



DISPOZIȚIE

nr. 1115-d

din 13 decembrie 2014

Cu privire la aprobarea și organizarea
implementării Politicii de securitate
a prelucrării datelor cu caracter personal
în cadrul subdiviziunilor administrației publice
ale municipiului Chișinău

În scopul asigurării protecției drepturilor și libertăților fundamentale ale persoanei fizice în ceea ce privește prelucrarea datelor cu caracter personal, în conformitate cu prevederile art. 30 din Legea nr. 133 din 08.07.2011 „Privind protecția datelor cu caracter personal”, pct. 15 și pct. 16 din Hotărârea Guvernului nr. 1123 din 14.12.2010 „Privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal”, în temeiul art. 15 alin. (2) din Legea nr. 136 din 17.06.2016 „Privind statutul municipiului Chișinău”, art. 29 alin. (2), art. 32 alin. (1) și art. 34 alin. (1) din Legea nr. 436-XVI din 28.12.2006 „Privind administrația publică locală”, mandatului judecătoresc nr. 1-1320/17 din 28.07.2017 emis de Judecătoria Chișinău, sediul Buiucani, dispoziției nr. 697-dc din 06.11.2017 „Cu privire la desemnarea doamnei Silvia Radu pentru exercitarea funcției de Primar general interimar al municipiului Chișinău”, Primarul general interimar al municipiului Chișinău DISPUNE:

1. Se aprobă Politica de securitate a prelucrării datelor cu caracter personal în cadrul subdiviziunilor administrației publice ale municipiului Chișinău (anexă).
2. Conducătorii preturilor de sector, subdiviziunilor administrației publice municipale (direcții generale, direcții) vor asigura:
 - 2.1 Aprobarea Politicii de securitate a prelucrării datelor cu caracter personal la nivelul autorității publice pe care o conduc;
 - 2.2 Elaborarea și aprobarea, până la data de 20.01.2018, a Regulamentelor privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemele de evidență gestionate în procesul de activitate;
 - 2.3 Notificarea, până la data de 15.02.2018, a Centrului Național pentru Protecția Datelor cu Caracter Personal privind categoriile de date cu caracter personal prelucrate de autoritatea publică pe care o conduc;

- 2.4 Măsuri tehnice și organizaționale necesare desfășurării procesului de management al securității datelor cu caracter personal prin implementarea prevederilor Politicii de securitate a datelor cu caracter personal;
 - 2.5 Desemnarea persoanei responsabile de implementarea și monitorizarea respectării prevederilor Politicii de securitate a datelor cu caracter personal;
 - 2.6 Întocmirea și aprobarea listei nominale a utilizatorilor, autorizați să acceseze datele cu caracter personal;
 - 2.7 Întocmirea și prezentarea trimestrială a rapoartelor despre incidentele de securitate aferente domeniului de management al datelor cu caracter personal.
3. Se numește, dl Adrian Talmaci, secretar interimar la Consiliului municipal Chișinău, responsabil de:
- 3.1 Coordonarea procesului de elaborare a Regulamentelor privind prelucrarea informațiilor ce conțin date cu caracter personal în sisteme de evidență gestionate de Primăria municipiului Chișinău și înaintarea acestora spre aprobarea primarului general până la data de 20.01.2018;
 - 3.2 Notificarea, până la data de 15.02.2018, a Centrului Național pentru Protecția Datelor cu Caracter Personal privind categoriile de date cu caracter personal prelucrate de Primăria municipiului Chișinău;
 - 3.3 Monitorizarea implementării prevederilor Politicii de securitate a datelor cu caracter personal în cadrul Primăriei municipiului Chișinău;
4. Secția control a Primăriei municipiului Chișinău, va asigura controlul respectării termenelor indicate în prezenta dispoziție, colectarea și prezentarea primarului general, până la data de 28.02.2018, a informației privind acțiunile întreprinse de către responsabilii desemnați.
5. Prezenta dispoziție intră în vigoare la data semnării și se aduce la cunoștința tuturor părților interesate.
6. Controlul executării prevederilor prezentei dispoziții mi-l asum.

