimina riscul ca informaţiile afişate pe ecran să poată fi văzute de persoane neautorizate. în situaţia în care se poate asigura o minimă intimitate, utilizarea dispozitivelor mobile în locaţiile publice trebuie restrânsă.

Pentru stocarea informaţiilor cu caracter sensibil se recomandă folosirea serverelor de reţea şi mai puţin a echipamentelor de tip mobil computing. Pentru a se asigura siguranţa informaţiei, discul fix al dispozitivului mobil şi părţile aferente pe care se va face stocarea trebuie să fie criptate.
în funcţie de arhitectura hardware şi software, dispozitivele de tip mobil computing trebuie să aibă configurate soluţii corespunzătoare de protecţie împotriva aplicaţiilor software cu potenţial distructiv (viruşi, spyware, malware etc.). Utilizatorul unui dispozitiv mobil trebuie să-şi actualizeze permanent programele de protecţie şi să se asigure că foloseşte ultima versiune dată de producător.

Toate echipamentele mobile vor avea configurată o aplicaţie „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 conţine informaţii cu caracter sensibil din cadrul Primăriei. în aceste condiţii, utilizatorul unui astfel de dispozitiv devine responsabil pentru disponibilitatea, integritatea şi confidenţialitatea datelor referitoare la Primărie, pe care le are la dispoziţie. Utilizarea calculatorului portabil în exteriorul Primăriei se permite doar cu acordul conducătorului şi 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-şi salveze periodic documentele pe care le dezvoltă pentru a preîntâmpina pierderea accidentală a informaţiilor 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 nelicenţiate şi instalarea aplicaţiilor de către utilizatori.

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

Protecţia împotriva viruşilor

Operatorul are implementate măsuri de protecţie ale sistemelor telefonice informatice, aplicaţiilor şi reţelelor şi de detectare a tuturor tipurilor de viruşi şi 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 viruşilor.
Departamentul IT are următoarele responsabilităţi:

-să se asigure că programul antivirus este instalat pe toate staţiile utilizatorilor şi pe toate serverele;
să actualizeze definiţiile viruşilor;

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

Salvarea şi restaurarea datelor

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

LISTA ANGAJAŢILOR FAMILIARIZAŢI CU PREVEDERILE POLITICII ANTI-SPAM ÎN CADRUL PRIMĂRIEI SATULUI ROGOJENI

Nr.	**Numele, prenumele**	**Funcţia**	**Am luat cunoştinţă (semnătura)**	**Data**
1.	Groza Ruslan	primar		
2.	Ardeleanu Viorica	secretara consiliului		
3.	Guzun Ana	contabila - şefa		
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.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, 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 operator” - înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

„destinatar” - înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terţă. Cu toate acestea, autorităţile 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 autorităţile publice respective respectă normele aplicabile în materie de protecţie a datelor, în conformitate cu scopurile prelucrării;

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

„consimţământ” - al persoanei vizate înseamnă orice manifestare de voinţă liberă, specifică, informată şi lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declaraţie sau printr-o acţiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;

„încălcarea securităţii datelor cu caracter personal” - înseamnă o încălcare a securităţii 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 securităţii resurselor informaţionale ale **PRIMĂRIEI SATULUI ROGOJENI.**
(în continuare **''Operator"** sau **''entitatea").** Se va urmări protecţia resurselor informaţionale împotriva modificărilor neautorizate sau accidentale, asigurând acurateţea şi completitudinea acestora, precum şi protecţia resurselor informaţionale 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 şi se va aplica tuturor prelucrărilor efectuate de Operator. în cazul în care se constată existenţa anumitor aspecte legate de gestionare datelor cu caracter general pentru care prezenta politică nu oferă directive corespunzătoare, angajaţii trebuie să solicite imediat consiliere din partea Responsabilului pentru Protecţia Datelor (DPO), dacă a fost numit, sau reprezentantului legal al Operatorului.

4. PREVEDERI GENERALE

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

Reţelele, aplicaţiile şi sistemele informatice ale Operatorului sunt disponibile în momentul în care este nevoie de ele. Acestea nu pot fi accesate decât de către utilizatorii autorizaţi şi conţin informaţii corecte şi complete.

Prin implementarea unor măsuri atât tehnice, cât şi operaţionale, Operatorul va proteja toate programele, echipamentele şi activele informaţionale aflate în patrimoniul ei.

