APROBAT:
Şef interimar al Direcţiei generale sistenţă socială şi sănătate şi sănătate a Consiliului municipal Chişinău
Irina Banova _____
"19" aprilie 2018

L.Ş.

Redactată în baza ordinului
Şefului interimar al Direcţiei
nr.84-b din data 19.04.2018

REGULAMENTUL PRIVIND PRELUCRAREA INFORMAŢIILOR CE CONŢIN DATE CU CARACTER PERSONAL ÎN SECRETARIAT DIN CADRUL DIRECŢIEI GENERALE SISTENŢĂ SOCIALĂ ŞI SĂNĂTATE ŞI SĂNĂTATE A CONSILIULUI MUNICIPAL CHIŞINĂU

I. Dispoziţii generale

Regulamentul Registrului de evidenţă a corespondenţei al Direcţiei generale sistenţă socială şi sănătate a Consiliului municipal Chişinău (în continuare Regulament) este elaborat în conformitate cu prevederile Legii nr. 190-XIII din 19 iulie 1994 cu privire la petiţionare, Legii nr. 71-XVI din 22 martie 2007 cu privire la registre, Legii nr.133 din 8 iulie 2011 privind protecţia datelor cu caracter personal, Instrucţiunilor privind ţinerea lucrărilor de secretariat referitoare la petiţiile persoanelor fizice şi juridice, adresate organelor de stat, întreprinderilor, instituţiilor şi organizaţiilor Republicii Moldova, aprobate prin Hotărîrea Guvernului nr. 208 din 31 martie 1995, Regulilor de întocmire a documentelor organizatorice şi de dispoziţie şi Instrucţiunii-tip cu privire la ţinerea lucrărilor de secretariat în organele administraţiei publice centrale de specialitate şi ale autoadministrării locale ale Republicii Moldova, aprobate prin Hotărîrea Guvernului nr. 618 din 05 octombrie 1993, Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, aprobate prin Hotărîrea Guvernului nr. 1123 din 14 decembrie 2010.

Prezentul Regulament reglementează modalitatea ţinerii Registrului de evidenţă a corespondenţeial Direcţiei generale sistenţă socială şi sănătate a Consiliului municipal Chişinău, precum şi procedura de înregistrare, securizare, modificare şi radiere a datelor din acest Registru.

Noţiunile utilizate în prezentul Regulament au semnificaţia prevăzută de Legea cu privire la registre, Legea cu privire la petiţionare, Legea privind protecţia datelor cu caracter personal, Regulamentul Registrului de evidenţă a operatorilor de date cu caracter personal, aprobat prin Hotărîrea Guvernului nr. 296 din 15 mai 2012, Cerinţele faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, aprobate prin Hotărîrea Guvernului nr. 1123 din 14 decembrie 2010.

Astfel, în sensul prezentului Regulament se definesc următoarele noţiuni:

adresare - orice cerere, reclamaţie, propunere, sesizare, adresată organelor de resort, inclusiv cererea prealabilă prin care se contestă un act administrativ sau nesoluţionarea în termenul stabilit de lege a unei cereri;

Registrul de evidenţă a corespondenţei – resursa informaţională specializată (totalitatea informaţiilor ţinute în formă automatizată şi manuală) care asigură evidenţa informaţiei sistematizate, principalul obiectiv al căruia constă în asigurarea evidenţei corespondenţei parvenite la Direcţia generală

asistență socială a Consiliului municipal Chișinău;

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;

sistem de evidenţă 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 funcţionale sau geografice. În calitate de sistem de evidenţă a datelor cu caracter personal se constituie inclusiv dar nu se limitează la, bazele de date, sistemele informaționale şi informatice în care sînt stocate şi prelucrate automatizat sau manual date cu caracter personal;

registrator – angajatul al Direcției generale sistență socială și sănătate a Consiliului municipal Chișinău împuternicit cu atribuţiile de introducere, modificare, păstrare a informaţiei din Registru.

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

Subiecţi ai raporturilor juridice apărute ca rezultat al instituirii, administrării şi ţinerii a Registrului sînt:

- Direcției generale sistență socială și sănătate a Consiliului municipal Chișinău, în calitate de proprietar și deținător al Registrului;
- Persoanele împuternicite de ținerea Registrului și cele responsabile de efectuarea controlului intern al acestuia;
- Persoanele fizice, ale căror date cu caracter personal vor fi stocate în Registru;
- Persoanele interesate de a accesa și vizualiza datele din Registru.

