



DECIZIE
nr. 06/05
din 12.10.2022

Cu privire la aprobarea actelor regulatorii
în domeniul prelucrării datelor cu caracter personal
în cadrul Primăriei orașului Cimișlia

În conformitate art. 4 alin. (3) din Legea privind descentralizarea administrativă nr. 435 din 28.12.2006 art. 3 alin. (2), art. 14 alin (3) ale Legii privind administrația publică locală nr. 436 din 28.12.2006, art. 8-13, art. 15 ale Legii privind transparența în procesul decizional nr. 239 din 13.11.2008, Legea contabilității nr. 113 din 27.04.2007, Legea privind protecția datelor cu caracter personal nr. 133 din 08.07.2011, art. 10, art. 118-126 din Codul Administrativ al Republicii Moldova nr. 116 din 19.07.2018, art. 91-94 din Codul muncii al Republicii Moldova, Hotărârea de Guvern privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal nr. 1123 din 14.12.2010, ținând cont de cerințele cu privire la asigurarea securității datelor cu caracter personal, **Consiliul orășenesc Cimișlia, DECIDE:**

1. Se aprobă Politica de Securitate privind protecția datelor cu caracter personal în cadrul sistemelor informaționale gestionate de Primăria orașului Cimișlia, conform Anexei nr. 1.
2. Se aprobă Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență al corespondenței și petițiilor parvenite în adresa Primăriei orașului Cimișlia, conform Anexei nr. 2.
3. Se aprobă Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență a resurselor umane în cadrul Primăriei orașului Cimișlia, conform Anexei nr. 3.
4. Se aprobă Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență contabilă în cadrul Primăriei orașului Cimișlia, conform Anexei nr. 4.
5. Executarea prezentei Decizii se pune în seama primarului orașului Cimișlia, Dl Sergiu Andronachi.
6. Controlul executării prezentei Decizii se pune în sarcina Comisiei de specialitate drept, disciplină, învățământ, cultură, protecție social, sănătate, turism și culte.
7. Prezenta Decizie va fi publicată în Registrul de Stat al Actelor Locale și pe pagina oficială a Primăriei orașului Cimișlia.

Președintele ședinței

Larisa BORODIN

Secretarul Consiliului

Cristina PÎNZARI



Anexa nr. 1
La Decizia nr. 06/05 din 12.10.2022
“Cu privire la aprobarea acelor regulatorii în
domeniul prelucrării datelor cu caracter personal
în cadrul Primăriei oraşului Cimişlia”

POLITICA DE SECURITATE
PRIVIND PROTECŢIA DATELOR CU CARACTER PERSONAL LA PRELUCRAREA
ACESTORA ÎN CADRUL SISTEMELOR INFORMAŢIONALE GESTIONATE DE
PRIMĂRIA ORAŞULUI CIMIŞLIA

I. PREAMBUL

La prelucrarea datelor cu caracter personal în cadrul entităţii sunt aplicate principiile prevăzute de actele **internationale** - 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, aprobate prin Hotărârea Guvernului nr. 1123 din 14 decembrie 2010 şi alte acte legislative/normative de profil.

II. INTRODUCERE

PRIMĂRIA ORAŞULUI CIMIŞLIA are sediul înregistrat în **or. Cimişlia, str. Ştefan cel Mare 14, MD-4101**. Prezenta Politică de securitate privind protecţia datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale (în continuare – Politică) este aprobată de către **PRIMĂRIA ORAŞULUI CIMIŞLIA** care acţionează în baza legislaţiei.

Prezenta Politică este aprobată, inclusiv, în vederea conformării **PRIMĂRIEI ORAŞULUI CIMIŞLIA** cu prevederile Hotărârii Guvernului Republicii Moldova nr. 1123 din data de 14 decembrie 2010 "privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal" şi Legii Republicii Moldova nr.133 din 08.07.2011 "privind protecţia datelor cu caracter personal".

III. NOȚIUNI GENERALE

În prezenta Politică de Securitate, sînt definite/utilizate următoarele noţiuni:

Date cu caracter personal – orice informaţie referitoare la o persoană fizică identificată sau identificabilă (subiect al datelor cu caracter personal). Persoana identificabilă este persoana care poate fi identificată, direct sau indirect, prin referire la un număr de identificare sau la unul ori mai multe elemente specifice identităţii sale fizice, fiziologice, psihice, economice, culturale sau sociale;

Categorii speciale de date cu caracter personal – datele care dezvăluie originea rasială sau etnică a persoanei, convingerile ei politice, religioase sau filozofice, apartenenţa socială, datele privind starea de sănătate sau viaţa sexuală, precum şi cele referitoare la condamnările penale, măsurile procesuale de constrîngere sau sancţiunile contravenţionale;

Operator – persoana fizică sau persoana juridică de drept public sau de drept privat, inclusiv autoritatea publică, orice altă instituţie ori organizaţie care, în mod individual sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal prevăzute în mod expres de legislaţia în vigoare;

Persoană împuternicită de către operator – persoana fizică sau persoana juridică de drept public ori de drept privat, inclusiv autoritatea publică şi subdiviziunile ei teritoriale, care prelucrează date cu caracter personal în numele şi pe seama operatorului, pe baza instrucţiunilor permise de la operator;

Autentificare – verificarea identicatorului atribuit subiectului de acces, confirmarea autenticităţii;

Control de securitate – acțiuni întreprinse de către **PRIMĂRIA ORAȘULUI CIMIȘLIA** Hotărârii Guvernului Republicii Moldova nr. 1123 din data de 14 decembrie 2010 în vederea asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaționale și/sau registrelor ținute;

Fișiere temporare – ansamblu de date sau informații pe suport digital creat pentru o perioadă de timp limitat până la inițierea îndeplinirii sarcinilor pentru care au fost desemnate;

Identificare – atribuirea unui identificator subiecților și obiectelor de acces și/sau compararea identificatorului prezentat cu lista identificatoarelor atribuite;

Integritate – certitudinea, necontradictorialitatea și actualitatea informației care conține date cu caracter personal, protecția ei de distrugere și modificare neautorizată;

Mijloace de protecție criptografică a informației care conține date cu caracter personal – mijloace tehnice, de program și tehnico-aplicative, sisteme și complexe de sisteme ce realizează algoritmi de conversie criptografică a informației care conține date cu caracter personal, destinate să asigure integritatea și confidențialitatea informației în procesul de prelucrare, depozitare și transmitere a acesteia prin canalele de comunicații;

Nivel de protecție – nivel de securitate proporțional riscului pe care îl comportă prelucrarea față de datele cu caracter personal respective, precum și față de drepturile și libertățile persoanelor, elaborat și actualizat corespunzător nivelului dezvoltării tehnologice și costurilor implementării acestor măsuri;

Politica de securitate a datelor cu caracter personal – document, elaborat de către operatorul de date – **PRIMĂRIA ORAȘULUI CIMIȘLIA**, care oferă o descriere precisă a măsurilor de securitate și trăsăturilor de protecție selectate pentru securitatea datelor, ținându-se cont de potențialele pericole pentru datele cu caracter personal prelucrate și riscurile reale la care sînt expuse acestea;

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

Persoana responsabilă de politica de securitate a datelor cu caracter personal – persoana responsabilă de funcționarea corespunzătoare a sistemului complex de protecție a informației care conține date cu caracter personal, precum și de elaborarea, implementarea și monitorizarea respectării prevederilor politicii de securitate a deținătorului de date cu caracter personal;

Protecția informației contra acțiunilor neintenționate – ansamblu de măsuri orientate spre prevenirea acțiunilor neintenționate, provocate de erorile utilizatorului, defectele mijloacelor tehnico-aplicative, fenomenele naturii sau alte cauze ce nu au ca scop direct modificarea informației, dar care conduc la distorsiunea, distrugerea, copierea, blocarea accesului la informație, precum și la pierderea, distrugerea acesteia sau la defectarea suportului material al informației care conține date cu caracter personal;

Purtător de date cu caracter personal – suport magnetic, optic, laser, de hîrtie sau alt suport al informației, pe care se creează, se fixează, se transmite, se recepționează, se păstrează sau, în alt mod, se utilizează documentul și care permite reproducerea acestuia;

Restaurarea datelor – procedurile cu privire la reconstituirea/prestabilirea datelor cu caracter personal în starea în care se aflau până la momentul pierderii sau distrugerii acestora;

Tehnologie informațională – totalitatea metodelor, procedurilor și mijloacelor de prelucrare și transmitere a informației care conține date cu caracter personal și regulile de aplicare a acesteia;

Utilizator – persoana care acționează sub autoritatea deținătorului de date cu caracter personal, cu drept recunoscut de acces la sistemele informaționale de date cu caracter personal;

Sesiune de lucru – perioada care durează din momentul pornirii calculatorului și aplicației de utilizare a resursei informaționale sau din momentul pornirii resursei informaționale și până la momentul opririi acestora;

Sistem informațional de date cu caracter personal – totalitatea resurselor și tehnologiilor informaționale interdependente, de metode și de personal, destinată păstrării, prelucrării și furnizării de informație care conține date cu caracter personal;

Prelucrarea datelor cu caracter personal – orice operațiune sau serie de operațiuni care se efectuează asupra datelor cu caracter personal prin mijloace automatizate sau neautomatizate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, păstrarea, restabilirea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ștergerea sau distrugerea;

Stocare – păstrarea pe orice fel de suport a datelor cu caracter personal;

sistem de evidență a datelor cu caracter personal – orice serie structurată de date cu caracter personal accesibile conform unor criterii specifice, fie că este centralizată, descentralizată ori repartizată după criterii funcționale sau geografice;

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

Depersonalizarea datelor – modificarea datelor cu caracter personal astfel încât detaliile privind circumstanțele personale sau materiale să nu mai permită atribuirea acestora unei persoane fizice identificate sau identificabile ori să permită atribuirea doar în condițiile unei investigații care necesită cheltuieli disproporționate de timp, mijloace și forță de muncă.

