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

2017

I. DISPOZIŢII GENERALE

1.1. Politica de securitate a prelucrării datelor cu caracter personal în cadrul subdiviziunilor administrației publice municipale (în continuare – Politica) stabileşte principiile şi cerinţele faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale automatizate şi mecanice de date cu caracter personal.

1.2. Politica are drept scop stabilirea regulilor de implementare de către subdiviziunile administrației publice municipale (conform *anexei A* la prezenta Politică) a măsurilor tehnice şi organizatorice necesare pentru asigurarea securităţii, confidenţialităţii şi integrităţii datelor cu caracter personal prelucrate în cadrul sistemelor informaţionale automatizate şi mecanice de date cu caracter personal şi/ sau registrelor ţinute manual.

1.3. Politica este elaborată în conformitate cu prevederile Legii Nr. 133 din 08.07.2011 privind protecţia datelor cu caracter personal şi Legii nr. 71-XVI din 22 martie 2007 cu privire la registre, Hotărârii Guvernului nr. 1123 din 14.12.2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, precum şi Convenţiei pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal (Strasbourg, 28 ianuarie 1981).

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

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);

autentificare - verificarea identificatorului atribuit subiectului de acces, confirmarea autenticităţii;

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 constrângere sau sancţiunile contravenţionale;

date cu caracter personal (DCP) (categoria obişnuită) – 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;

fişiere temporare - ansamblu de date sau informaţii pe suport digital creat pentru o perioadă de timp limitat până la iniţierea îndeplinirii sarcinilor pentru care au fost desemnate;

identificare - atribuirea unui identificator subiecţilor şi obiectelor de acces şi/sau compararea identificatorului prezentat cu lista identificatoarelor atribuite;

integritate - certitudinea, necontradictorialitatea şi actualitatea informaţiei care conţine date cu caracter personal, protecţia ei de distrugere şi modificare neautorizată;

politica de securitate a datelor cu caracter personal - un set de reguli, cerinţe şi instrucţiuni aplicabile la nivelul entității, care stă la baza infrastructurii de securitate şi stabileşte limitele unui comportament acceptabil în utilizarea resurselor informaţionale şi de comunicaţii ale entității.

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

persoana responsabilă de politica de securitate a datelor cu caracter personal – persoana responsabilă de funcţionarea corespunzătoare a sistemului complex de protecţie a informaţiei, care conţine date cu caracter personal, precum şi de elaborarea, implementarea şi monitorizarea respectării prevederilor politicii de securitate a deţinătorului de date cu caracter personal;

prelucrarea datelor cu caracter personal – orice operaţiune sau serie de operaţiuni 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, ştergerea sau distrugerea;

protecţia informaţiei contra acţiunilor neintenţionate - ansamblu de măsuri orientate spre prevenirea acţiunilor neintenţionate, provocate de erorile utilizatorului, defectele mijloacelor tehnico-aplicative, fenomenele naturii sau alte cauze ce nu au ca scop direct modificarea informaţiei, dar care conduc la distorsiunea, distrugerea, copierea, blocarea accesului la informaţie, precum şi la pierderea, distrugerea acesteia sau la defectarea suportului material al informaţiei care conţine date cu caracter personal;

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

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 informaţională (TI) - totalitatea metodelor, procedeelor şi mijloacelor de prelucrare şi transmitere a informaţiei care conţine date cu caracter personal şi regulile de aplicare a acesteia;

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

sesiune de lucru - perioada care durează din momentul pornirii calculatorului şi aplicaţiei de utilizare a resursei informaţionale sau din momentul pornirii resursei informaţionale şi până la momentul opririi acestora;

sistem informaţional de date cu caracter personal - totalitatea resurselor şi tehnologiilor informaţionale interdependente, de metode şi de personal, destinată păstrării, prelucrării şi furnizării de informaţie care conţine date cu caracter personal;

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

II. CERINŢE GENERALE

2.1. Măsurile de protecţie a datelor cu caracter personal reprezintă o parte componentă a lucrărilor de creare, dezvoltare şi exploatare a sistemelor informaţionale de date cu caracter personal şi vor fi efectuate neîntrerupt de către persoanele responsabile angajate în cadrul APM.

2.2. Protecţia datelor cu caracter personal este asigurată printr-un complex de măsuri tehnice şi 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 protecţia 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:

a) prelucrate în mod corect și conform prevederilor normative din domeniu;

b) colectate doar în scopuri determinate, explicite și legitime pentru asigurarea prestării serviciilor publice corespunzătoare;

c) 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 protecţie a datelor cu caracter personal prelucrate în sistemele informaţionale şi mecanice de date cu caracter personal ale APM se realizează ținându-se cont de necesitatea asigurării confidenţialităţii acestor măsuri.