Angajaţii Direcției generale sistență socială și sănătate a Consiliului municipal Chișinău poartă răspundere personală pentru îndeplinirea cerinţelor prezentului Regulament, asigurarea confidenţialităţii, securităţii şi păstrarea în stare corespunzătoare a informaţiei din Registru.

II. Condiţii generale faţă de ţinerea Registrului

2.1 Registrul de evidență a corespondenței reprezintă un sistem de evidență a informației în formă manuală și în formă electronică, inclusiv a celei care conține datele cu caracter personal.

2.2 De către Direcției generale sistență socială și sănătate a Consiliului municipal Chișinău (Secretariat) va fi asigurată ținerea în formă manuală a unor Registre (ținînd 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.

2.3 Persoanele responsabile din cadrul Secretariat vor asigura evidența în formă electronică a adresărilor parvenite la Direcției generale sistență socială și sănătate a Consiliului municipal Chișinău .

2.4 Obiectul înregistrării reprezintă informația referitor la persoanele care au înaintat adresări Direcției generale sistență socială și sănătate a Consiliului municipal Chișinău.

2.5 Registrul va fi ţinut în limba de stat.

2.6 Registratorul este obligat:

- să introducă în Registru numai informaţia 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, încît să excludă posibilitatea de a fi radiată (ștearsă, distrusă) în mod mecanic, chimic sau în orice alt mod, fără a lăsa urme vizibile ale radierii (ștergerii, distrugerii);
- să asigure accesul la informaţia 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.

2.7 Datele din registru vor reflecta starea veridică şi actuală a informației privind persoanele vizate în

corespondența cu Direcției generale sistență socială și sănătate a Consiliului municipal Chișinău.

2.8 Atît forma manulă, cît și cea electronică a Registrului va cuprinde în mod obligatoriu:

- denumirea Registrului;
- denumirea Direcției generale sistență socială și sănătate a Consiliului municipal Chișinău 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.

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

III. Condiţii generale privind introducerea informaţiei în Registru

3.1 Informaţia privind corespondenţa parvenită în adresa Direcţiei generale sistenţă socială şi sănătate a Consiliului municipal Chişinău va fi recepţionată şi înregistrată în aceiaşi zi de persoana responsabilă din cadrul Secretariat în Registrul de evidenţă a corespondenţei, iar versiunea electronică parvenită se înregistrează în arhiva electronică a Direcţiei generale sistenţă socială şi sănătate a Consiliului municipal Chişinău cu perfectarea fişele de evidenţă şi control a acestora.

3.2 Înregistrarea informaţiei în Registru se face prin introducerea menţiunilor necesare în cartea de înregistrări (forma manuală) şi în sistemul informatic „Petiţii" (forma electronică) în baza datelor furnizate prin documentele transmise de furnizorii datelor registrului, atît pe suport de hîrtie cît în formă electronică, perfectate în modul stabilit de lege.

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

3.4 După caz, se va întocmi manual fişa de evidenţă şi control pentru adresările înaintate (în condiţiile stabilite prin Instrucţiunile privind ţinerea lucrărilor de secretariat referitoare la petiţiile persoanelor fizice şi juridice, adresate organelor de stat, întreprinderilor, instituţiilor şi organizaţiilor Republicii Moldova, aprobate prin Hotărîrea Guvernului nr. 208 din 31 martie 1995), introducîndu-se datele cu caracter personal ce vizează petiţionarul (nume, prenume, adresa de domiciliu, numărul de telefon) precum şi rezoluţia conducerii Direcţiei generale sistenţă socială şi sănătate a Consiliului municipal Chişinău, termenul de soluţionare stabilit de conducerea Direcţiei generale sistenţă socială şi sănătate a Consiliului municipal Chişinău, datele despre starea executării etc.

3.5 După examinarea şi soluţionarea definitivă, pe fişa de evidenţă şi control în Sistemul informatic „Petiţii" se face menţiunea despre finalizarea examinării adresării şi modificarea statutului acesteia în document arhivat iar în forma manuală a Registrului se indică în menţiuni .

3.6 Modificările şi radierile făcute în Registru se efectuează în baza deciziei şi cu semnătura registratorului în situaţia existenţei unui motiv întemeiat în acest sens.

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

3.8 Greşelile de ordin tehnic comise de către persoana împuternicită de ţinerea Registrului se rectifică de către aceasta. Corectarea greşelii se specifică într-o rubrică aparte, urmată de semnătura persoanei care a efectuat înscrierea.