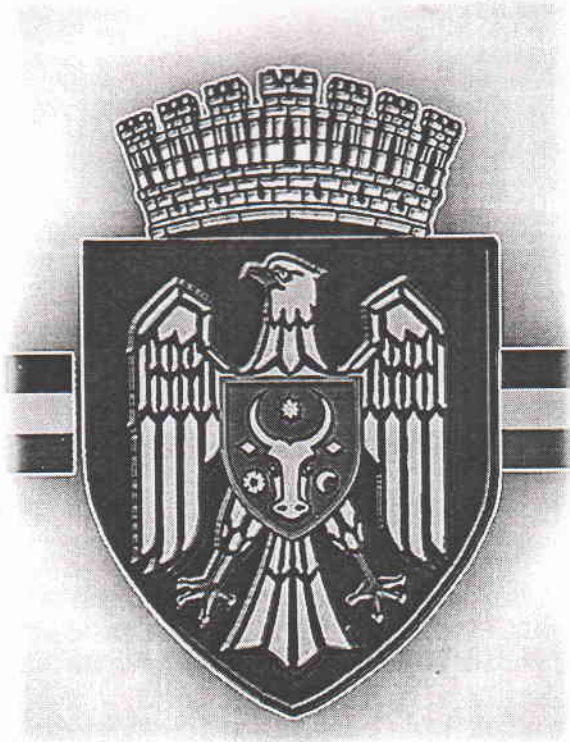
PRIMAR GENERAL INTERIMAR



Silvia RADU

Anexă
la dispoziția primarului general interimar
nr. 1115-d din 13.12.2017

Primăria municipiului Chișinău



POLITICA

**DE SECURITATE A PRELUCRĂRII DATELOR
CU CARACTER PERSONAL
ÎN CADRUL SUBDIVIZIUNILOR ADMINISTRAȚIEI PUBLICE
ALE MUNICIPIULUI CHIȘINĂU**

I. DISPOZIȚII GENERALE

1.1. Politica de securitate a prelucrării datelor cu caracter personal în cadrul subdiviziunilor administrației publice municipale (în continuare – Politica) stabilește principiile și cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale automatizate și mecanice de date cu caracter personal.

1.2. Politica are drept scop stabilirea regulilor de implementare de către subdiviziunile administrației publice municipale a măsurilor tehnice și organizatorice necesare pentru asigurarea securității, confidențialității și integrității datelor cu caracter personal prelucrate în cadrul sistemelor informaționale automatizate și mecanice de date cu caracter personal și/ sau registrelor ținute manual.

1.3. Politica este elaborată în conformitate cu prevederile Legii nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal și Legii nr. 71-XVI din 22.03.2007 cu privire la registre, Hotărârii Guvernului nr. 1123 din 14.12.2010 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 Convenției pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal (Strasbourg, 28 ianuarie 1981).

1.4. În sensul prezentei Politici, se definesc următoarele noțiuni:

autorități publice municipale (APM) – subdiviziuni ale Consiliului municipal Chișinău (direcții generale, direcții, alte unități structurale), preturi de sector, subdiviziuni ale Primăriei municipiului Chișinău (direcții, secții, servicii);

autenticare - verificarea identicatorului atribuit subiectului de acces, confirmarea autenticității;

categorii speciale de date cu caracter personal – datele care dezvăluie originea rasială sau etnică a persoanei, convingerile ei politice, religioase sau filozofice, apartenența socială, datele privind starea de sănătate sau viața sexuală, precum și cele referitoare la condamnările penale, măsurile procesuale de constrângere sau sancțiunile contravenționale;

date cu caracter personal (DCP) (categoria obișnuită) – orice informație 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 identității sale fizice, fiziologice, psihice, economice, culturale sau sociale;

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 identicator subiecților și obiectelor de acces și/sau compararea identicatorului prezentat cu lista identificatoarelor atribuite;

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

Politica de securitate a prelucrării datelor cu caracter personal

politica de securitate a datelor cu caracter personal - un set de reguli, cerințe și instrucțiuni aplicabile la nivelul entității, care stă la baza infrastructurii de securitate și stabilește limitele unui comportament acceptabil în utilizarea resurselor informaționale și de comunicații ale entității.

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;

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;

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 hârtie 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 datelor cu caracter personal în starea în care se aflau până la momentul pierderii sau distrugerii acestora;

tehnologie informațională (TI) - 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;

stocare - păstrarea pe orice fel de suport a datelor cu caracter personal.