IV. OBIECTIVELE POLITICII DE SECURITATE

Obiectivele principale ale Politicii sunt disponibilitatea, integritatea și confidențialitatea tuturor informațiilor, inclusiv datelor cu caracter personal prelucrate de **PRIMĂRIA ORAȘULUI CIMIȘLIA**, atât în cadrul prelucrării manuale, cât și sistemelor și proceselor de tehnologie informațională. Securitatea reprezintă o componentă esențială a derulării optime a proceselor bazate pe IT în cadrul **PRIMĂRIEI ORAȘULUI CIMIȘLIA**. Baza unei securități IT adecvate o constituie respectarea prezentei Politici. Aceasta cuprinde cerințe și reguli pentru protecția tuturor informațiilor, inclusiv datele cu caracter personal, sistemelor și proceselor IT împotriva influențelor naturale, erorilor umane și tehnice, precum și împotriva acțiunilor deliberate care pot provoca pagube materiale, respectiv imateriale, sau care pot duce la încălcări ale legislației. Având în vedere că siguranța IT nu poate fi garantată exclusiv cu ajutorul unor sisteme tehnice, prezenta Politică vizează, de asemenea, aspecte de ordin organizatorico-juridic și de altă natură.

PRIMĂRIA ORAȘULUI CIMIȘLIA va proteja datele cu caracter personal atât a petiționarilor/vizitatorilor, cât și a angajaților săi.

Reglementările prezentei Politici reprezintă un standard minim pentru **PRIMĂRIA ORAȘULUI CIMIȘLIA**, inclusiv toți angajații **PRIMĂRIEI ORAȘULUI CIMIȘLIA**. Pornind de la această reglementare, toți angajații **PRIMĂRIEI ORAȘULUI CIMIȘLIA** urmează să respecte strict prevederile Politicii și regulilor interne ale **PRIMĂRIEI ORAȘULUI CIMIȘLIA** privind protecția datelor cu caracter personal și sistemelor IT.

V. DISPOZIȚII PRIVIND IERARHIA ȘI RESPONSABILITATEA PERSOANEI RESPONSABIL DE POLITICA DE SECURITATE

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

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

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

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

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

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

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

VI. MIJLOACE SUPUSE PRINCIPILOR DE PROTECTIE A DATELOR CU CARACTERE PERSONAL

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

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

- suporturi magnetice, optice, laser sau alte suporturi ale informației electronice, masive informaționale și baze de date;

- sistemele informaționale, rețelele, sistemele operaționale, sistemele de gestionare a bazelor de date și alte aplicații, sistemele de telecomunicații, inclusiv mijloacele de confecționare și multiplicare a documentelor și alte mijloace tehnice de prelucrare a informației.

VII. MĂSURILE DE PROTECȚIE A DATELOR CU CARACTER PERSONAL

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

- 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;
- neadmiterea dezvăluirii terților a informației cu accesibilitate limitată;
- eficientizarea resurselor informaționale atât pe suport de hârtie cât și cel în format electronic.

VIII. METODE DE PROTECȚIE A DATELOR CU CARACTER PERSONAL PRELUCRATE ÎN SISTEMLILE INFORMAȚIONALE

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

- preîntâmpinarea conexiunilor neautorizate la rețelele telecomunicaționale și interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste rețele,
- excluderea accesului neautorizat la datele cu caracter personal prelucrate;
- preîntâmpinarea acțiunilor speciale tehnice și de program, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program;
- 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,
- 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,
- 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,
- 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.

IX. PROCEDURI ORGANIZATORICE ȘI TEHNICE

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

1. Măsurile generale de administrare a securității informaționale

- a) În cazul neutilizării temporare a purtătorilor de informație pe suport de hârtie sau electronici (digitali) care conțin date cu caracter personal, aceștia se păstrează în safeuri sau dulapuri metalice care se încuie.
- b) Computerele, terminalele de acces și imprimantele sînt deconectate la terminarea sesiunilor de lucru.
- c) Este asigurată securitatea punctelor de primire/expediere a corespondenței, precum și securitatea contra accesului neautorizat la aparatele fax și de copiere.
- d) Este asigurată securitatea și accesul fizic la mijloacele de reprezentare a informației care conține date cu caracter personal, în scopul împiedicării vizualizării acestora de către persoane neautorizate.
- e) Mijloacele de prelucrare a datelor cu caracter personal, informația care conține date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal sînt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a conducerii.
- f) Toate programele utilizate în cadrul sistemului informatic respectă condițiile de licențiere.
- g) Este interzisă instalarea programelor de tip Shareware sau freeware, fără aprobarea administratorului sistemului informatic.

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

- a) Accesul în sediile/oficiile/birourile ori spațiile unde sînt amplasate sistemele informaționale de date cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară, conform listei sau însemnelor corespunzătoare (insigne, ecusoane, cartele de identificare).
- b) Se asigură administrarea și monitorizarea accesului fizic în toate punctele de acces la sistemele informaționale de date cu caracter personal, inclusiv se reacționează la încălcarea regimului de acces.
- c) Perimetrul de securitate a **PRIMĂRIEI ORAȘULUI CIMIȘLIA** reprezintă perimetrul sediului în care se prelucrează/stochează date cu caracter personal.
- d) Perimetrul clădirii sau încăperilor în care sînt amplasate mijloacele de prelucrare a datelor cu caracter personal este integru din punct de vedere fizic, pereții exteriori ai încăperilor sînt rezistenți, intrările sunt echipate cu lacăte și semnalizare.
- e) Amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespund necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.
- f) Ușile și ferestrele se încuie în cazul în care în încăpere lipsesc membrii.
- g) Computerele, serverele, alte terminale de acces sunt amplasate în locuri cu acces limitat pentru persoane străine.
- h) Accesul în perimetrul de securitate a clădirii **PRIMĂRIEI ORAȘULUI CIMIȘLIA** unde se prelucrează/stochează date cu caracter personal cu utilaje foto/video neautorizate este interzis, ținînd cont de necesitatea asigurării regimului de confidențialitate și securitate a prelucrării datelor cu caracter personal, prevăzut de art. 29 și art. 30 ale Legii privind protecția datelor cu caracter personal, precum și pct. 26 din Cerințe.

- i) Folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare în perimetrul de securitate este admisă doar în cazul prezenței unei permisiuni speciale a conducerii.

3. Identificarea și autentificarea utilizatorilor

- a) Este efectuată identificarea și autentificarea utilizatorilor sistemelor informaționale de date cu caracter personal și a proceselor executate în numele acestor utilizatori.
- b) Toți utilizatorii (inclusiv personalul care asigură susținerea tehnică, administratorii de rețea, programatorii și administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu conține semnalmente nivelului de accesibilitate al utilizatorului.
- c) Pentru confirmarea ID-ului utilizatorului sînt utilizate parole, mijloace fizice speciale de acces cu memorie (token) sau cartele cu microprocesoare, mijloace biometrice de autentificare, bazate pe caracteristici unice și individuale ale persoanei.
- d) În cazul în care contractul de muncă/raporturile de serviciu ale utilizatorului au fost încetate, suspendate sau modificate și noile sarcini nu necesită accesul la date cu caracter personal ori drepturile de acces ale utilizatorului au fost modificate, ori utilizatorul a abuzat de codurile primite în scopul comiterii unei fapte prejudiciabile, a absentat o perioadă îndelungată, codurile de identificare și autentificare se revocă sau se suspendă de administratorul I.T.

4. Identificarea și autentificarea echipamentului

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

5. Administrarea identificatorilor utilizatorilor

Administrarea identificatorilor utilizatorilor include:

- identificarea univocă a fiecărui utilizator,
- verificarea autenticității fiecărui utilizator.

6. Utilizarea parolilor în procesul asigurării securității informaționale

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

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

7. Controlul administrării accesului

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

8. Accesul de la distanță

- a) Toate metodele de acces de la distanță la sistemele informaționale de date cu caracter personal sunt securizate (utilizându-se VPN, criptarea, cifrarea etc.), precum și sînt documentate, supuse monitorizării și controlului.
- b) Fiecare metodă de acces de la distanță la sistemele informaționale de date cu caracter personal este autorizată de persoanele responsabile ale **PRIMĂRIEI ORAȘULUI CIMIȘLIA** și permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

9. Limitarea folosirii tehnologiilor fără fir

- a) Accesul fără fir la sistemele informaționale de date cu caracter personal este limitat la maximum, este documentat, supus monitorizării și controlului.
- b) Accesul fără fir la sistemele informaționale de date cu caracter personal este permis doar în cazul utilizării mijloacelor criptografice de protecție a informației.
- c) Folosirea tehnologiilor fără fir se autorizează de persoanele responsabile ale **PRIMĂRIEI ORAȘULUI CIMIȘLIA**.

10. Securitatea electroenergetică

- a) Echipamentul electric utilizat pentru menținerea funcționalității sistemelor informaționale de date cu caracter personal, a cablurilor electrice, este asigurat contra deteriorărilor și conectărilor nesancționate, prin montarea lor în nișe speciale.
- b) În cazul apariției situațiilor excepționale, de avarie sau de forță majoră, este asigurată posibilitatea deconectării electricității la sistemele informaționale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component TI.
- c) Sunt implementate sisteme automatizate de depistare și semnalizare a incendiilor în birourile unde sînt amplasate sistemele informaționale de date cu caracter personal și mijloacele de prelucrare a datelor cu caracter personal.