4.2.Informarea utilizatorilor. Fiecare angajat/prestator de servicii care utilizează resursele informaţionale ale Operatorului de date **PRIMĂRIA SATULUI ROGOJENI,** va participa în momentul angajării şi ulterior, anual, la cursuri de securitate a informaţiilor organizate de conducerea Operatorului. De asemenea, fiecărui angajat/prestator de servicii îi vor fi puse la dispoziţie, în momentul angajării/semnării contractului de colaborare, copii ale prezentei politici, precum şi ale tuturor normelor şi procedurilor operaţionale IT, pe care va trebui să le respecte. Aceştia îşi vor exprima acordul cu privire la respectarea acestor norme prin semnarea formulatorului din **Anexa 1** a acestui document.
De asemenea, prezenta politică precum şi celelalte norme şi proceduri operaţionale IT vor fi postate pe Intranetul Operatorului într-o locaţie disponibilă tuturor angajaţilor. Angajaţii vor fi informaţi cu privire la această locaţie. Prezenta politică precum şi celelalte procedurii operaţionale se adresează deopotrivă şi prestatorilor de servicii ai Operatorului, care vor folosi sau vor avea acces la resursele fizice şi informaţionale ale Operatorului. Pentru a dovedi luarea la cunoştinţă 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, aplicaţiile şi reţele care sunt utilizate în cadrul tuturor proceselor

Operatorului. Totodată, se vor identifica măsurile necesare pentru protecţia împotriva breşelor de confidenţialitate, integritate şi disponibilitate.
4.4. Utilizarea informaţiilor. Fiecare angajator/ prestator de servicii care utilizează resursele informaţionale ale Operatorului de date **PRIMĂRIA SATULUI ROGOJENI** trebuie să aibă acces doar la informaţia necesară pentru a-şi îndeplini sarcinile. Informaţiile sensibile trebuie accesate doar de către angajaţii / prestatorilor de servicii cărora proprietarul aplicaţiei respective le-a acordat drept de acces.

Informaţiile Operatorului nu trebuie folosite în alte scopuri decât cele de afaceri aprobate în mod oficial de către Conducere. Folosirea neaprobată a informaţiilor 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 informaţiilor Operatorului, cum ar fi listele de distribuţie a e-mail-urilor, este interzisă.

Nu este permisă utilizarea de programe licenţiate de către Operator pe calculatoare personale, cu excepţia cazului în care sistemul a fost desemnat să proceseze informaţii ale Operatorului.
Toate activităţile utilizatorilor sunt înregistrate şi analizate ulterior. O conduită nepotrivită poate duce la acţiuni 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 performanţa la locul de muncă, şi nu limitează accesul altor utilizatori la resursele sistemului.

4.5. Politica pentru parole
Accesul la sistemul informatic al Operatorului trebuie să fie restricţionat pe bază de nume de utilizator şi 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 aplicaţie accesată la alta. Alegeţi parole diferite pentru aplicaţii faţă de cele pentru accesul în reţea.

Utilizatorii nu trebuie să dezvăluie nimănui parolele utilizate în cadrul sistemelor informatice ale Operatorului, nici măcar celorlalţi angajaţi. Toate parolele sunt calificate ca informaţii confidenţiale.

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 circumstanţă nicio parolă NIMĂNUI;
- NU împărtăşească 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 maşină”);
- NU scrie în clar parola pe hârtie sau în mesaje electronice;
- NU păstreze parolele scrise;
- NU stocheze parolele sub formă de fişiere pe NICIUN sistem de calcul (nici pe echipamentele mobile) fără ca acele fişiere să fie criptate.

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

Parolele adecvate au următoarele caracteristici:

- conţin atât majuscule, cât şi litere mici (A-Z, a-z);
- conţin cifre şi cel puţin un caracter alfanumeric (0-9,!@#$%^A&*()_+:?;.);
- nu se bazează pe informaţii personale precum nume, numere de telefon etc.;
- nu coincid şi nu conţin 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 specificaţii:

- 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 naştere, adrese, numere de telefon, numărul de la maşină sau alte informaţii personale;
- cuvinte sau succesiuni de litere sau cifre de genul: abcdef,l23456,zyxwvuts, 123321 etc.;
- oricare dintre cuvintele de mai sus scrise în ordinul invers;
- coincid sau conţin numele de utilizator;
- au lungimea mai mică de opt caractere.

4.6.Accesul la distanţă

Accesul la distanţă 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 distanţă se acordă după aprobarea Departamentului IT şi conducătorului Operatorului.