II. CERINȚE GENERALE

- 2.1. Măsurile de protecție a datelor cu caracter personal reprezintă o parte componentă a lucrărilor de creare, dezvoltare și exploatare a sistemelor informaționale de date cu caracter personal și vor fi efectuate neîntrerupt de către persoanele responsabile angajate în cadrul APM.
- 2.2. Protecția datelor cu caracter personal este asigurată printr-un complex de măsuri tehnice și organizatorice de preîntâmpinare a prelucrării ilicite a datelor cu caracter personal.
- 2.3. Orice prelucrare a datelor cu caracter personal, cu excepția situațiilor menționate în art. 5 alin. (5) din Legea nr. 133 din 08.07.2001 privind protecția datelor cu caracter personal, poate fi efectuată numai dacă persoana vizată și-a dat consimțământul în mod expres și neechivoc pentru acea prelucrare.
- 2.4. APM asigură ca datele personale ale subiecților să fie:
- prelucrate în mod corect și conform prevederilor normative din domeniu;
 - colectate doar în scopuri determinate, explicite și legitime pentru asigurarea prestării serviciilor publice corespunzătoare;
 - stocate într-o formă care să permită identificarea subiecților datelor cu caracter personal pe o perioadă care nu va depăși durata necesară atingerii scopurilor pentru care sunt colectate și ulterior prelucrate.
- 2.5. Măsurile de protecție a datelor cu caracter personal prelucrate în sistemele informaționale și mecanice de date cu caracter personal ale APM se realizează ținându-se cont de necesitatea asigurării confidențialității acestor măsuri.
- 2.6. Sunt supuse protecției toate resursele informaționale ale APM, care conțin date cu caracter personal, inclusiv:
- suporturile 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 de prelucrare a informației.
- 2.7. Protecția datelor cu caracter personal în sistemele informaționale de date cu caracter personal este asigurată 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 de telecomunicații și resursele informaționale;
 - respectării cadrului normativ de folosire a sistemelor informaționale și a programelor de prelucrare a datelor cu caracter personal;
 - asigurării caracterului complet, integru, veridic al datelor cu caracter personal în rețelele de telecomunicații și resurselor informaționale;
 - păstrării posibilităților de gestionare a procesului de prelucrare și păstrare a datelor cu caracter personal.
- 2.8. 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;

- b) excluderea accesului neautorizat la datele cu caracter personal prelucrate;
- c) preîntâmpinarea acțiunilor speciale tehnice și de program, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program;
- d) preîntâmpinarea acțiunilor intenționate și/sau neintenționate a utilizatorilor interni și/sau externi, precum și a altor angajați ai deținătorului de date cu caracter personal, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program.

2.9. În cazul colectării datelor cu caracter personal în modul direct de la subiectul acestora, operatorul din cadrul APM este obligat să furnizeze solicitantului următoarele informații: (i) identitatea operatorului, (ii) scopul prelucrării datelor, (iii) destinatarii datelor cu caracter personal sau existența dreptului de acces al terților la acestea.

2.10. 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, inclusiv cu utilizarea măsurilor organizaționale, tehnice și de regim.

2.11. 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.

2.12. APM se obligă să înceteze prelucrarea datelor cu caracter personal care vizează subiectul de date care și-a manifestat, în formă scrisă și cu o motivare întemeiată, dreptul la opoziție privind prelucrarea datelor sale personale, cu excepția cazurilor în care legea stabilește altfel.

2.13. În condițiile în care, conform prevederilor normative și în vederea asigurării transparenței activității APM se impune necesitatea publicării actelor administrative, rapoartelor, informațiilor sau oricărui alt tip al documentelor care conțin date cu caracter personal, publicarea acestora se permite doar după depersonalizarea datelor personale.

2.14. Operatorul depersonalizează datele cu caracter personal prin retragerea din ele a părții care permite identificarea persoanei fizice, transformându-le în date anonime, care nu pot fi asociate cu o persoană identificată sau identificabilă. În cazul depersonalizării, regimul de confidențialitate stabilit pentru datele respective se anulează.

III. ROLURI ȘI RESPONSABILITĂȚI

3.1. **Primarul General** va dispune delegarea atribuțiilor pentru atingerea obiectivelor în vederea asigurării securității datelor cu caracter personal, precum și modului de prelucrare a acestora în cadrul APM. (Directiva privind protecția datelor permite desemnarea unui funcționar care să acționeze în calitate de funcționar responsabil pentru protecția datelor cu caracter personal). Misiunea acestuia este aceea de a garanta că drepturile și libertățile persoanelor vizate nu vor fi afectate în mod negativ prin operațiunile de prelucrare.

3.2. Responsabilitatea privind securitatea datelor cu caracter personal prelucrate cu ajutorul sistemelor informaționale dar și a programelor de aplicații implicate în procesul de prelucrare revine responsabililor din cadrul APM.

3.3. Managerii operaționali din cadrul subdiviziunilor structurale sunt responsabili de implementarea acestei politici de securitate, precum și de inițierea măsurilor corective și de îmbunătățire, în conformitate cu cadrul funcțional existent.