11. Controlul instalării și scoaterii componentelor T.I.

- a) Este exercitat controlul și evidența instalării și scoaterii mijloacelor de program, mijloacelor tehnice și celor tehnice de program, utilizate în cadrul sistemelor informaționale de date cu caracter personal.
- b) Informațiile, care conțin date cu caracter personal și care se conțin pe purtătorii de informații, se distrug fizic sau se transcriu și se nimicesc prin metode sigure, evitîndu-se folosirea funcțiilor standarde de nimicire.

12. Dezvăluirea datelor cu caracter personal

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

- b) Dezvăluirea prin transmitere a datelor cu caracter personal prin rețele comunicaționale ce nu corespund Cerințelor, (*spre exemplu: expedierea informației prin intermediul e-mail-urilor personale de tipul @gmail.com, @mail.ru, @yahoo.com, etc.*) sînt interzise.
- c) Sînt interzise operațiunile de dezvăluire a datelor cu caracter personal între **PRIMĂRIA ORAȘULUI CIMIȘLIA** și alte entități care sunt amplasate geografic în stînga Nistrului care refuză să se supună juridic legislației Republicii Moldova, reieșind din considerentul că la moment nu există posibilitatea exercitării unui control efectiv asupra acestei părți teritoriale, inclusiv în partea ce ține de conformitatea prelucrării datelor cu caracter personal prevederilor Legii privind protecția datelor cu caracter personal.
- d) Procedura dezvăluirii prin transmitere a datelor cu caracter personal stocate pe suport de hîrtie și/sau suport digital, peste hotarele Republicii Moldova, urmează a fi reglementată prin act normativ instituțional/acord bilateral luîndu-se în considerare necesitatea asigurării unui nivel adecvat de protecție a datelor cu caracter personal.
- e) Transmiterea transfrontalieră a datelor cu caracter personal este efectuată în strictă corespundere cu prevederile art. 32 al Legii privind protecția datelor cu caracter personal, în special în cazurile cînd tratatul internațional în baza căruia se efectuează transmiterea nu conține garanții privind protecția drepturilor subiectului de date cu caracter personal.
- f) Volumul și categoriile datelor cu caracter personal colectate în scopul ținerii evidenței **PRIMĂRIEI ORAȘULUI CIMIȘLIA**, este limitat la strictul necesar pentru realizarea scopurilor declarate.
- g) Acces la sistemele informaționale gestionate în cadrul **PRIMĂRIEI ORAȘULUI CIMIȘLIA**, din partea Procuraturii Generale (*după caz procuraturile teritoriale/specializate*), Ministerului Afacerilor Interne, Centrului Național Anticorupție etc., va fi permis doar în cazul în care solicitarea va corespunde prevederilor art. 15 și art. 212 Cod de procedură penală. Se explică că în conformitate cu prevederile art.157 Cod de procedură penală, documentele în orice formă (*scrisă, audio, video, electronică etc.*) care provin de la persoane oficiale fizice sau juridice dacă în ele sînt expuse ori adevărate circumstanțe care au importanță pentru cauză, (*inclusiv informația stocată în auditul sistemelor informaționale și de evidență*), pot fi solicitate printr-un demers al organului de urmărire penală în cadrul urmăririi penale sau în procesul judecării cauzei. În acest caz, însă, urmează a fi respectate prevederile art.214 Cod de procedură penală, care stipulează că în cursul procesului penal nu pot fi administrate, utilizate și răspîndite fără necesitate informație oficială cu accesibilitate limitată.

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

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

În cazul în care, avocatul sau persoana împuternicită solicită să ia cunoștință cu fișa personală a clientului, aceștia urmează a fi informați în scris despre obligațiile ce le revin în conformitate

cu prevederile art. 15 Cod de procedură penală, art. 29 și 30 ale Legii privind protecția datelor cu caracter personal, inclusiv despre răspunderea prevăzută de art. 74¹ Cod contravențional.

13. Drepturile subiecților de date cu caracter personal

- a) În cazul în care datele cu caracter personal sînt colectate direct de la subiectul acestor date, în conformitate cu prevederile art.12 al Legii privind protecția datelor cu caracter personal, persoanei necesită a-i fi furnizate următoarele informații, exceptînd cazul în care el deține deja informațiile respective:
 - privind identitatea operatorului, a persoanei împuternicite de către operator, sau, după caz, a reprezentantului operatorului (*denumirea, adresa juridică, IDNO-ul*);
 - datele de contact ale responsabilului de protecția datelor personale, după caz;
 - privind scopul concret al prelucrării datelor cu caracter personal colectate;
 - privind destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
- existența drepturilor la informare și de acces la datele colectate; de intervenție asupra datelor (*în special de a rectifica, actualiza, bloca sau șterge datele cu caracter personal a căror prelucrare contravine legii datorită caracterului incomplet sau inexact al acestora*) și de opoziție, precum și condițiile în care aceste drepturi pot fi exercitate; dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sînt obligatorii sau voluntare, inclusiv consecințele posibile ale refuzului de a răspunde la întrebările prin care se colectează informația.
- b) Subiecților de date cu caracter personal le este asigurat dreptul de acces și posibilitatea de a lua cunoștință cu actele întocmite în scopul verificării corectitudinii întocmirii lor, contestării împotriva neincluserii sau includerii incorecte a unor date, precum și împotriva altor erori comise la înscrierea datelor despre sine. În acest sens, persoanele responsabile de prelucrarea datelor cu caracter personal, vor asigura accesul persoanei doar la datele cu caracter personal care-o vizează nemijlocit, fiind exclusă posibilitatea consultării datelor cu caracter personal ce vizează alți subiecți, conținute în fișele personale (*alte materiale*), cu excepția cazurilor în care solicitantii își realizează un interes legitim care nu prejudiciază interesele sau drepturile și libertățile fundamentale ale subiectului datelor cu caracter personal.
- c) Dreptul de informare este asigurat de către operatorul datelor cu caracter personal (*sau entitățile ce asigură mentenanța sistemului și sau prestează servicii externalizate ale operatorului*) tuturor persoanelor supuse prelucrării.
- d) În cazul realizării de către subiectul de date cu caracter personal a dreptului de intervenție, datele inexacte vor fi actualizate prin rectificare sau ștergere, ca bază servind doar surse legale (*acte de identitate, de stare civilă, resurse informaționale principale de stat etc.*), modificarea urmînd a fi efectuată în toate sistemele informaționale și de evidență gestionate.

14. Stocarea, păstrarea și distrugerea datelor cu caracter personal prelucrate

- a) Accesul în spațiile/perimetrul unde sînt amplasate sistemele informaționale și de evidență a datelor cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară conform politicii de securitate instituționale /regulamentelor departamentale aprobate.
- b) Stocarea și păstrarea formatului electronic al datelor cu caracter personal, structurate în sisteme de evidență, în computere care sînt conectate la internet, nu sînt echipate cu mijloace de protecție speciale tehnice și de program și nu au instalate programe licențiate, programe antivirus, sisteme de control al securității soft-ului, de asigurare a efectuării periodice a copiilor de siguranță și de efectuare a auditului - este interzisă.

- c) Introducerea în perimetrul de securitate instituțional și utilizarea calculatoarelor personale ori a purtătorilor de informații în scopuri de serviciu este interzisă. Mai mult, accesul la computerele din dotare sunt protejate/restricționate prin crearea profilurilor de utilizatori, iar drepturile de administrator sînt încredințate doar persoanei responsabile pentru implementarea politicii de securitate desemnate din cadrul **PRIMĂRIEI ORAȘULUI CIMIȘLIA**.
- d) Stocarea datelor cu caracter personal pe suport magnetic, optic, laser, de hîrtie sau alt suport al informației, pe care se creează, se fixează, se transmite, se recepționează, se păstrează sau, în alt mod, se utilizează documentul și care permite reproducerea acestuia, este asigurat prin plasarea acestora în safeuri sau dulapuri metalice care se încuie. Scoaterea, fără autorizare, a purtătorilor de date cu caracter personal din perimetrul de securitate al operatorului este interzisă.

15. Auditul sistemelor informaționale gestionate

- a) Se efectuează înregistrarea tentativelor de intrare/ieșire a utilizatorului în sistem, conform următorilor parametri:
- data și timpul tentativei intrării/ieșirii;
 - ID-ul utilizatorului;
 - rezultatul tentativei de intrare/ieșire - pozitivă sau negativă.
- b) Se efectuează înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:
- data și timpul tentativei de obținere a accesului (executate a operațiunii),
 - denumirea (identificatorul) aplicației sau procesului, o ID-ul utilizatorului,
 - specificațiile resursei protejate (identificator, nume logic, nume fișier, număr etc.),
 - tipul operațiunii solicitate (citire, înregistrare, ștergere etc.),
 - rezultatul tentativei de obținere a accesului (executare a operațiunii) — pozitivă sau negativă.
- c) Este efectuată înregistrarea modificărilor drepturilor de acces (competențelor) utilizatorului și statutului obiectelor de acces, conform următorilor parametri:
- data și timpul modificării competențelor,
 - ID-ul administratorului care a efectuat modificările,
 - ID-ul utilizatorului și competențele acestuia sau specificarea obiectelor de acces și statutul nou al acestora.
- d) Se efectuează înregistrarea ieșirii din sistem a informației care conține date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecților și statutul obiectelor de acces, conform următorilor parametri:
- data și timpul eliberării,
 - denumirea informației și căile de acces la aceasta,
 - specificarea echipamentului (dispozitivului) care a eliberat informația (numele logic),
 - ID-ul utilizatorului, care a solicitat informația.