Accesul de la distanţă 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 iniţia conexiunea la reţeaua Operatorului, angajaţii trebuie să se asigure că echipamentul de calcul pe care îl folosesc nu este conectat în acelaşi timp la o altă reţea.
- Orice altă configuraţie hardware sau software de acces de la distanţă în afara celor agreate de Operator trebuie aprobată de Departamentul IT.
- Conectarea de la distanţă la reţeaua Operatorului implică folosirea unui software antivirus agreat şi actualizat zilnic la ultimele semnături de virusuri.
- Angajaţii vor accesa sistemele Operatorului de la distanţa numai folosind echipamentele Operatorului, configurate şi protejate corespunzător (PC-uri, Laptopuri, PDA-uri, tablete

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

4.7. Raportarea incidentelor

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

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

Procesul de raportare a incidentelor de securitate a informaţiei foloseşte aceleaşi căi de raportare ca şi în cazul incidentelor obişnuite.

5. ROLURI ŞI RESPONSABILITĂŢI

5.1. Angajaţii

Toţi angajaţii care activează în cadrul Operatorului au următoarele responsabilităţi:

- să respecte Politica privind resursele informatice;
- să asiste în sesiuni de informare şi la cursuri de securitatea informaţiei;
- să se familiarizeze şi să acţioneze în concordanţă cu toate cerinţele Operatorului ;
- să solicite şefului lor direct acces la resursele informaţionale care le sunt necesare;
- să raporteze toate activităţile suspecte şi problemele de securitate;
- să raporteze orice suspiciune de breşă de securitate sau breşă de securitate ca atare;
- să prevină introducerea în sistemele informaţionale din cadrul Operatorului de produse software cu potenţial distructiv;
- să păstreze în bună stare resursele informaţionale, produsele software şi echipamentele hardware ale Operatorului.

5.2. Conducerea Operatorului

Are următoarele responsabilităţi:

- să asigure securitatea bunurilor organizaţiei (informaţie, echipamente hardware, produse software folosite de către angajaţi şi de către terţe părţi);
- să asigure aplicarea politicii de securitate a Informaţiei;
- să se asigure că toţi angajaţii sunt conştienţi de responsabilităţile de securitate pe care le au;
- să se asigure raportarea şi înregistrarea tuturor incidentelor de securitate;
- să asigure că orice încălcare a securităţii informaţiei de către angajaţi este investigată în mod corespunzător;
- să asigure faptul că angajaţii au fost instruiţi corespunzător cu privire la securitatea informaţiei;
- să emită decizii prin care este dispusă cercetarea faptelor angajaţilor care au încălcat prevederile prezentei proceduri.

6. Dispoziţii finale

Răspunderea în cazul încălcării procedurii

Încălcarea prevederilor acestei proceduri poate determina aplicarea unor măsuri disciplinare, inclusiv desfacerea contractului de muncă din motive care ţin 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 informaţionale ale Operatorului de date **PRIMĂRIA SATULUI ROGOJENI,** de asemenea poartă răspundere deplină în conformitate cu legislaţia în vigoare, în cazul în care se face vinovată de încălcarea prevederilor prezentei Proceduri.
În condiţiile menţionate, lipsa de înţelegere în cazul în care procedura va fi încălcată nu va putea fi invocată de către utilizatorii cărora le este adresată această procedură.

LISTA ANGAJAŢILOR FAMILIARIZAŢI CU PREVEDERILE POLITICII PRIVIND RESURSELE INFORMATICE ÎN CADRUL PRIMĂRIEI SATULUI ROGOJENI

Nr.	Numele, prenumele	Funcţia	Am luat cunoştinţă (semnătura)	Data
1.	Groza Ruslan	primar		
2.	Ardeleanu Viorica	secretara consiliului		
3.	Guzun Ana	contabila - şefa		
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 1 - Acord de respectare a Politicii de Securitate a Informaţiilor în cadrul PRIMĂRIEI SATULUI ROGOJENI