3.4. O responsabilitate considerabilă revine tuturor angajaților entității, în calitate de utilizatori, în funcție de nivelurile de securitate primite de fiecare în parte pentru acces la resurse, precum și personalului extern care desfășoară activități în folosul entității. Tuturor acestora le revine obligația de a asigura confidențialitatea informațiilor, de a proteja datele cu care vin în contact, precum și resursele tehnologice alocate spre folosință, într-o manieră eficientă, etică și legală.

3.5. Prelucrarea datelor cu caracter personal prin persoana împuternicită de către operator pentru accesul la Registre sau Sisteme informaționale de stat se reglementează printr-un contract sau alt act juridic, care să prevadă drepturile, obligațiile și răspunderea utilizatorului.

IV. SECURITATEA MEDIULUI FIZIC ȘI A TEHNOLOGIILOR INFORMAȚIONALE UTILIZATE ÎN PROCESUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL

4.1. Autorizarea accesului fizic:

4.1.1. Accesul în sediile/ oficiile/ birourile ori spațiile unde sunt amplasate sistemele informaționale de date cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară și doar în timpul orelor de program, conform listei și însemnelor corespunzătoare (permis nominal de acces), conform listei nominale de acces la sistemul informațional.

4.1.2. Accesul în camera de servere este permisă doar personalului Secției tehnologii și sisteme informaționale (în continuare - STSI), personalul străin având acces în această încăpere doar sub stricta supraveghere a unui specialist STSI, iar toate operațiunile de acces la servere sau alte mijloace tehnice se fac de către șeful STSI sau persoana autorizată cu înregistrările respective.

4.1.3. Administrarea și monitorizarea accesului fizic se efectuează în toate punctele de acces la sistemele informaționale de date cu caracter personal, inclusiv se reacționează la încălcarea regimului de acces.

4.1.4. Înainte de acordarea accesului fizic la sistemele informaționale de date cu caracter personal se verifică competențele de acces. Persoanele noi angajate sunt instruite în domeniul prelucrării datelor cu caracter personal și semnează declarația de confidențialitate emisă în acest sens.

4.2. Securitatea sediilor/oficiilor/birourilor și mijloacelor de prelucrare a datelor cu caracter personal:

4.2.1. Perimetrul sediilor și încăperii în care sunt amplasate mijloacele de prelucrare a datelor cu caracter personal sunt păstrate întregre din punct de vedere fizic, toți pereții sunt întregi, ușile se încuie, iar ferestrele se închid.

4.2.2. Computerele, serverele, registrele și alte terminale de acces, în limita posibilității sunt amplasate în locuri cu acces limitat pentru persoane străine.

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

4.3. 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 deținătorului de date cu caracter personal.

4.4. Controlul vizitatorilor este supravegheat în încăperile unde aceștia au acces, în birourile cu acces interzis aceștia pot intra doar sub supravegherea personalului autorizat. În cazul depistării persoanelor cu acces interzis în birourile cu acces limitat, acești vor fi rugați să părăsească încăperea în mod cât mai urgent. Incidentul va fi adus la cunoștința administrației imediat.

4.5. Accesul vizitatorilor în încăperile în care sunt păstrate sistemele prin care sunt gestionate datele cu caracter personal se înregistrează în registru special instituit în acest sens sau se monitorizează prin intermediul sistemului de „control acces”.

4.6. Securitatea electroenergetică asigură integritatea funcțională a echipamentului electric utilizat pentru menținerea funcționalității sistemelor informaționale de date cu caracter personal, a cablurilor electrice, inclusiv protecția acestora contra deteriorărilor. Întru evitarea pierderii datelor și terminarea corectă a sesiunii de lucru a sistemului în cazul deconectării de la sursa de alimentare cu energie electrică sunt instalate surse autonome de alimentare cu energie electrică de scurtă durată (baterii – UPS).

4.7. Securitatea cablurilor de rețea, prin care se efectuează operațiuni de prelucrare a datelor cu caracter personal, asigură protejarea contra conectărilor nesanționate sau deteriorărilor. Cablurile de tensiune sunt separate de cele comunicaționale pentru a exclude bruiatul. Specialiștii STSI efectuează controale, nu mai rar decât o dată în lună, în scopul verificării cazurilor de conectare neautorizată la cablurile de rețea.