2.6. Sunt supuse protecţiei toate resursele informaţionale ale APM, care conţin date cu caracter personal, inclusiv:

a) suporturile magnetice, optice, laser sau alte suporturi ale informaţiei electronice, masive informaţionale şi baze de date;

b) sistemele informaţionale, reţelele, sistemele operaţionale, sistemele de gestionare a bazelor de date şi alte aplicaţii, sistemele de telecomunicaţii, inclusiv mijloacele de confecţionare şi multiplicare a documentelor și alte mijloace de prelucrare a informaţiei.

2.7. Protecţia datelor cu caracter personal în sistemele informaţionale de date cu caracter personal este asigurată în scopul:

a) preîntâmpinării scurgerii informaţiei care conţine date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;

b) preîntâmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în reţelele de telecomunicaţii şi resursele informaţionale;

c) respectării cadrului normativ de folosire a sistemelor informaţionale şi a programelor de prelucrare a datelor cu caracter personal;

d) asigurării caracterului complet, integru, veridic al datelor cu caracter personal în reţelele de telecomunicaţii şi resurselor informaţionale;

e) păstrării posibilităţilor de gestionare a procesului de prelucrare şi păstrare a datelor cu caracter personal.

2.8. Protecţia datelor cu caracter personal prelucrate în sistemele informaţionale se efectuează prin următoarele metode:

a) preîntâmpinarea conexiunilor neautorizate la reţelele telecomunicaţionale şi interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste reţele;

b) excluderea accesului neautorizat la datele cu caracter personal prelucrate;

c) preîntâmpinarea acţiunilor speciale tehnice şi de program, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program;

d) preîntâmpinarea acţiunilor intenţionate şi/sau neintenţionate a utilizatorilor interni şi/sau externi, precum şi a altor angajaţi ai deţinătorului de date cu caracter personal, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi 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 informaţii care conţin date cu caracter personal, transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informaţii, inclusiv cu utilizarea măsurilor organizaţionale, tehnice şi de regim.

2.11. Preîntâmpinarea distrugerii, modificării datelor cu caracter personal sau defecţiunilor în funcţionarea soft-ului destinat prelucrării datelor cu caracter personal este asigurată prin metoda folosirii mijloacelor de protecţie speciale tehnice şi de program, inclusiv a programelor licenţiate, programelor antivirus, organizării sistemului de control al securităţii soft-ului şi efectuarea periodică a copiilor de siguranţă.

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 părţii 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 confidenţialitate stabilit pentru datele respective se anulează.

III. ROLURI ȘI RESPONSABILITĂȚI

3.1. **Primarul General** va dispune delegarea atribuţiilor pentru atingerea obiectivelor în vederea asigurării securității datelor cu caracter personal, precum și modului de prelucrare a acestora în cadrul APM. (Directiva privind protecţia datelor permite desemnarea unui funcţionar care să acţioneze în calitate de funcţionar responsabil pentru protecţia datelor cu caracter personal). Misiunea acestuia este aceea de a garanta că drepturile şi libertăţile persoanelor vizate nu vor fi afectate în mod negativ prin operaţiunile 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 şi de iniţierea măsurilor corective şi de îmbunătăţire, în conformitate cu cadrul funcţional existent.
3.4. O responsabilitate considerabilă revine tuturor angajaţilor entității, în calitate de **utilizatori**, în funcţie de nivelurile de securitate primite de fiecare în parte pentru acces la resurse, precum şi personalului extern care desfăşoară activităţi în folosul entității. Tuturor acestora le revine obligaţia de a asigura confidențialitatea informațiilor, de a proteja datele cu care vin în contact, precum şi resursele tehnologice alocate spre folosinţă, într-o manieră eficientă, etică şi 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 ŞI A TEHNOLOGIILOR INFORMAŢIONALE UTILIZATE ÎN PROCESUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL

4.1. Autorizarea accesului fizic:

4.1.1. Accesul în sediile/ oficiile/ birourile ori spaţiile unde sunt amplasate sistemele informaţionale de date cu caracter personal este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară şi doar în timpul orelor de program, conform listei şi însemnelor corespunzătoare (permis nominal de acces), conform listei nominale de acces la sistemul informaţional.
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 operaţiunile de acces la servere sau alte mijloace tehnice se fac de către şeful STSI sau persoana autorizată cu înregistrările respective.
4.1.3. Administrarea şi monitorizarea accesului fizic se efectuează în toate punctele de acces la sistemele informaţionale de date cu caracter personal, inclusiv se reacţionează la încălcarea regimului de acces.
4.1.4. Înainte de acordarea accesului fizic la sistemele informaţionale de date cu caracter personal se verifică competenţele de acces. Persoanele noi angajate sunt instruite în domeniul prelucrării datelor cu caracter personal şi semnează declaraţia de confidenţialitate emisă în acest sens.