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

3.10 Rectificările şi radierile înscrisurilor din Registru se efectuează astfel încît textul iniţial să fie citabil.

IV. Condiţii generale privind păstrarea şi furnizarea informaţiei din Registru

4.1 Păstrarea/stocare informaţiei în registru este asigurată de registrator pînă la adoptarea deciziei conducerii Direcţiei generale sistenţă socială şi sănătate a Consiliului municipal Chişinău despre lichidarea registrului, dar nu mai mult decît pe perioada stabilită de Indicatorul documentelor-tip şi al termenelor lor de păstrare pentru organele administraţiei publice, pentru instituţiile, organizaţiile şi întreprinderile Republicii Moldova, aprobat de Serviciul de Stat de Arhivă nr.57 din 27.07.2016.

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

4.3 În acest sens, persoana împuternicită de ţinerea şi păstrarea Registrului este obligată:

- să prevină accesul nesancţionat la datele stocate în Registru;
- să întreprindă acţiuni în vederea neadmiterii cazurilor de utilizare ilegală, dezvăluire ilegală a informaţiei conţinute în acesta, de modificare sau nimicire a acestor date.

4.4 Persoanele împuternicite de ţinerea şi controlul registrului sînt obligate să nu divulge informaţia la care au primit acces în legătură cu exercitarea atribuţiilor funcţionale, inclusiv după încetarea activităţii în cadrul Direcţiei generale sistenţă socială şi sănătate a Consiliului municipal Chişinău .

4.5 Registratorul este obligat să asigure accesul la informaţia din registru pentru angajaţii autorizaţi ai Direcţiei generale sistenţă socială şi sănătate a Consiliului municipal Chişinău şi alte persoane, care au dreptul de a primi informaţia respectivă, în conformitate cu legislaţia în vigoare sau care demonstrează dreptul şi interesul legitim de a primi aceste informaţii, din momentul în care acestea vor fi disponibile, dar nu mai tîrziu de 15 zile de la data depunerii cererii.

4.6 Informaţia poate fi furnizată gratuit sau contra plată în conformitate cu Legea privind accesul la informaţie.

4.7 Extrasul din Registru trebuie să fie semnat de conducerea Direcţiei generale sistenţă socială şi sănătate a Consiliului municipal Chişinău , cu indicarea datei întocmirii/eliberării acestuia.

V. Condiţiile suplimentare privind gestionarea Registrului în formă manuală

5.1 Ţinerea manuală a Registrului de evidenţă a corespondenţei se efectuează sub formă de fişier sau prin introducerea menţiunilor în cartea pentru înregistrări.

5.2 În acest sens, evidenţa corespondenţei în cadrul Direcţiei generale sistenţă socială şi sănătate a Consiliului municipal Chişinău este dusă prin intermediul mai multor Registre ţinute în formă manuală, cum ar fi:

- „Registrul cererilor parvenite de la angajaţii Direcţiei generale sistenţă socială şi sănătate a Consiliului municipal Chişinău, gestionate de persoana desemnată din cadrul Secretariat;
- „Registrul de intrare/ieşire a corespondenţei aoficiale", gestionat de persoana desemnată din cadrul Secretariat; etc

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

- să efectueze înscrierile citeţ şi clar. Prescurtările vor fi făcute astfel pentru a fi evitate diferite interpretări. Textul greşit se taie cu o linie, fiind posibilă citirea textului greşit înscris.
- să nu înlocuiască neîntemeiat filele din cartea registrului prin extragerea lor, încleierea unor noi file etc;
- să asigure, în cazul deteriorării cărţii, posibilitatea restabilirii imediate a datelor din registru fără a cauza daune informaţiei, ce se conţine în ea;
- să asigure şnuruirea cărţilor pentru înregistrări (în caz că nu este o carte integrală) şi numerotarea filelor. Numărul de file se indică pe ultima pagină şi se autentifică (inclusiv conţinutul cărţii) prin aplicarea semnelor de control de către conducerea Direcţiei generale sistenţă socială şi sănătate a Consiliului municipal Chişinău: semnătura şi ştampila.

5.4 Informaţia va fi introdusă în Registru în ordine cronologică, ţinîndu-se cont de necesitatea prezenţei menţiunilor privind:

- numărul şi data de intrare;
- denumirea instituţiei;

- numărul de ieşire a instituţiei emitente;
- conţinutul succint al documentului;
- numele şi prenumele executantului, termenul de executare;
- rezultatul examinării: admisă/respinsă/oferite explicaţii de rigoare/acte de reacţionare adoptate de conducerea Direcţiei generale sistenţă socială şi sănătate a Consiliului municipal Chişinău.