4.8. 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 fiind păstrați în safeuri sau dulapuri metalice încuiate;

b) computerele, terminalele de acces și imprimantele sunt 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 prin supravegherea exercitată de către personalul subdiviziunilor vizate;

d) accesul fizic la mijloacele de reprezentare a informației care conține date cu caracter personal, în scopul împiedicării vizualizării acesteia de către persoane neautorizate este interzis și controlat;

e) mijloacele de prelucrare a datelor cu caracter personal, informația care conține date cu caracter personal sau mijloacele de program destinate prelucrării datelor cu caracter personal sunt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a conducătorului autorității publice.

V. IDENTIFICAREA ȘI AUTENTIFICAREA UTILIZATORULUI SISTEMULUI INFORMAȚIONAL DE DATE CU CARACTER PERSONAL

5.1. Identificarea și autentificarea utilizatorilor sistemelor informaționale de date cu caracter personal și a proceselor executate în numele acestor utilizatori este obligatorie. 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 trebuie să conțină semnamentele nivelului de accesibilitate al utilizatorului.

5.1.1 Pentru confirmarea ID-ului utilizatorului sunt utilizate parole. În cazul în care atribuțiile utilizatorului au fost modificate și noile sarcini nu necesită accesul la date cu caracter personal, ori utilizatorul a abuzat de codurile permise în scopul comiterii unei fapte prejudiciabile, a absentat o perioadă îndelungată, codurile de identificare și autentificare se revocă în mod automat în decursul a două săptămâni de la ultimul acces, sau în mod individual imediat la momentul depistării faptelor prejudiciabile comise, precum și încetării/ suspendării/ modificării raporturilor de serviciu.

5.1.2. Se utilizează autentificarea multifactorială, care prezumă parole complexe (minimum 8 caractere), cu includerea simbolurilor, literelor și cifrelor. În mod obligatoriu fiecare parolă conține una sau mai multe litere scrise cu majusculă. Parola nu va conține inițialele sau date care pot caracteriza o anumită persoană (data de naștere, adresă, poreclă, etc.).

5.2. Administrarea identificatorilor utilizatorilor include:

- a) identificarea univocă a fiecărui utilizator;
- b) verificarea autenticității fiecărui utilizator;
- c) obținerea autorizației de la persoana responsabilă pentru eliberarea ID-ului utilizatorului doar în cazul semnării declarației de confidențialitate și trecerii procedurii de instruire;
- d) garantarea faptului că ID-ul utilizatorului este eliberat unei persoane determinate concret;
- e) dezactivarea contului de utilizator după o perioadă inactivă;
- f) executarea copiilor de arhivă a ID-urilor utilizatorilor.

5.3. Asigurarea conexiunii bilaterale în cazul introducerii informației de autentificare a utilizatorilor se asigură prin conexiunea bilaterală a stațiilor de lucru din cadrul APM cu utilizatorul în momentul trecerii de către acesta a procedurilor de autentificare, care nu compromite mecanismul de autentificare.

5.4. Utilizarea parolelor în procesul asigurării securității informaționale respectă regulile de asigurare a securității informaționale în cazul alegerii și folosirii parolelor care includ:

- a) păstrarea confidențialității parolelor;
- b) interzicerea înscrierii parolelor pe suport de hârtie, în cazul în care nu se asigură securitatea păstrării acestuia;
- c) modificarea parolelor de fiecare dată când sunt prezente indiciile eventualei compromiteri a sistemului sau parolei;
- d) alegerea parolelor calitative, care nu sunt legate de informația cu caracter personal a utilizatorului, nu conțin simboluri identice consecutive și nu sunt compuse integral din grupuri de cifre sau litere;
- e) modificarea parolelor peste anumite intervale de timp (cel puțin 6 luni) și la necesitate;
- f) dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate).

5.5. Pentru asigurarea posibilității de stabilire a responsabilității sunt utilizate parole individuale pentru fiecare utilizator. Se interzice transmiterea parolelor individuale către alți angajați sau persoane terțe.

5.6. Se va asigura ca la momentul introducerii parolei aceasta să nu fie reflectată pe monitor, iar după trei tentative greșite de autentificare sistemul va bloca accesul utilizatorului.