16. Asigurarea protecției contra programelor dăunătoare (virusurilor)

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

17. Testarea posibilităților funcționale de asigurare a securității sistemelor informaționale de date cu caracter personal

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

18. Gestionarea incidentelor de securitate

- a) Personalul care asigură exploatarea sistemelor informaționale de date cu caracter personal trece, minimum o dată în an, instruirea referitor la responsabilitățile și obligațiile în cazul executării acțiunilor de gestionare și reacționare la incidentele de securitate.
- b) Personalul **PRIMĂRIEI ORAȘULUI CIMIȘLIA** informează neîntârziat conducerea despre incidentele care încalcă securitatea sistemelor informaționale de date cu caracter personal.
- c) Prelucrarea incidentelor include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor și restabilirea securității.
- d) Până la 31 ianuarie a fiecărui an, operatorul de date cu caracter personal informează în scris Centrul Național pentru Protecția Datelor cu Caracter Personal despre incidentele de securitate constatate.
- e) "În cazul producerii incidentelor de securitate în cadrul **PRIMĂRIEI ORAȘULUI CIMIȘLIA** persoana responsabilă va întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia și va înlătura cauzele incidentului de securitate cu informarea, în termen de 72 ore din momentul producerii incidentului de securitate, a Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova.
- f) În cadrul controalelor efectuate de Centrul Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova i se va oferi suportul necesar și asigurat accesul la informațiile necesare relevante obiectului controlului."

19. Marcarea documentelor

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

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

20. Responsabilitatea pentru asigurarea securității datelor cu caracter personal precum și a informațiilor cu accesibilitate limitată

Operatorul de date cu caracter personal, persoana împuternicită de către operator, persoanele terțe după caz, pentru nerespectarea dispozițiilor Politicii de securitate - poartă răspundere civilă (Codul civil), contravențională (art. 74¹ Cod contravențional) și penală (art. art. 177, 178, 180 Cod penal).

Anexă

**la Politica de securitate privind protecția datelor cu
caracter personal la prelucrarea acestora în cadrul sistemelor
informaționale gestionate de Primăria orașului Cimișlia**

**LISTA ANGAJAȚILOR FAMILIARIZAȚI CU PREVEDERILE POLITICII DE
SECURITATE INFORMAȚIONALĂ PRIVIND PROTECȚIA DATELOR CU CARACTER
PERSONAL LA PRELUCRAREA ACESTORA ÎN CADRUL SISTEMELOR
INFORMAȚIONALE GESTIONATE DE PRIMĂRIA ORAȘULUI CIMIȘLIA**

Nr.	Numele, prenumele	Funcția	Am luat cunoștință (semnătura)	Data
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				
31				
32				
33				

Secretarul Consiliului



Cristina PÎNZARI

Anexa nr. 2

La Decizia nr. 06/05 din 12.10.2022

**“Cu privire la aprobarea acelor regulatorii în
domeniul prelucrării datelor cu caracter personal
în cadrul Primăriei oraşului Cimişlia”**

**REGULAMENTUL
PRIVIND PRELUCRAREA INFORMAȚIILOR CE CONȚIN DATE
CU CARACTER PERSONAL ÎN SISTEMUL DE EVIDENȚĂ A
CORESPONDENȚEI ȘI PETIȚIILOR PARVENITE ÎN ADRESA
PRIMĂRIEI ORAȘULUI CIMIȘLIA**

I. Dispoziții generale

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

2. Prezentul Regulament reglementează modalitatea Ținerii sistemului de evidență a corespondenței și petițiilor parvenite în adresa **PRIMĂRIEI ORAȘULUI CIMIȘLIA**, precum și procedura de înregistrare, securizare, modificare și radiere a datelor din Registru.

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

Astfel, în sensul prezentului Regulament se definesc următoarele noțiuni:

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

Cerere – orice cerere prin intermediul căreia se solicită emiterea unui act administrativ individual sau efectuarea unei operațiuni administrative;

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

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

Registrul de evidență a corespondenței – resursa informațională specializată (totalitatea informațiilor ținute în formă automatizată și manuală) care asigură evidența informației sistematizate, principalul obiectiv al căruia constă în asigurarea evidenței corespondenței parvenite la Centrul de Informare și Prestări Servicii din cadrul **PRIMĂRIEI ORAȘULUI CIMIȘLIA**;

Registrador – angajatul **PRIMĂRIEI ORAȘULUI CIMIȘLIA** împuternicit cu atribuțiile de introducere, modificare, păstrare a informației din Registru.

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

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

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

5. Angajații **PRIMĂRIEI ORAȘULUI CIMIȘLIA** poartă răspundere personală pentru îndeplinirea cerințelor prezentului Regulament, asigurarea confidențialității, securității și păstrarea în stare corespunzătoare a informației din Registru.

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

II. Condiții generale față de ținerea sistemului de evidență a corespondenței și petițiilor (Registru)

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

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

8. Persoana responsabilă din cadrul Primăriei va asigura suplimentar evidența în formă electronică a corespondenței și petițiilor parvenite la **PRIMĂRIA ORAȘULUI CIMIȘLIA**.

9. Obiectul înregistrării reprezintă informația referitor la persoanele care au depus adresări/petiții în adresa **PRIMĂRIEI ORAȘULUI CIMIȘLIA**.

10. Registru va fi ținut în limba de stat.

11. Registratorul este obligat:

- să introducă în Registru numai informație veridică, colectată de la adresant sau din alte surse neinterzise de lege;
- să asigure evidența în ordine cronologică a fiecărei înscrieri în Registru;
- să nu admită modificarea neîntemeiată a datelor introduse în Registru;
- să efectueze înregistrările în Registru astfel, încât să excludă posibilitatea de a fi radiată (ștersă, distrusă) în mod mecanic, chimic sau în orice alt mod, fără a lăsa urme vizibile ale radierii (ștergerii, distrugerii);
- să asigure accesul la informația din registru doar persoanelor care au dreptul de a primi informația respectivă, în conformitate cu legislația în vigoare;
- să prevină accesul neautorizat la datele din Registru, utilizarea, difuzarea, modificarea sau nimicirea lor ilegală.

12. Datele din registru vor reflecta starea veridică și actuală a informației privind persoanele care s-au adresat la **PRIMĂRIA ORAȘULUI CIMIȘLIA**.

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

- denumirea Registrului;
- denumirea **PRIMĂRIEI ORAȘULUI CIMIȘLIA** ca proprietar, posesor și deținător al Registrului;
- numele, prenumele și funcția persoanei responsabile de introducerea datelor în Registru și a administratorului acestuia;
- numele, prenumele și funcția persoanei care va exercita controlul asupra ținerii Registrului;
- numărul Registrului, termenele de ținere și păstrare a acestuia.

14. Datele cu caracter personal din Registru vor fi prelucrate în condițiile stabilite de legislația privind protecția datelor cu caracter personal. În acest sens, vor fi realizate măsuri de asigurare a gradului de exactitate a datelor registrului și de protecție a acestora contra distrugerii

întâmplătoare sau neautorizate, modificării, dezvăluirii sau oricăror alte acțiuni ilegale la ținerea registrului.

15. Prelucrarea datelor cu caracter personal în sistemul de evidență al corespondenței și petițiilor parvenite în adresa **PRIMĂRIEI ORAȘULUI CIMIȘLIA** se efectuează în conformitate cu prevederilor art. 5 alin. 5 lit. b), d) și e) al Legii privind protecția datelor cu caracter personal.

III. Condiții generale privind introducerea informației în Registru

16. Informația privind corespondența parvenită în adresa **PRIMĂRIEI ORAȘULUI CIMIȘLIA** va fi recepționată și înregistrată în aceeași zi de persoana responsabilă din cadrul entității și după caz, în fișele de evidență și control a acestora, iar versiunea electronică parvenită se înregistrează în arhiva electronică a **PRIMĂRIEI ORAȘULUI CIMIȘLIA**.

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

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

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

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

21. Modificările și radierile făcute în Registru se efectuează în baza deciziei și cu semnătura registratorului 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, corectările necesare și va informa despre aceasta furnizorul datelor.

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

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

25. Rectificările și radierile înscrierilor din Registru se efectuează astfel încât textul inițial să fie citabil.

IV. Condiții generale privind păstrarea și furnizarea informației din Registru

26. Păstrarea Registrului este asigurată de registrator până la adoptarea deciziei conducerii **PRIMĂRIEI ORAȘULUI CIMIȘLIA** despre lichidarea registrului, dar nu mai mult decât pe perioada stabilită de Indicatorul documentelor-tip și al termenelor lor de păstrare pentru

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

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

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

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

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

30. Registratorul este obligat să asigure accesul la informația din registru pentru angajații autorizați ai **PRIMĂRIEI ORAȘULUI CIMIȘLIA** și alte persoane, care au dreptul de a primi informația respectivă, în conformitate cu legislația în vigoare sau care demonstrează dreptul și interesul legitim de a primi aceste informații, din momentul în care acestea vor fi disponibile, dar nu mai târziu de 5 zile lucrătoare 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 ORAȘULUI CIMIȘLIA**, cu indicarea datei întocmirii/eliberării acestuia.