Numele complet al utilizatorului:_____
Datele de contact:_____

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

- Să respect toate prevederile politicilor şi procedurilor existente în cadrul Operatorului, precum şi în Politica privind resursele informatice. în acest sens, am luat la cunoştinţă conţinutul tuturor acestor documente.
- Să adopt toate măsurile de precauţie necesare în vederea eliminării riscurilor de dezvăluire către persoane neautorizate a informaţiilor interne ale Operatorului sau a informaţiilor care mi-au fost încredinţate de către Operator.
- Să returnez odată cu finalizarea activităţii mele pentru Operator, toate materialele la care am primit acces ca rezultat al activităţii mele în cadrul acesteia. înţeleg faptul că îmi este interzisă folosirea acestor informaţii în scopuri personale şi nici nu am autorizarea de a dezvălui aceste materiale terţilor fără aprobarea explicită în scris a managerului desemnat pentru relaţia cu angajatorul meu din interiorul Operatorului.
- Să informez prompt şeful direct despre orice situaţie 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 şi 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. Dispoziţii generale

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

Aceste sisteme de supraveghere prin mijloace video se adresează, în principal, spaţiilor în care se desfăşoară activităţi de vânzare, spaţii comerciale dar şi birourilor de acces public.

Totodată utilizarea unui astfel de sistem include anumite responsabilităţi şi garanţii din partea proprietarului de sistem, referitor la prelucrarea şi protecţia datelor cu caracter personal ce se înregistrează în sistem, atribuţii şi reglementări descrise în legea nr. 133 din 18.07.2011 privind protecţia datelor cu caracter personal.

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

Mijloacele de supraveghere video se instalează şi utilizează cu respectarea principiului:

- legalităţii;
- proporţionalităţii;
- transparenţei;
- securităţii.

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

- Stabilirea unui set unitar de reguli care reglementează implementarea şi utilizarea sistemului de supraveghere prin mijloace video, în scopul asigurării securităţii persoanelor şi bunurilor, pazei şi protecţiei bunurilor, imobilelor, valorilor şi a materialelor cu regim special, respectînd în acelaşi timp obligaţiile ce revin entităţii, în calitate de operator de date, conform Legii nr. 133 din 18.07.2011 şi măsurile de securitate adoptate pentru protecţia datelor cu caracter personal, protejarea vieţii private, a intereselor legitime şi garantarea drepturilor fundamentale ale persoanelor vizate.
- Stabilirea responsabilităţilor privind administrarea şi exploatarea sistemului de supraveghere prin mijloace video, precum şi cele privind întocmirea, avizarea şi aprobarea documentelor aferente acestor activităţi.
- Scopul utilizării sistemului de supraveghere prin mijloace video este de a asigura buna administrare şi funcţionare a entităţii, în special în vederea controlului de securitate şi pază. De asemenea, sistemul de supraveghere prin mijloace video este necesar pentru a sprijini politicile de securitate instituite de actele normative care reglementează protecţia datelor cu caracter personal şi contribuie la îndeplinirea atribuţiilor structurii de securitate.
- Prezentul Regulamentul 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, vieţii private şi alte drepturi fundamentale şi interese legitime ale subiecţilor.

3. Zonele supravegheate

- Camerele de supraveghere video sânt amplasate în locuri vizibile. Orice utilizare ascunsă a acestora este strict interzisă, cu excepţia cazurilor expres reglementate de legislaţie.
- Camerele de supraveghere video sânt amplasate conform anexelor nr. 1 şi 2 al prezentului Regulament.
-
- Nu sânt monitorizate zonele în care persoanele pot conta, în mod rezonabil, pe intimitate, precum birourile de serviciu şi toaletele. Instalarea mijloacelor de supraveghere video se poate realiza numai în condiţiile în care echipamentele sânt orientate exclusiv asupra căilor de acces şi perimetrului acestor bunuri, fără ca în raza lor de acoperire să fie vizualizate alte spatii publice, ori bunurile terţilor.

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 mişcare. Toate camerele funcţionează în regim 24/24 ore şi 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 confidenţialitate şi dreptul de acces la informaţia prelucrată în sistemul de evidenţă.
-

5. Limitarea scopului

- Sistemul de supraveghere prin mijloace video va fi utilizat numai în scop legal, fără a se urmări în special obţinerea unor informaţii pentru anchetele interne sau procedurile disciplinare, cu excepţia situaţiilor în care se produce un incident de securitate sau se observă un comportament infracţional (în circumstanţe excepţionale imaginile pot fi transmise organelor competente în cadrul unor investigaţii disciplinare sau penale).
- în vederea protejării vieţii private a altor subiecţi decât cei vizaţi 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 anonimizată.
- Persoana responsabilă va gestiona accesul la sistemul de supraveghere prin mijloace video numai cu acordul scris al conducerii **PRIMĂRIEI SATULUI ROGOJENI.**