VI. ADMINISTRAREA ACCESULUI UTILIZATORILOR

- 6.1. Administrarea accesului se implementează prin mecanisme de înregistrare și evidență a persoanelor care au acces sau participă la operațiunile de prelucrare a datelor cu caracter personal și care, în caz de necesitate, permit identificarea cazurilor neautorizate de acces sau de prelucrare ilegală a datelor cu caracter personal.
- 6.2. Sunt folosite mijloace automatizate de suport în scopul administrării conturilor de acces (account-uri). Acțiunea conturilor de acces a utilizatorilor temporari, care prelucrează date cu caracter personal, încetează automat la expirarea unei perioade stabilite în timp sau după o perioadă de maxim trei luni de când utilizatorii nu sunt activi. Informația despre crearea, activarea, modificarea, revizuirea, dezactivarea și ștergerea conturilor de acces se stochează utilizând mijloace automatizate.
- 6.3. Acordarea accesului la sistemele informaționale de date cu caracter personal este autorizat în conformitate cu prezenta Politică.
- 6.4. Revizuirea drepturilor de acces ale utilizatorilor sunt revizuite cu regularitate pentru asigurarea faptului că nu au fost acordate drepturi de acces neautorizate (maximum peste fiecare șase luni) și după oricare schimbare de statut al utilizatorului.
- 6.5. Repartizarea obligațiilor subiecților care asigură funcționarea sistemelor informaționale de date cu caracter personal este efectuată prin intermediul investiției cu drepturi/competențe corespunzătoare de acces, prin dispoziția/ ordinul emis de conducătorul APM în acest sens. Utilizatorii sistemelor informaționale de date cu caracter personal se investesc doar cu acele drepturi/competențe, care sunt necesare pentru realizarea de către ei a obiectivelor stabilite acestora.
- 6.6. Înainte de acordarea accesului în sistem, utilizatorii sunt informați despre faptul că folosirea sistemelor informaționale de date cu caracter personal este controlată și că folosirea neautorizată a acestora se urmărește în conformitate cu legislația.
- 6.7. Sesiunea de lucru în sistemul informațional, destinat prelucrării datelor cu caracter personal, se blochează automat, după maxim 15 minute de perioadă inactivă a utilizatorului fapt care face imposibil accesul de mai departe până în momentul când utilizatorul nu deblochează sesiunea de lucru prin metoda trecerii repetate a procedurilor de identificare și autentificare.
- 6.8. Se efectuează controlul acțiunilor utilizatorului în vederea evaluării corectitudinii și conformării operațiunilor și acțiunilor efectuate prin intermediul sistemelor informaționale de date cu caracter personal.
- 6.9. Informația ieșită din sistem, care conține date cu caracter personal, se marchează, indicându-se prescripții pentru prelucrarea ulterioară și răspândirea acesteia.
- 6.10. Se interzice accesul de la distanță a sistemelor informaționale de date cu caracter personal formate de APM, inclusiv folosirea tehnologiilor fără fir sau utilizarea echipamentului portativ și mobil (cu excepția notebook-urilor aflate la balanța APM și setate corespunzător de către STSI).

VII. PROTECȚIA SISTEMELOR INFORMAȚIONALE ȘI COMUNICAȚIILOR ÎN CARE SUNT PRELUCRATE DATE CU CARACTER PERSONAL

- 7.1. Se asigură separarea posibilităților funcționale ale utilizatorului de posibilitățile funcționale de gestionare a sistemelor informaționale de date cu caracter personal.
- 7.2. Se asigură izolarea funcțiilor de securitate de funcțiile care nu se atribuie la securitatea sistemelor informaționale de date cu caracter personal.

7.3. Este asigurată posibilitatea limitării, cu ajutorul mecanismelor de stabilire a priorităților, a folosirii resurselor informaționale în care sunt prelucrate date cu caracter personal.

7.4. Se efectuează monitorizarea permanentă și controlul comunicațiilor la perimetrul exterior al sistemelor informaționale de date cu caracter personal, inclusiv la cele mai importante puncte de contact în interiorul perimetrului acestor sisteme informaționale. Amplasarea resurselor general accesibile se asigură în spațiile special destinate a rețelei. Este asigurată imposibilitatea accesului din exterior a utilizatorilor la rețeaua internă în care se prelucrează date cu caracter personal.

7.5. Se asigură confidențialitatea datelor cu caracter personal transmise, utilizându-se mijloace de protecție criptografică a informației.

VIII. AUDITUL SECURITĂȚII ÎN SISTEMELE INFORMAȚIONALE DE DATE CU CARACTER PERSONAL

8.1. Înregistrările de audit a securității registrelor ținute manual în care sunt 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.