5.5 Registrul se păstrează de persoana responsabilă într-un loc cu accesebilitate limitată şi va conţine un compartiment separat în care se vor consemna înregistrările de audit a securităţii, prevăzute de pct. 11.2 al Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal.

VI. Condiţii suplimentare privind gestionarea Registrului în formă electronică

6.1 Ţinerea în formă electronică a Registrului de evidenţă a corespondenţei este realizat de Direcţiei generale sistenţă socială şi sănătate a Consiliului municipal Chişinău prin intermediul unui sistem informaţional automatizat special constituit - Sistemul informatic „Petiţii".

6.2 Introducerea, modificarea şi păstrarea informaţiei în acest Registru este asigurată de registratorul desemnat din cadrul Secretariat.

6.3 La înscrierea informaţiei privind cadresăriel parvenite în Registru se inserează şi o listă de date despre obiect, inclusiv date cu privire la faptul înregistrării în compartimentele special destinate, şi anume:

- tipul adresării;
- data şi numărul de intrare;
- numele, prenumele adresantului;
- adresa de domiciliu, e-mail (în cazul existenţei);
- problema abordată;
- rezoluţia conducerii Direcţiei generale sistenţă socială şi sănătate a Consiliului municipal Chişinău;

6.4 Suplimentar la Registru se completeazr fişa de onsoţire, care include:

- executorii;
- termenul de rezolvare şi data expirării;
- date privind executarea;
- date privind posibila prelungire (termenul, numărul documentul prin care s-a efectuat prelungirea, informarea adresantului);
- rezultatul examinării: admisă/respinsă/oferite explicaţii de rigoare/acte de reacţionare adoptate de Direcţiei generale sistenţă socială şi sănătate a Consiliului municipal Chişinău.

VII. Măsurile de protecţie a datelor cu caracter personal prelucrate în registrul de evidenţă a corespondenţei

7.1 În cazul neutilizării temporare a purtătorilor de informaţie pe suport de hîrtie sau electronic care conţin date preluate din registrul de evidenţă a corespondenţei, aceştia se păstrează în safeuri care se încuie.

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

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

7.4 Accesul fizic la mijloacele de reprezentare a informaţiei preluate din registrul de evidenţă a corespondenţei este blocat împotriva vizualizării de către persoane neautorizate.

7.5 Mijloacele de prelucrare a informaţiilor preluate din registrul de evidenţă a corespondenţei sau soft-urile destinate prelucrării acestora sînt scoase din perimetrul de securitate doar în baza permisiunii scrise a operatorului.

7.6 Scoaterea şi introducerea mijloacelor de prelucrare a informaţiilor din registrul de evidenţă a corespondenţei din/în perimetrul de securitate se înregistrează întru-n registru specializat.

7.7 Măsurile de protecţie a datelor cu caracter personal, prelucrate în registrul de evidenţă a corespondenţei, se înfăptuiesc ţinînd cont de necesitatea asigurării confidenţialităţii şi integrităţii acestora, prin protecţie în formă manuală, electronică şi externă.

7.8 Cerinţe speciale faţă de marcare: toate informaţiile ieşite din registrul de evidenţă a corespondenţei, care conţin date cu caracter personal, sînt supuse marcării, cu indicarea prescripţiilor pentru prelucrarea ulterioară şi răspîndirea acestora, inclusiv cu indicarea numărului de identificare unic al operatorului de date cu caracter personal.

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

7.10 Înainte de acordarea accesului fizic la registrul de evidenţă a corespondenţei, se verifică competenţele de acces.

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

7.12 Perimetrul de securitate se consideră perimetrul biroului în care este amplasat registrul de evidenţă a corespondenţei, fiind integru din punct de vedere fizic.

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

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

7.15 Uşile şi ferestrele sînt încuiate în cazul în care în încăpere lipsesc angajaţii autorizaţi de administrarea sistemului.

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

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

7.18 Computerele, unde este amplasat fizic registrul de evidenţă a corespondenţei, 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.

7.19 Securitatea cablurilor de reţea: cablurile de reţea, prin care se efectuează operaţiunile de transmitere a datelor preluate din registrul de evidenţă a corespondenţei, sînt protejate contra conectărilor nesancţionate sau deteriorărilor. Pentru a exclude bruiajul, cablurile de tensiune sînt separate de cele comunicaţionale.