6. Categorii 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 şi dezvăluirea acestora

- Accesul la imaginile video înregistrate în timp real este limitat la un număr redus de angajaţi ai **PRIMĂRIEI SATULUI ROGOJENI,** care pot fi identificaţi individual, în conformitate cu lista aprobată de către conducerea entităţii.
- Accesul la imaginile video şi/ sau la arhiva în care sânt stocate imaginile înregistrate este permis numai persoanei responsabile în conformitate cu Politica de securitate a **PRIMĂRIEI SATULUI ROGOJENI** şi numai cu acordul scris al conducerii.
- Vizualizarea şi/sau efectuarea copiilor din fişierele 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 îşi exercită atribuţiile conform legii, a unor copii din fişierele temporare în care sânt stocate imaginile video, este permis numai cu acordul scris al conducerii **PRIMĂRIEI SATULUI ROGOJENI.**

8. Protecţia sistemului informaţional de date cu caracter personal în care sânt stocate (prelucrate) imaginile video

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

- sistemul informaţional 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 protecţie a datelor cu caracter personal şi responsabilii de securitate din cadrul entităţii vor fi consultaţi înainte de achiziţionarea sau instalarea oricărui nou sistem de supraveghere prin mijloace video.
- toate sistemele trebuie să corespundă cerinţelor de securitate descrise în legislaţie (HG nr. 1123 privind aprobarea cerinţelor faţă de asigurarea securităţii datelor cu caracter personal).
- accesul fizic la sistemul informaţional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video are numai persoana responsabilă desemnată şi conducerea **PRIMĂRIEI SATULUI ROGOJENI;**
- accesul la înregistrările video prelucrate este restricţionat prin introducerea unui şir de parole;
- în cazul deconectării energiei electrice, sistemul informaţional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video este dotat cu sursă autonomă de alimentare cu energie electrică (UPS);
- sistemul informaţional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video este dotat cu firewall care asigură protecţia în reţea;
- Echipamentele sînt astfel instalate încît să se afle sub supraveghere doar acele spaţii identificate în analiza de risc ca avînd nevoie de protecţie suplimentară.
- Utilizatorii sistemului de supraveghere prin mijloace video sunt instruiţi să nu monitorizeze astfel de zone.
- **PRIMĂRIA SATULUI ROGOJENI** actualizează în permanenţă listă persoanelor care au acces la sistemul informaţional 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 entităţii.
- Accesul neautorizat în Camera de control este interzis. Accesul este strict limitat la angajaţii autorizaţi: personalul cu funcţii de asigurare al securităţii fizice şi control acces, administratorul de sistem, responsabilii cu securitatea informaţiei şi conducerea entităţii.
- De la caz la caz, se poate acorda accesul în Camera de control şi altor persoane, în afara celor menţionate mai sus, doar pe bază de autorizare din partea responsabilului de securitate din cadrul entităţii. Aceste persoane nu vor avea acces la datele personale prelucrate în activitatea de supraveghere video, accesul acestora fiind permis strict pentru executarea lucrărilor menţionate în autorizarea din partea responsabilului de securitate din cadrul entităţii.

10. Măsuri tehnice şi organizatorice

Pentru a proteja securitatea sistemului de supraveghere prin mijloace video şi pentru a spori gradul de protecţie a vieţii private, au fost introduse următoarele măsuri tehnice şi organizatorice:

- limitarea timpului de stocare a materialului filmat, în conformitate cu cerinţele de securitate şi legislaţia în vigoare privind conservarea datelor.
- mediile de stocare (serverele pe care se stochează imaginile înregistrate) se află în spaţii securizate şi protejate de măsuri de securitate fizică.
- toţi utilizatorii cu drept de acces la sistemul de supraveghere prin mijloace video au semnat acorduri de confidenţialitate, 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 atribuţiilor de serviciu.
- doar administratorii de sistem numiţi în acest sens de către operator, şi responsabilul de securitate, au dreptul de a accesa fişierele înregistrate în sistem, la cererea conducerii unităţii.

11. Drepturi de acces

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

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

- să vizioneze materialul filmat în timp real: imaginile care se derulează în timp real sunt accesibile responsabililor de securitate şi agenţilor de pază desemnaţi să desfăşoare 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 şi incidentele de securitate, de către persoanele special desemnate;
- să copieze, să descarce, să şteargă sau să modifice orice material filmat de sistemul de supraveghere prin mijloace video.