8.2. Responsabilul de administrarea sistemelor informaționale este obligat să întocmească următoarele proceduri de audit al sistemului:

- a) Înregistrarea tentativelor de intrare/ieșire a utilizatorului în sistem, conform datei și timpului tentativei intrării/ ieșirii, ID-ul utilizatorului și rezultatului tentativei de intrare/ieșire (pozitivă sau negativă).
- b) Înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative și proceselor, destinate prelucrării datelor cu caracter personal, înregistrarea modificărilor drepturilor de acces ale utilizatorilor și statutul obiectelor de acces conform datei și timpului tentativei de pornire, denumirii/ identificatorului programului aplicativ sau procesului, ID-ului utilizatorului, rezultatului tentativei de pornire (pozitivă sau negativă).
- c) Înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării datelor cu caracter personal, conform datei și timpului tentativei de obținere a accesului (executare a operațiunii), denumirii (identificatorul aplicației sau procesului, ID-ul utilizatorului, specificațiilor resursei protejate (identificator, nume logic, nume fișier, număr etc), tipului operațiunii solicitate (citire, înregistrare, ștergere etc), rezultatului tentativei de obținere a accesului (executare a operațiunii) - pozitivă sau negativă.
- d) Înregistrarea modificărilor drepturilor de acces (competențelor) utilizatorului și statutului obiectelor de acces, conform datei și timpul modificării competențelor, ID-ului administratorului care a efectuat modificările, ID-ul utilizatorului și competențele acestuia sau specificarea obiectelor de acces și statutul nou al acestora.

8.3. În caz de deranjament al auditului securității în sistemele informaționale de date cu caracter personal sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, este informată persoana responsabilă de politica de securitate a datelor cu caracter personal și întreprinse măsuri în vederea restabilirii capacității de lucru a sistemului de audit.

8.4. Se efectuează monitorizarea permanentă și analiza înregistrărilor de audit a securității în sistemele informaționale de date cu caracter personal, în scopul depistării activităților neobișnuite sau

suspecte de utilizare a acestor sisteme informaționale, cu întocmirea raportului referitor la cazurile depistării acestor activități, stocate în mijloacele electronice de calcul.

8.5. Rezultatele auditului securității în sistemele informaționale de date cu caracter personal, care reprezintă operațiuni de prelucrare a datelor cu caracter personal și mijloacele de efectuare a auditului, se protejează contra accesului neautorizat prin instituirea măsurilor de securitate adecvate, inclusiv prin asigurarea confidențialității și integrității acestora.

8.6. Durata stocării rezultatelor auditului securității în sistemele informaționale de date cu caracter personal se justifică în politica de securitate a datelor cu caracter personal, dar în orice caz acest termen nu este mai mic de 2 ani, pentru a fi posibil folosirea acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigații sau procese judiciare.

IX. ASIGURAREA INTEGRITĂȚII INFORMAȚIEI CARE CONȚINE DATE CU CARACTER PERSONAL ȘI A TEHNOLOGIILOR INFORMAȚIONALE

9.1. Se asigură identificarea, înregistrarea și înlăturarea deficiențelor mijloacelor de program destinate prelucrării datelor cu caracter personal, inclusiv instalarea corectărilor și pachetelor de reînnoire a acestor mijloace de program.

9.2. Se asigură protecția contra infiltrării programelor dăunătoare mijloacelor de program destinate prelucrării datelor cu caracter personal, măsură care asigură posibilitatea reînnoirii automate și la timp a mijloacelor de asigurare a protecției contra programelor dăunătoare și signaturilor de virus.

9.3. Se utilizează tehnologii și mijloace de constatare a intruziunilor, care permit monitorizarea evenimentelor în sistemele informaționale de date cu caracter personal și constatarea atacurilor, inclusiv care asigură identificarea tentativelor folosirii neautorizate a sistemelor informaționale.

9.4. Se asigură protecția și posibilitatea depistării modificării neautorizate a soft-urilor destinate prelucrării datelor cu caracter personal și informației care conține date cu caracter personal.

9.5. 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).

X. COPIILE DE REZERVĂ ȘI RESTABILIREA INFORMAȚIEI CARE CONȚINE DATE CU CARACTER PERSONAL ȘI IT

10.1. Copiile de rezervă ale informației care conține date cu caracter personal. Copiile de siguranță a informațiilor care conțin date cu caracter personal și soft-urilor folosite pentru prelucrările automatizate a datelor cu caracter personal, sunt efectuate automatizat odată la 24 ore, fiind păstrate cel puțin 1 an în locuri sigure, cu acces limitat.

10.2. Copiile de siguranță se testează în scopul verificării siguranței purtătorilor de informații și integrității informației care conține date cu caracter personal. 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 SISTEMELOR INFORMAȚIONALE DE DATE CU CARACTER PERSONAL

11.1. Incidentele de securitate a informației sunt evenimente ce au dus sau ar fi putut duce la realizarea riscurilor de securitate a informației, ca rezultat al eșecului în cadrul proceselor, sistemelor, oamenilor sau în rezultatul evenimentelor externe. Un incident se produce nu doar atunci când există impact asupra securității resurselor informaționale (realizarea riscului) și atunci când un asemenea impact este posibil (risc nerealizat).