V. Condițiile suplimentare privind gestionarea Registrului în forma 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 ORAȘULUI CIMIȘLIA** este dusă prin intermediul mai multor Registre ținute în formă manuală, cum ar fi:

Registrul petițiilor persoane fizice,

Registrul petițiilor persoane juridice,

Registrul de eliberare a certificatelor/confirmărilor cu privire la domeniul funciar,

Registrul cadastral al deținătorilor de terenuri, loturi de pe lângă casă,

Registrul de evidență a contractelor de arendă funciară a terenurilor din rezerva primăriei,

Registrul electronic de evidență a contractelor de arendă între persoanele fizice și juridice,

Registrul de evidență a atribuirii sectoarelor de teren familiilor nou formate,

Registrul de evidență și eliberare a certificatelor privind lipsa datoriilor la bugetul local,

Registrul de evidență și eliberare a certificatelor privind salarizarea angajaților și alte acte confirmative,

Registrul de evidență și eliberare a certificatelor privind:

- componența familiei;
- deținerea cotei agricole;
- lipsa sau existența restanțelor față de bugetul Primăriei (SCITL);
- locul de trai (Forma 1);

- *existența (creșterea) în gospodăriile persoanelor fizice a producției vegetale, apicole, floricolă și animală etc;*
- *suportarea cheltuielilor funerare;*
- *lipsa persoanei în teritoriu;*
- *nașterea și educarea copiilor*

Registrul de înregistrare a scrisorilor/petițiilor de la persoanele fizice (format hârtie și electronic),

Registrul de dispoziții ale primarului,

Registrul de evidență a corespondenței de ieșire,

Registrul privind eliberarea copiilor/extraselor deciziilor Consiliului orașenesc Cimișlia,

Registrul de dispoziții pe resurse umane,

Registrul Certificatelor de urbanism informativ,

Registrul Certificatelor de urbanism pentru proiectare,

Registrul Autorizațiilor de construire,

Registrul Autorizațiilor de desființare,

Registrul Autorizațiilor de schimbare a destinației construcțiilor și amenajărilor,

Registrul eliberării autorizațiilor de funcționare a construcțiilor,

Registrul Proceselor verbale de recepție finală.

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, încheierea 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 șnuruirea 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 în 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 ORAȘULUI CIMIȘLIA**;
- rezultatul examinării: admisă/respinsă/oferte explicații de rigoare/acte de reacționare adoptate de conducerea **PRIMĂRIEI ORAȘULUI CIMIȘLIA**
- alte date relevante.

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

VI. Condiții suplimentare privind gestionarea Registrului în formă electronică

38. Ținerea în formă electronică a Registrului de evidență a corespondenței este realizat de **PRIMĂRIA ORAȘULUI CIMIȘLIA** prin intermediul unui sistem informațional automatizat special constituit - Sistemul informatic.

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

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

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

40.1. Sistemul informațional de evidență al corespondenței și petițiilor va fi gestionat, pe toată perioada ciclului de viață, în conformitate cu prevederile stabilite de Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr. 1123 din 14 decembrie 2010, în special pct. 11-13, 22, 24, 26, 28, 30, 32-33, 35-37, 39-73, 75-78, 85-86, 88, 90.

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

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

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

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

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

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

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

47. Cerințe speciale față de marcarea: toate informațiile ieșite din sistemul de evidență a corespondenței și petițiilor, care conțin date cu caracter personal, sînt supuse marcării, cu indicarea prescripțiilor pentru prelucrarea ulterioară și răspândirea acestora, inclusiv cu indicarea numărului de identificare unic al operatorului de date cu caracter personal.

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

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

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

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

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

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

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

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

55. Ușile și ferestrele sînt încuiate în cazul în care în încăpere lipsesc angajații autorizați de administrarea sistemului.

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

57. Securitatea electroenergetică: este asigurată securitatea echipamentului electric utilizat pentru menținerea funcționalității sistemului de evidență a corespondenței și petițiilor, a cablurilor electrice, inclusiv protecția acestora contra deteriorărilor și conectărilor nesancționate. În cazul apariției situațiilor excepționale, de avarie sau de forță majoră, este asigurată posibilitatea deconectării electricității la registru, inclusiv posibilitatea deconectării oricărui component TI.

58. Computerele, unde este amplasat fizic sistemul de evidență a corespondenței și petițiilor, dispun de UPS-uri, care sînt folosite pentru încheierea corectă a sesiunii de lucru a sistemelor (componentelor) în cazul deconectării de la sursa de alimentare cu energie electrică.

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

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

61. Controlul instalării și scoaterii componentelor TI: se efectuează controlul și evidența instalării și scoaterii mijloacelor de program, mijloacelor tehnice și celor tehnice de program,

utilizate în cadrul sistemului de evidență a corespondenței și petițiilor. La expirarea termenului de păstrare, informațiile, care conțin date cu caracter personal și care se conțin pe purtătorii de informații, se distrug.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- a) data și timpul tentativei intrării/ieșirii;
- b) ID-ul utilizatorului;

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

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

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

76. Rezultatele auditului securității în sistemul de evidență a corespondenței și petițiilor (operațiunile de prelucrare a informațiilor și mijloacele de efectuare a auditului), se protejează contra accesului neautorizat prin aplicarea măsurilor de securitate adecvate și asigurarea confidențialității și integrității acestora.

77. Durata minimă a stocării rezultatelor auditului securității în sistemul de evidență a corespondenței și petițiilor constituie 2 /doi/ ani, în scopul asigurării posibilității de folosire a acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigații sau procese judiciare. În cazul în care investigările sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

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

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

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

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

80. Prelucrarea incidentelor de securitate include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor și restabilirea securității. Se monitorizează și documentează, în mod permanent, incidentele de securitate în sistemul de evidență a corespondenței și petițiilor.

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

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

XII. Dispoziții finale

83. Prezentul Regulament este revizuit de **Primăria orașului Cimișlia**, și ulterior aprobat de către **Consiliul orașenesc CIMIȘLIA** periodic, însă cel puțin o dată în an, precum și la necesitate.

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

85. Regulamentul este adus la cunoștința angajaților contra semnăturii.

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

Anexă nr. 1

**la Regulamentul privind prelucrarea informațiilor ce conțin date
cu caracter personal în sistemul de evidență a
corespondenței și petițiilor parvenite în adresa
Primăriei orașului Cimișlia**

DECLARAȚIE

despre familiarizarea cu prevederile Regulamentului privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență a corespondenței și petițiilor parvenite în adresa **PRIMĂRIEI ORAȘULUI CIMIȘLIA** și asumarea obligației de a păstra confidențialitatea informației

Prin prezenta, _____ (IDNP – _____) -

(numele/ prenumele, postul angajatului)

Declar că am luat act de prevederile cu privire la asigurarea securității datelor cu caracter personal în sistemul de evidență a corespondenței și petițiilor în cadrul **PRIMĂRIEI ORAȘULUI CIMIȘLIA** și în calitate de utilizator cu drept de acces la sistemul de evidență a corespondenței și petițiilor, îmi asum obligația să nu divulg date sau informații ce constituie date cu caracter personal de care am luat cunoștință în perioada executării obligațiilor de funcție.

Am fost avertizat de răspunderea disciplinară, materială, administrativă și penală prevăzută de legislația în vigoare pentru încălcarea acestor prevederi.

" ____ " _____ 2022

Semnătura _____

Anexă nr. 2

la Regulamentul privind prelucrarea informațiilor ce conțin date
cu caracter personal în sistemul de evidență a
corespondenței și petițiilor parvenite în adresa
Primăriei orașului Cimișlia

**LISTA ANGAJAȚILOR FAMILIARIZAȚI CU PREVEDERILE REGULAMENTULUI
PRIVIND PRELUCRAREA INFORMAȚIILOR CE CONȚIN DATE
CU CARACTER PERSONAL ÎN SISTEMUL DE EVIDENȚĂ A
CORESPONDENȚEI ȘI PETIȚIILOR PARVENITE ÎN ADRESA
PRIMĂRIEI ORAȘULUI CIMIȘLIA**

Nr.	Numele, prenumele	Funcția	Am luat cunoștință (semnătura)	Data
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				

Secretarul Consiliului



Cristina PÎNZARI

Anexa nr. 3
La Decizia nr. 06/05 din 12.10.2022
“Cu privire la aprobarea acelor regulatorii în
domeniul prelucrării datelor cu caracter personal
în cadrul Primăriei oraşului Cimişlia”

REGULAMENT
cu privire la asigurarea securităţii datelor cu caracter personal în sistemul
de evidenţă a resurselor umane în cadrul PRIMĂRIEI ORAŞULUI CIMIŞLIA

I. DISPOZIȚII GENERALE

1. Regulamentul cu privire la asigurarea securității datelor cu caracter personal în Sistemul de evidență a resurselor umane, în cadrul **PRIMĂRIEI ORAȘULUI CIMIȘLIA** stabilește responsabilitățile persoanelor din subdiviziunea Resurse Umane a Primăriei ce au acces la securitatea datelor cu caracter personal în cadrul acestui sistem de evidență.

2. Persoanele din subdiviziunile Resurse Umane ale **PRIMĂRIEI ORAȘULUI CIMIȘLIA** ce au acces la datele cu caracter personal nu vor depăși limitele stabilite de Politica de securitate a **PRIMĂRIEI ORAȘULUI CIMIȘLIA**, precum și normele legale stabilite prin prevederile Legii nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal, Hotărârii Guvernului nr.1123 din 14 decembrie 2010 „Privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal”, precum și a prevederilor prezentului Regulament.