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

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

VIII Identificarea şi autentificarea utilizatorului registrul de evidenţă a corespondenţei

8.1 Este efectuată identificarea şi autentificarea utilizatorilor informaţiilor preluate din registrul de evidenţă a corespondenţei şi a proceselor executate în numele acestor utilizatori.

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

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

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

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

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

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

8.8 Se efectuează, prin mijloace automatizate de suport, administrarea conturilor de acces a utilizatorilor care prelucrează datele cu caracter personal în registrul de evidenţă a corespondenţei, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea şi ştergerea acestora. Acţiunea conturilor de acces a utilizatorilor temporari, care prelucrează date cu caracter personal înregistrate în registrul de evidenţă a corespondenţei, 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 informaţiile din registrul de evidenţă a corespondenţei. Se folosesc mijloace automatizate de înregistrare şi informare despre crearea, modificarea, dezactivarea şi încetarea acţiunii conturilor de acces.

8.9 În scopul depistării şi evitării cazurilor de acordare a drepturilor de acces neautorizat, se revizuieşte cu regularitate, maximum la fiecare şase luni şi după oricare schimbare a statutului utilizatorului, drepturile de acces ale utilizatorilor la registrul de evidenţă a corespondenţei.

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

8.11 Se impun limite în privinţa persoanelor care au dreptul:

a) să vizualizeze informaţiile stocate în registrul de evidenţă a corespondenţei;

b) să copieze, să descarce, să şteargă sau să modifice orice informaţie stocată.

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

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

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

8.15 Înainte de acordarea accesului în sistemul informatic, utilizatorii sînt informaţi despre faptul că folosirea registrului de evidenţă a corespondenţeieste controlată şi că folosirea neautorizată a acestora este sancţionată în conformitate cu legislaţia civilă, contravenţională şi penală.

IX. Auditul securităţii în sistemele de evidenţă a documentelor

9.1 Se organizează generarea înregistrărilor de audit a securităţii în registrul de evidenţă a corespondenţeipentru evenimentele, indicate în lista corespunzătoare, supuse auditului.

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

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

9.3 Se efectuează înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative şi proceselor, destinate prelucrării informaţiilor din registrul de evidenţă a corespondenţei, înregistrarea modificărilor drepturilor de acces ale utilizatorilor şi statutul obiectelor de acces conform următorilor parametri:

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

9.4 Se efectuează înregistrarea tentativelor de obţinere a accesului (de executare a operaţiunilor) pentru aplicaţii şi procese destinate prelucrării informaţiilor din registrul de evidenţă a corespondenţei, conform următorilor parametri:

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

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

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

9.6 Se efectuează înregistrarea ieşirii din registrul de evidenţă a corespondenţei, înregistrarea modificărilor drepturilor de acces ale subiecţilor şi statutul obiectelor de acces, conform următorilor parametri:

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

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

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

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

X. Asigurarea integrităţii informaţiilor din Registrul de evidenţă a corespondenţei, ţinutîn forma electronică

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

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

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

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

XI. Gestionarea incidentelor de securitate a registrul de evidenţă a corespondenţei

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

11.2 Prelucrarea incidentelor de securitate include depistarea, analiza, preîntîmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii. Se monitorizează şi documentează, în mod permanent, incidentele de securitate în registrul de evidenţă a corespondenţei.

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

11.4 Anual, către 31 ianuarie, Direcţiei generale sistenţă socială şi sănătate a Consiliului municipal Chişinău prezintă Centrului raportul generalizat despre incidentele de securitate a sistemelor de evidenţă a datelor cu caracter personal.

11.5 Persoanele care se fac vinovate de încălcarea normelor privind obţinerea, păstrarea, prelucrarea şi protecţia informaţiilor din registrul de evidenţă a corespondenţei poartă răspundere civilă, contravenţională şi penală.

XII. Dispoziţii finale

12.1 Prezentul Regulament este revizuit şi ulterior aprobat de către conducerea Direcţiei generale sistenţă socială şi sănătate a Consiliului municipal Chişinău periodic, însă cel puţin o dată în an, precum şi la necesitate.

12.2 Prezentul Regulament se completează cu prevederile legislaţiei în vigoare.

12.3 Regulamentul este adus la cunoştinţa angajaţilor contra semnăturii.

12.4 Modificarea şi completarea prezentului Regulament se face în modul stabilit pentru aprobarea lui.