11.2. Personalul care asigură exploatarea sistemelor informaționale de date cu caracter personal va trece, minimum o dată în an, instruirea referitor la responsabilitățile și obligațiile în cazul executării acțiunilor de gestionare și reacționare la incidentele de securitate.

11.3. În cazul depistării unui incident de securitate, este asigurat mecanismul de informare neîntârziată a conducerii autorității publice. Prelucrarea incidentelor include în mod obligator: depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor și restabilirea securității inițiale.

11.4. Incidentele de securitate a sistemelor informaționale de date cu caracter personal se urmăresc și se documentează în regim permanent.

11.5. Anual, către 31 ianuarie, persoana responsabilă de Politica de securitate va prezenta CNPDCP raportul generalizat despre incidentele de securitate a sistemelor informaționale de date cu caracter personal.

11.6. Nerespectarea cerințelor prezentei Politicii condiționează survenirea răspunderii civile, contravenționale și penale, conform legislației în vigoare

XII. SPECIFICUL CERINȚELOR DE SECURITATE ÎN CAZUL PRELUCRĂRII CATEGORIILOR SPECIALE A DATELOR CU CARACTER PERSONAL

12.1. Categoria specială a datelor cu caracter personal o constituie informația care dezvăluie originea rasială sau etnică, convingerile politice, religioase, privind starea de sănătate sau viața intimă, precum și cele privind condamnările penale ale unei persoane fizice.

12.2. Prelucrarea categoriilor speciale de date cu caracter personal se efectuează doar în cazul obținerii consimțământului explicit al subiectului, în cazul incapacității de exercițiu sau al capacității limitate de exercițiu, consimțământul pentru prelucrarea datelor personale este obținut de la reprezentantul legal și doar în formă scrisă.

12.3. În cazul prelucrării datelor cu caracter personal din categoria celor speciale, APM implementează cerințele nivelului doi de securitate a sistemelor de date cu caracter personal care constau în:

12.3.1. Încăperile unde sunt instalate sistemele informaționale de date cu caracter personal se echipează cu sisteme de control al accesului și supraveghere video în scopul urmăririi accesului persoanelor în aceste spații.

12.3.2. Pentru asigurarea securității sediilor, oficiilor, birourilor sunt instalate sisteme de constatare a intruziunilor pentru ușile exterioare și ferestrele amplasate în locuri accesibile.

12.3.3. Utilajul de rezervă și purtătorii de informații care conțin date cu caracter personal se păstrează în locuri care permit evitarea distrugerilor sau deteriorărilor ca rezultat al calamităților în sediul/ oficiul/ biroul de bază.

- 12.3.4. Se asigură administrarea centralizată a mecanismelor de protecție contra programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal.
- 12.3.5. Copiile de siguranță a datelor se păstrează în cutii metalice cu sigiliu aplicat și stocate în afara zonei de amplasare a informației care conține date cu caracter personal de soft-urile de bază.
- 12.3.6. Sunt utilizate mijloace automatizate pentru urmărirea incidentelor de securitate a sistemelor informaționale de date cu caracter personal, colectarea și analiza informației despre aceste incidente se efectuează de către persona desemnată pentru monitorizarea modului de aplicare a cerințelor prezentei Politici.
- 12.3.7. Se interzice instalarea altor dispozitive electrice, radio sau de alt gen în încăperile unde sunt amplasate mijloacele tehnice de prelucrare a datelor cu caracter personal din categoria specială.

**XIII. SPECIFICUL CERINȚELOR DE SECURITATE ÎN CAZUL FORMEI
MANUALE DE ȚINERE A REGISTRELOR ÎN CARE SUNT
PRELUCRATE DATE CU CARACTER PERSONAL**

- 13.1. Prevederile prezentelor Cerințe, cu excepția celor aplicabile în exclusivitate sistemelor de date/ programelor informatice, se aplică corespunzător de către deținătorii de date cu caracter personal în cazul formei manuale de ținere a registrelor în care sunt prelucrate seriile structurate de date cu caracter personal, accesibile conform criteriilor centralizate sau descentralizate, ori repartizate conform criteriilor funcționale sau geografice.

SECRETAR INTERIMAR AL MUNICIPIULUI CHIȘINĂU



Adrian TALMACI