II. SCOPUL PRELUCRĂRII INFORMAȚIILOR CE CONȚIN DATE CU CARACTER PERSONAL

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

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

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

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

a) prelucrarea informației privind modificările survenite la prelucrarea datelor cu caracter personal ce vizează angajații și care au impact asupra executării contractului individual de muncă;

- b) stabilirea sistemului de salarizare a personalului în conformitate cu legislația în vigoare a Republicii Moldova;
 - c) prelucrarea certificatelor de concedii medicale ale angajaților în vederea stabilirii indemnizațiilor corespunzătoare;
 - d) elaborarea, înregistrarea și prelucrarea ordinelor rectorului referitor la personal;
 - e) prezentarea la CNAM a evidenței nominale a noilor angajați și a celor concediați, format hârtie și format electronic;
 - f) înregistrarea și prelucrarea dosarelor pentru concursul de suplinire a posturilor vacante;
 - g) întocmirea declarației persoanei asigurate REV 1 pentru fiecare angajat și transmiterea acestora Casei Teritoriale de Asigurări Sociale, Centru pe suport de hârtie;
 - h) asistarea procesului (prin furnizarea informației necesare) pentru completarea periodică (lunară) a raportului și dării de seamă privind venitul achitat și impozitul pe venit reținut din acesta;
 - i) completarea lunară, trimestrială și anuală a rapoartelor statistice referitoare la personalul primăriei;
 - j) prelucrarea cererilor și a documentelor necesare executării contractelor individuale de muncă;
 - k) eliberarea certificatelor care atestă calitatea de salariat al primăriei la cererea angajaților;
 - l) ținerea dosarelor personale ale salariaților;
 - m) înregistrarea datelor în carnetele de muncă;
 - n) alte scopuri, necesare realizării activităților ce țin de gestionarea resurselor umane.
6. Datele cu caracter personal ce fac obiectul reglementării prezentului Regulament vor fi stocate de către responsabilii din cadrul Primăriei, astfel încât să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sunt prelucrate, iar la expirarea termenului respectiv, înregistrările se vor distruge/șterge, în funcție de suportul pe care au fost efectuate. În cazul obligațiilor expres prevăzute de lege acestea pot rămâne la păstrare primind statut de document de arhivă.
7. Orice utilizare a datelor cu caracter personal, introduse în sistemul de evidență a Resurselor Umane în alte scopuri decât cele menționate mai sus este interzisă.
8. Prelucrarea datelor cu caracter personal în sistemul de evidență a resurselor umane se efectuează în conformitate cu prevederilor art. 5 alin. 5 lit. a), b) și e) al Legii privind protecția datelor cu caracter personal.

III. LOCAȚIA ȘI DESCRIEREA SISTEMULUI DE EVIDENȚĂ A RESURSELOR UMANE

9. Datele cu caracter personal conținute în sistemul de evidență a Resurselor Umane în cadrul entității se prelucrează și se stochează:
- 1) pe suport de hârtie;
 - 2) în format electronic:
- a) Software – Sistemul de evidență a resurselor umane 1C - contabilitate, versiunea 8.3
 - b) Hardware – Nr. de inventariere – 31490188, 31490215; 31490246/3, 31490246/4
10. Prelucrarea informațiilor în sistemul de evidență resurse umane pe suport de hârtie este structurată după criteriul “mape-dosare”, fiind păstrate în dulapuri, care sânt amplasate fizic în biroul specialistului resurse umane a **PRIMĂRIEI ORAȘULUI CIMIȘLIA, or. Cimișlia, str. Ștefan cel Mare 14, MD-4101.**

IV. DURATA DE STOCARE

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

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

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

IV. DREPTURILE ANGAJAȚILOR SI PERSOANELOR VIZATE

13. Primăria în calitate de operator de date cu caracter personal, garantează respectarea drepturilor privind protecția datelor cu caracter personal ce le revin angajaților, precum și, după caz, altor persoane vizate.

14. În conformitate cu principiile de protecție a datelor cu caracter personal, persoanele vizate beneficiază de următoarele drepturi: la informare, de acces la date, de intervenție, de opoziție asupra datelor cu caracter personal ce-i vizează, precum și dreptul de a se adresa în justiție.

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

16. Acordarea dreptului de acces al angajaților la informațiile ce-i vizează se efectuează doar prin solicitarea expresă, în formă scrisă, cu acordul nemijlocit al primarului. Informațiile furnizate vor fi acordate astfel, încât să nu prejudicieze drepturile terților. Persoanele care solicită date cu caracter personal trebuie să indice scopul solicitării, precum și perioada concretă pentru care solicită informațiile.

17. Există posibilitatea refuzării dreptului de acces în situația în care se aplică excepțiile prevăzute de lege. Necesitatea de a restricționa accesul se poate impune în cazul în care există obligația de a proteja drepturile și libertățile unor terțe persoane, de exemplu, dacă în informațiile solicitate apar și alte persoane și nu există posibilitatea de a obține consimțământul acestora sau nu pot fi extrase, prin editare, datele cu caracter personal nerelevante.

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

18. Măsurile generale de administrare a securității informaționale:

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

19. Măsurile de protecție a datelor cu caracter personal, prelucrate în sistemul de evidență a Resurselor Umane, se 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 nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal.*

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

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

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

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

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

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

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

28. Securitatea electroenergetică: este asigurată securitatea echipamentului electric utilizat pentru menținerea funcționalității sistemului de evidență a Resurselor Umane, a cablurilor electrice, inclusiv protecția acestora contra deteriorărilor și conectărilor nesancționate. În cazul apariției situațiilor excepționale, de avarie sau de forță majoră, este asigurată posibilitatea deconectării electricității la sistemul de evidență a Resurselor Umane, inclusiv posibilitatea deconectării oricărui component TI.

29. Computerele, unde este amplasat fizic sistemul de evidență a Resurselor Umane, dispun de UPS-uri, care sunt folosite pentru încheierea corectă a sesiunii de lucru a sistemelor (componentelor) în cazul deconectării de la sursa de alimentare cu energie electrică.

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

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

32. Controlul instalării și scoaterii componentelor TI: se efectuează controlul și evidența instalării și scoaterii mijloacelor de program, mijloacelor tehnice și celor tehnice de program, utilizate în cadrul sistemul de evidență a Resurselor Umane. La expirarea termenului de păstrare, informațiile, care conțin date cu caracter personal și care se conțin pe purtătorii de informații, se distrug.

VI. AUDITUL SECURITĂȚII ÎN SISTEMULUI DE EVIDENȚĂ A RESURSELOR UMANE

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

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

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

35. Rezultatele auditului securității în Sistemul de Evidență al Resurselor Umane (operațiunile de prelucrare a informațiilor și mijloacele de efectuare a auditului), se protejează contra accesului neautorizat prin aplicarea măsurilor de securitate adecvate și asigurarea confidențialității și integrității acestora.

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

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

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

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

39. Prelucrarea incidentelor de securitate include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor și restabilirea securității. Se monitorizează și documentează, în mod permanent, incidentele de securitate în sistemul de evidență a Resurselor Umane.

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

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

VIII. DISPOZIȚII FINALE

42. Prezentul Regulament este aprobat de către **CONSILIUL ORĂȘENESC CIMIȘLIA** și revizuit periodic de **PRIMĂRIA ORĂȘULUI CIMIȘLIA**, la necesitate, în cazul modificării legislației în vigoare.

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

44. Modificarea și completarea prezentului Regulament se face în modul stabilit pentru aprobarea acestuia.

Anexa nr. 1
la Regulamentul cu privire la asigurarea securității datelor
cu caracter personal în sistemul
de evidență a resurselor umane în cadrul
PRIMĂRIEI ORAȘULUI CIMIȘLIA

DECLARAȚIE

despre familiarizarea cu prevederile Regulamentului cu privire la asigurarea securității datelor cu caracter personal în sistemul de evidență a resurselor umane în cadrul **PRIMĂRIEI ORAȘULUI CIMIȘLIA** și asumarea obligației de a păstra confidențialitatea informației

Prin prezenta, _____ (IDNP – _____) -

(numele/ prenumele, postul angajatului)

Declar că am luat act de prevederile cu privire la asigurarea securității datelor cu caracter personal în sistemul de evidență a resurselor umane în cadrul **PRIMĂRIEI ORAȘULUI CIMIȘLIA** și în calitate de utilizator cu drept de acces la sistemul de evidență resurse umane, îmi asum obligația să nu divulg date sau informații ce constituie date cu caracter personal de care am luat cunoștință în perioada executării obligațiilor de funcție.

Am fost avertizat de răspunderea disciplinară, materială, administrativă și penală prevăzută de legislația în vigoare pentru încălcarea acestor prevederi.

" ____ " _____ 2022

Semnătura _____

Anexa nr. 2
la Regulamentul cu privire la asigurarea securității datelor
cu caracter personal în sistemul
de evidență a resurselor umane în cadrul
PRIMĂRIEI ORAȘULUI CIMIȘLIA

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

Nr.	Numele, prenumele	Funcția	Am luat cunoștință (semnătura)	Data
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				
21.				
22.				
23.				
24.				
25.				
26.				
27.				
28.				

Secretarul Consiliului



Cristina PÎNZARI

Anexa nr. 4
La Decizia nr. 06/05 din 12.10.2022
“Cu privire la aprobarea acelor regulatorii în
domeniul prelucrării datelor cu caracter personal
în cadrul Primăriei oraşului Cimişlia”

REGULAMENTUL
PRIVIND PRELUCRAREA INFORMAȚIILOR CE CONȚIN DATE
CU CARACTER PERSONAL ÎN SISTEMUL DE EVIDENȚĂ CONTABILĂ
A PRIMĂRIEI ORAȘULUI CIMIȘLIA

I. DISPOZIȚII GENERALE

1.1. Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență contabilă (în continuare Regulament) este elaborat în vederea implementării în cadrul **PRIMĂRIEI ORAȘULUI CIMIȘLIA**, a prevederilor Legii nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal, Legii contabilității nr. 113 din 27 aprilie 2007 și a Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr.1123 din 14 decembrie 2010, precum și întru respectarea prevederilor art. 91 - 94 ale Codului muncii al Republicii Moldova.