12. Instructaj

- Toţi membrii personalului cu drepturi de acces beneficiază de o instruire iniţială în domeniul protecţiei datelor.
- Această procedură va fi integrată în programul de instruire şi îndrumare, pentru toţi utilizatorii cu drept de acces şi atribuţii în operarea sistemului de supraveghere prin mijloace video.
- Şeful subdiviziunii va asigura că întregul personal din subordine, implicat în operarea sistemului de supraveghere prin mijloace video, este instruit şi informat cu privire la toate aspectele funcţionale, operaţionale şi administrative ale acestei activităţi.

13.Măsuri de păstrare a confidenţialităţii

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

14. Dezvăluirea datelor cu caracter personal

- Orice activitate de dezvăluire a datelor personale către terţi va fi documentată şi supusă unei analize riguroase privind pe de-o parte necesitatea comunicării, şi pe de altă parte compatibilitatea dintre scopul în care se face comunicarea şi scopul în care aceste date au fost colectate iniţial pentru prelucrare.
- Orice situaţie de dezvăluire va fi consemnată de administratorul sistemului într-un Registru de evidenţă a cazurilor de dezvăluire.
- **PRIMĂRIA SATULUI ROGOJENI** are obligaţia punerii la dispoziţia organelor judiciare, la solicitarea scrisă a acestora, înregistrările video în care este surprinsă săvârşirea unor fapte de natură contravenţională/penală.
- Sistemul de supraveghere prin mijloace video nu este utilizat pentru verificarea prezenţei la program sau evaluarea performanţei la locul de muncă.
- In cazuri excepţionale, dar cu respectarea garanţiilor descrise mai sus, se poate acorda acces altor servicii din cadrul entităţii (Protecţie Antiincendiară, Resurse Umane, Riscuri), în cadrul unei anchete disciplinare, de accidentare sau de securitate, cu condiţia ca informaţiile să ajute la investigarea unei infracţiuni, accident de muncă sau a unei abateri disciplinare de natură să prejudicieze drepturile şi libertăţile 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 depăşi limitele admisibile de program, în funcţie 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 legislaţia Republicii Moldova. Toate persoanele implicate în activitatea de supraveghere video şi cele responsabile de administrarea imaginilor filmate, vor respecta procedurile şi regulamentele de acces la date cu caracter personal ale entităţii.

17. Informarea persoanelor vizate

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

18. Exercitarea drepturilor de acces, intervenţie şi opoziţie

- Pe întreaga perioadă de stocare a datelor cu caracter personal, persoanele vizate au dreptul de acces la datele personale care le privesc deţinute de PRIMĂRIA SATULUI ROGOJENI, de a solicita intervenţia (ştergere/ actualizare/ rectificare/ anonimizare) sau de a se opune prelucrărilor, conform legii.
- Orice cerere de a accesa, rectifica, bloca şi/sau şterge 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, intervenţie sau opoziţie se dă în termen de 15 zile calendaristice. Dacă nu se poate respecta acest termen, persoana vizată va fi informată asupra motivului de amînare a răspunsului, de asemenea i se va comunica şi procedura care va urma pentru soluţionarea 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 posibilităţii, cu condiţia de a nu prejudicia drepturile terţilor (persoana vizată va putea vizualiza doar propria imagine, imaginile altor persoanelor care pot apărea în înregistrare vor fi editate astfel încît să nu fie posibilă recunoaşterea/identificarea lor). în cazul unei asemenea solicitări, persoana vizată este obligată:

a) să se identifice dincolo de orice suspiciune (să prezinte actul de identitate cînd participă la vizionare), să menţioneze data, ora, locaţia şi împrejurările în care a fost înregistrată de camerele de supraveghere.

b) De asemenea, persoana vizată va prezenta şi o fotografie recentă astfel încît utilizatorii desemnaţi să o poată identifica mai uşor în imaginile filmate.

c) Persoana va putea vizualiza doar propria imagine, imaginile persoanelor care pot apărea în înregistrare vor fi editate astfel încît să nu fie posibilă recunoaşterea/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 înscrieri 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 cînd, 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	Funcţia	Am luat cunoştinţă (semnătura)	Data
Groza Ruslan	primar		
Ardeleanu Viorica	secretara consiliului		
Guzun Ana	contabila - şefa		
Odagiu Maria	specialistă		
Iacicurinscaia Olga	Muncitoare auxiliară		
Ianciu Dumitru	Muncitor auxiliar		
Fosa Svetlana	Muncitoare auxiliară		
Iacicurinscaia Olga	Îngrijitoare de încăperi		