1.2. Prezentul Regulament reglementează condițiile generale și cerințele față de prelucrarea datelor cu caracter personal ale angajaților **PRIMĂRIEI ORAȘULUI CIMIȘLIA** în cadrul sistemului de evidență contabilă.

II. SCOPUL

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

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

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

- numele, prenumele și patronimicul;
- sexul;
- numărul personal de identificare de stat (IDNP);
- data nașterii și domiciliul;
- telefon mobil/fix/fax;
- semnătura/semnătura digitală;
- date din acte de stare civilă,
- profesie, funcție
- formare profesională, diplome, studii
- cetățenia;
- situație economică sau financiară;
- imagine;
- date bancare,
- date din permisul de conducere
- sancțiuni disciplinare
- codul personal de asigurări sociale (CPAS);
- codul personal de asigurări medicale (CPAM);

- adresa domiciliului ,reședinței,
- datele privind locul de muncă,
- mărimea salariului brut și alte premii, sporuri, stimulări,
- datele privind situația familială ;
- datele din certificatele de concediu medical

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

a) Prelucrarea informației privind modificările survenite la prelucrarea datelor cu caracter personal ce vizează angajații **PRIMĂRIEI ORAȘULUI CIMIȘLIA** și care au impact asupra calculării plăților salariale, precum și a persoanelor fizice și juridice cu care **PRIMĂRIA ORAȘULUI CIMIȘLIA** intră în relații contractuale;

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

c) Prelucrarea certificatelor de concedii medicale ale angajaților în vederea stabilirii indemnizațiilor de incapacitate temporară de muncă;

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

e) Calcularea și reținerea taxelor ce țin de plățile salariale aferente angajaților: primele de asigurare obligatorie de asistență medicală, contribuțiile la bugetul asigurărilor sociale de stat, impozitul pe venit, etc.;

f) Calcularea și virarea primelor de asigurare obligatorie de asistență medicală și a contribuțiilor la bugetul asigurărilor sociale de stat, aferente plăților salariale - obligație a angajatorului;

g) Furnizarea informației necesare pentru elaborarea rapoartelor lunare privind contribuțiile de asigurare socială de stat obligatorii (forma IPC 18) și rapoartelor trimestriale privind primele de asigurare obligatorie de asistență medicală (forma IPC 18);

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

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

j) Completarea lunară, trimestrială și anuală a dărilor de seamă cu prezentarea acestora Inspectoratului Fiscal de Stat, precum și perfectarea și eliberarea informației privind veniturile calculate și achitate în folosul persoanei fizice și impozitul pe venit reținut din aceste venituri angajaților **PRIMĂRIEI ORAȘULUI CIMIȘLIA**;

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

l) Eliberarea certificatelor de salariu, la cererea angajaților;

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

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

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

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

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

III. LOCAȚIA ȘI DESCRIEREA SISTEMULUI DE EVIDENȚĂ CONTABILĂ

3.1. Datele cu caracter personal conținute în sistemul de evidență contabilă în cadrul **PRIMĂRIEI ORAȘULUI CIMIȘLIA** se prelucrează/stocchează:

1. pe suport de hârtie;

2. în format electronic:

- Software – Sistemul de evidență contabilă 1C versiunea 8.3.

- Hardware – Calculator cu Nr. de inventariere: 31490183;31490246/1, 31490184, 31490185.

3.2 Prelucrarea informațiilor în sistemul de evidență contabilă pe suport de hârtie este structurată după criteriul “mape-dosare”, fiind păstrate în dulapuri, care sânt amplasate fizic în biroul contabilității **PRIMĂRIEI ORAȘULUI CIMIȘLIA or. Cimișlia, str.Ștefan cel Mare 14, MD-4101.**

3.3. Mentenanța programului contabil 1C a **PRIMĂRIEI ORAȘULUI CIMIȘLIA** este efectuată de către compania **IP „CENTRUL DE TEHNOLOGII INFORMATIONALE ÎN FINANȚE”** fiind încheiat contract privind prestarea serviciilor informatice Nr. _____ din 01/01/2022, cu următoarele principalele atribuții stabilite companiei prestatoare:

- Efectuarea ajustărilor în program, în baza modificărilor legislației Republicii Moldova;
- Eliminarea erorilor în funcționarea programului;
- Consultarea în rezolvarea dificultăților apărute în utilizarea programului;
- Examinarea solicitărilor parvenite din partea **PRIMĂRIEI ORAȘULUI CIMIȘLIA**;
- Vizite la fața locului, la solicitarea **PRIMĂRIEI ORAȘULUI CIMIȘLIA**;
- Examinarea și nedivulgarea informației cu accesibilitate limitată ce a devenit cunoscută la prestarea acestor servicii.

IV. DURATA DE STOCARE

4.1. Prelucrarea datelor cu caracter personal în sistemul de evidență contabilă se efectuează pe perioada valabilității contractelor de achiziție publică, pe perioada activității angajaților Primăriei (din momentul semnării contractului până la finalizarea efectuării acțiunilor prevăzute de actele legislative în cazul încetării raporturilor de muncă).

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

V. DREPTURILE ANGAJAȚILOR ȘI PERSOANELOR VIZATE

5.1. PRIMĂRIA ORAȘULUI CIMIȘLIA, în calitate de operator de date cu caracter personal, garantează respectarea drepturilor privind protecția datelor cu caracter personal ce le revin angajaților, precum și, după caz, altor persoane vizate.

5.2. În conformitate cu principiile de protecție a datelor cu caracter personal, persoanele vizate beneficiază de următoarele drepturi: la informare, de acces la date, de intervenție, de opoziție asupra datelor cu caracter personal ce-i vizează, precum și dreptul de a se adresa în justiție.

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

5.4. Acordarea dreptului de acces a angajaților la informațiile ce-i vizează se efectuează doar prin solicitarea expresă, în formă scrisă, cu acordul nemijlocit al conducerii **PRIMĂRIEI ORAȘULUI CIMIȘLIA**. Informațiile furnizate vor fi acordate astfel, încât să nu prejudicieze drepturile terților. Persoanele care solicită date cu caracter personal trebuie să indice scopul solicitării, precum și perioada concretă pentru care solicită informațiile.

5.5. Există posibilitatea refuzării dreptului de acces în situația în care se aplică excepțiile prevăzute de lege. Necesitatea de a restricționa accesul se poate impune în cazul în care există obligația de a proteja drepturile și libertățile unor terțe persoane, de exemplu, dacă în informațiile solicitate apar și alte persoane și nu există posibilitatea de a obține consimțământul acestora sau nu pot fi extrase, prin editare, datele cu caracter personal nerelevante.

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

6.1. Măsurile generale de administrare a securității informaționale

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

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

- 6.1.3.** Operatorul asigură securitatea punctelor de primire și expediere a corespondenței, precum și securitatea contra accesului neautorizat la aparatele de copiere.
- 6.1.4.** Accesul fizic la mijloacele de reprezentare a informației preluate din sistemul de evidență contabilă este blocat împotriva vizualizării de către persoane neautorizate.
- 6.1.5.** Mijloacele de prelucrare a informațiilor preluate din sistemul de evidență contabilă sau softurile destinate prelucrării acestora sânt scoase din perimetrul de securitate doar în baza permisiunii scrise a operatorului.
- 6.1.6.** Scoaterea și introducerea mijloacelor de prelucrare a informațiilor din sistemul de evidență contabilă din/în perimetrul de securitate se înregistrează în registru.
- 6.2.** Măsurile de protecție a datelor cu caracter personal, prelucrate în sistemul de evidență contabilă, se înfăptuiesc ținând cont de necesitatea asigurării confidențialității și integrității acestora, prin protecție în formă manuală, electronică.
- 6.3.** Cerințe speciale față de marcare: toate informațiile ieșite din sistemul de evidență contabilă, care conțin date cu caracter personal, sânt supuse marcării, cu indicarea prescripțiilor pentru prelucrarea ulterioară și răspândirea acestora, inclusiv cu indicarea numărului de identificare unic al operatorului de date cu caracter personal.
- 6.4.** Accesul în biroul unde este amplasat sistemul de evidență contabilă este restricționat, fiind permis doar persoanelor care au autorizația necesară și doar în timpul orelor de program. Accesul în birou este posibil doar cu autorizarea de acces și cheia de la lacătul mecanic.
- 6.5.** Biroul nu este lăsat niciodată fără supraveghere la ieșirea în exterior, ușa biroului se încuie cu lacătul.
- 6.6.** Înainte de acordarea accesului fizic la sistemul de evidență contabilă, se verifică competențele de acces.
- 6.7.** Registrele de monitorizare se păstrează minimum un an, la expirarea termenului indicat, acestea se lichidează, iar datele și documentele ce se conțin în registrul supus lichidării se transmit în arhivă.
- 6.8.** Perimetrul de securitate se consideră perimetrul biroului în care este amplasat sistemul de evidență contabilă, fiind integru din punct de vedere fizic.
- 6.9.** Zilnic, se inspectează perimetrul de securitate al clădirii și al biroului, unde este amplasat sistemul de evidență contabilă, din punct de vedere fizic.
- 6.10.** Computerele sânt amplasate în locuri cu acces limitat pentru persoane străine.
- 6.11.** Ușile și ferestrele sânt încuiate în cazul în care în încăpere lipsesc angajații autorizați de administrarea sistemului.
- 6.12.** Amplasarea sistemului de evidență contabilă răspunde necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.
- 6.13.** Securitatea electroenergetică: este asigurată securitatea echipamentului electric utilizat pentru menținerea funcționalității sistemului de evidență contabilă, a cablurilor electrice, inclusiv protecția acestora contra deteriorărilor și conectărilor nesancționate. În cazul apariției situațiilor excepționale, de avarie sau de forță majoră, este asigurată posibilitatea deconectării electricității la sistemele de evidență contabilă, inclusiv posibilitatea deconectării oricărui component TI.

6.14. Computerele, unde este amplasat fizic sistemul de evidență contabilă, dispun de UPS-uri, care sânt folosite pentru încheierea corectă a sesiunii de lucru a sistemelor (componentelor) în cazul deconectării de la sursa de alimentare cu energie electrică.

6.15. Securitatea cablurilor de rețea: cablurile de rețea, prin care se efectuează operațiunile de transmitere a datelor preluate din sistemul de evidență contabilă, sânt protejate contra conectărilor nesancționate sau deteriorărilor. Pentru a exclude bruiatul, cablurile de tensiune sânt separate de cele comunicaționale.

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

6.17. Controlul instalării și scoaterii componentelor TI: se efectuează controlul și evidența instalării și scoaterii mijloacelor de program, mijloacelor tehnice și celor tehnice de program, utilizate în cadrul sistemului de evidență contabilă. La expirarea termenului de păstrare, informațiile, care conțin date cu caracter personal și care se conțin pe purtătorii de informații, se distrug.

VII. IDENTIFICAREA ȘI AUTENTIFICAREA UTILIZATORULUI SISTEMULUI DE EVIDENȚĂ CONTABILĂ

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

7.2. Toți utilizatorii (inclusiv personalul care asigură mentenanța tehnică, administratorii de rețea, programatorii și administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu trebuie să conțină semnalmentele nivelului de accesibilitate al utilizatorului.

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

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

7.5. Întru asigurarea posibilității de stabilire a responsabilității fiecărui utilizator, sânt folosite identificatori și parole individuale ale acestora. Este asigurată posibilitatea utilizatorilor de a alege și schimba parolele individuale, inclusiv de activare a procedurii de evidență a introducerilor greșite ale acestora. După trei tentative greșite de autentificare, accesul este blocat, în mod automatizat.

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

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

7.8. Se efectuează, prin mijloace automatizate de suport, administrarea conturilor de acces a utilizatorilor care prelucrează datele cu caracter personal în sistemul de evidență contabilă, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea și ștergerea acestora. Acțiunea conturilor de acces a utilizatorilor temporari, care prelucrează date cu caracter personal înregistrate în sistemul de evidență contabilă, încetează automat la expirarea perioadei stabilite în timp (pentru fiecare tip de cont de acces în parte). Se dezactivează automat, după o perioadă de maxim 1 /una/ lună, conturile de acces ale utilizatorilor neactivi, care prelucrează informațiile din sistemul de evidență contabilă. Se folosesc mijloace automatizate de înregistrare și informare despre crearea, modificarea, dezactivarea și încetarea acțiunii conturilor de acces.

7.9. În scopul depistării și evitării cazurilor de acordare a drepturilor de acces neautorizat, se revizuieste cu regularitate, maximum la fiecare șase luni și după oricare schimbare a statutului utilizatorului, drepturile de acces ale utilizatorilor la sistemul de evidență contabilă.

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

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

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

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

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

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

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

VIII. AUDITUL SECURITĂȚII ÎN SISTEMELE DE EVIDENȚĂ CONTABILĂ

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

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

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

8.3. Se efectuează înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative și proceselor, destinate prelucrării informațiilor din sistemele de evidență contabilă, înregistrarea modificărilor drepturilor de acces ale utilizatorilor și statutul obiectelor de acces conform următorilor parametri:

- a) data și timpul tentativei de pornire;
- b) denumirea/identificatorul programului aplicativ sau al procesului;
- c) ID-ul utilizatorului;
- d) rezultatul tentativei de pornire – pozitivă sau negativă.

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

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

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

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

8.6. Se efectuează înregistrarea ieșirii din sistemul de evidență contabilă, înregistrarea modificărilor drepturilor de acces ale subiecților și statutul obiectelor de acces, conform următorilor parametri:

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

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

8.8. Rezultatele auditului securității în sistemul de evidență contabilă (operațiunile de prelucrare a informațiilor și mijloacele de efectuare a auditului), se protejează contra accesului neautorizat prin aplicarea măsurilor de securitate adecvate și asigurarea confidențialității și integrității acestora.

8.9. Durata minimă a stocării rezultatelor auditului securității în sistemul de evidență contabilă constituie 2 /doi/ ani, în scopul asigurării posibilității de folosire a acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigații sau procese judiciare. În cazul în care investigațiile sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

IX. ASIGURAREA INTEGRITĂȚII INFORMAȚIILOR DIN SISTEMUL DE EVIDENȚĂ CONTABILĂ

9.1. Se asigură identificarea, protocolarea și înlăturarea deficiențelor de soft-uri destinate prelucrării informațiilor din sistemul de evidență contabilă, inclusiv instalarea corectărilor și pachetelor de reînnoire a acestora, protecția contra infiltrării programelor dăunătoare în soft-uri, măsuri care asigură posibilitatea reînnoirii automate și la timp a mijloacelor de asigurare a protecției contra programelor dăunătoare și signaturilor de virus.

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

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

9.4. Copiile de siguranță: reieșind din volumul prelucrărilor efectuate, individual, se stabilește de către operator intervalul de timp în care se execută copiile de siguranță a informațiilor din sistemul de evidență contabilă și soft-urilor folosite pentru prelucrările automatizate a acestora. Copiile de siguranță se testează în scopul verificării siguranței purtătorilor de informații și integrității informației indicate. Procedurile de restabilire a copiilor de siguranță se actualizează și se testează cu regularitate, în scopul asigurării eficacității acestora.

X. GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMULUI DE EVIDENȚĂ CONTABILĂ

10.1. Persoanele care asigură exploatarea sistemului de evidență contabilă trec, minimum o dată în an, instruirea cu privire la responsabilitățile și obligațiile în cazul executării acțiunilor de gestionare și reacționare la incidentele de securitate.

10.2. Prelucrarea incidentelor de securitate include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor și restabilirea securității. Se monitorizează și documentează, în mod permanent, incidentele de securitate în sistemul de evidență contabilă.

10.3. „În cazul producerii incidentelor de securitate persoanele responsabile va întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia

și va înlătura cauzele incidentului de securitate cu informarea în termen de 72 ore din momentul producerii incidentului de securitate a Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova. Totodată, în cadrul controalelor efectuate de Centrul Național pentru Protecția Datelor cu Caracter Personal, persoanele responsabile sînt obligate să ofere suportul necesar și să asigure accesul la informațiile necesare relevante obiectului controlului.”

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

XI. DISPOZIȚII FINALE

11.1. Prezentul Regulament este revizuit de **PRIMĂRIA ORAȘULUI CIMIȘLIA** și ulterior aprobat de către **CONSILIUL ORĂȘENESC CIMIȘLIA**, periodic, însă cel puțin o dată în an, precum și la necesitate.

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

11.3. Regulamentul este adus la cunoștința angajaților contra semnăturii.

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

Anexa nr. 1

**la Regulamentul privind prelucrarea informațiilor
ce conțin date cu caracter personal în sistemul
de evidență contabilă a PRIMĂRIEI ORAȘULUI CIMIȘLIA**

DECLARAȚIE

despre familiarizarea cu prevederile Regulamentului privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență contabilă a **PRIMĂRIEI ORAȘULUI CIMIȘLIA** și asumarea obligației de a păstra confidențialitatea informației

Prin prezenta, _____ (IDNP – _____) -

(numele/ prenumele, postul angajatului)

Declar că am luat act de prevederile cu privire la asigurarea securității datelor cu caracter personal în sistemul de evidență contabilă în cadrul **PRIMĂRIEI ORAȘULUI CIMIȘLIA** și în calitate de utilizator cu drept de acces la sistemul de evidență contabilă, îmi asum obligația să nu divulg date sau informații ce constituie date cu caracter personal de care am luat cunoștință în perioada executării obligațiilor de funcție.

Am fost avertizat de răspunderea disciplinară, materială, administrativă și penală prevăzută de legislația în vigoare pentru încălcarea acestor prevederi.

" ____ " _____ **2022**

Semnătura _____

Anexa nr. 2
la Regulamentul privind prelucrarea informațiilor
ce conțin date cu caracter personal în sistemul
de evidență contabilă a PRIMĂRIEI ORAȘULUI CIMIȘLIA

**LISTA ANGAJAȚILOR FAMILIARIZAȚI CU PREVEDERILE
REGULAMENTULUI
PRIVIND PRELUCRAREA INFORMAȚIILOR CE CONȚIN DATE
CU CARACTER PERSONAL ÎN SISTEMUL DE EVIDENȚĂ CONTABILĂ
A PRIMĂRIEI ORAȘULUI CIMIȘLIA**

Nr.	Numele, prenumele	Funcția	Am luat cunoștință (semnătura)	Data
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				

Secretarul Consiliului



Cristina PÎNZARI