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

4.2.1. Perimetrul sediilor şi încăperii în care sunt amplasate mijloacele de prelucrare a datelor cu caracter personal sunt păstrate integre din punct de vedere fizic, toţi pereţii sunt întregi, uşile se încuie, iar ferestrele se închid.
4.2.2. Computerele, serverele, registrele şi alte terminale de acces, în limita posibilităţii sunt amplasate în locuri cu acces limitat pentru persoane străine.
4.2.3. Amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespunde necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.

4.3. Folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare în perimetrul de securitate este admisă doar în cazul prezenţei unei permisiuni speciale a conducerii deţinătorului de date cu caracter personal.

4.4. Controlul vizitatorilor este supravegheat în încăperile unde aceştia au acces, în birourile cu acces interzis aceştia pot intra doar sub supravegherea personalului autorizat. În cazul depistării persoanelor cu acces interzis în birourile cu acces limitat, aceşti vor fi rugaţi să părăsească încăperea în mod cât mai urgent. Incidentul va fi adus la cunoştinţa administraţiei 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 menţinerea funcţionalităţii sistemelor informaţionale de date cu caracter personal, a cablurilor electrice, inclusiv protecţia acestora contra deteriorărilor. Întru evitarea pierderii datelor şi 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 reţea, prin care se efectuează operaţiuni de prelucrare a datelor cu caracter personal, asigură protejarea contra conectărilor nesancţionate sau deteriorărilor. Cablurile de tensiune sunt separate de cele comunicaţionale pentru a exclude bruiajul. Specialiştii STSI efectuează controale, nu mai rar decât o dată în lună, în scopul verificării cazurilor de conectare neautorizată la cablurile de reţea.

4.8. Măsurile generale de administrare a securităţii informaţionale:

a) în cazul neutilizării temporare a purtătorilor de informaţie pe suport de hârtie sau electronici (digitali) care conţin date cu caracter personal, aceştia fiind păstrați în safeuri sau dulapuri metalice încuiate;

b) computerele, terminalele de acces şi imprimantele sunt deconectate la terminarea sesiunilor de lucru;

c) este asigurată securitatea punctelor de primire/ expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele fax şi de copiere prin supravegherea exercitată de către personalul subdiviziunilor vizate;

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

e) mijloacele de prelucrare a datelor cu caracter personal, informaţia care conţine 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 ŞI AUTENTIFICAREA UTILIZATORULUI SISTEMULUI INFORMAŢIONAL DE DATE CU CARACTER PERSONAL

5.1. Identificarea şi autentificarea utilizatorilor sistemelor informaţionale de date cu caracter personal şi a proceselor executate în numele acestor utilizatori este obligatorie. Toţi utilizatorii (inclusiv personalul care asigură susţinerea tehnică, administratorii de reţea, programatorii şi

administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu trebuie să conţină semnalmentele 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 şi noile sarcini nu necesită accesul la date cu caracter personal, ori utilizatorul a abuzat de codurile primite în scopul comiterii unei fapte prejudiciabile, a absentat o perioadă îndelungată, codurile de identificare şi autentificare se revocă 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 conţine una sau mai multe litere scrise cu majusculă. Parola nu va conţine iniţialele sau date care pot caracteriza o anumită persoană (data de naştere, adresă, poreclă, etc.).

5.2. Administrarea identificatorilor utilizatorilor include:

a) identificarea univocă a fiecărui utilizator;

b) verificarea autenticităţii fiecărui utilizator;

c) obţinerea autorizaţiei de la persoana responsabilă pentru eliberarea ID-ului utilizatorului doar în cazul semnării declaraţiei de confidenţialitate şi 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 informaţiei de autentificare a utilizatorilor se asigură prin conexiunea bilaterală a staţiilor 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 securităţii informaţionale respectă regulile de asigurare a securităţii informaţionale în cazul alegerii şi folosirii parolelor care includ:

a) păstrarea confidenţialităţii 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 informaţia cu caracter personal a utilizatorului, nu conţin simboluri identice consecutive şi 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 posibilităţii de stabilire a responsabilităţii 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 **s**e implementează prin mecanisme de înregistrare şi evidenţă a persoanelor care au acces sau participă la operaţiunile de prelucrare a datelor cu caracter personal şi 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). Acţiunea 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 informaţionale 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 şase luni) şi după oricare schimbare de statut al utilizatorului.

6.5. Repartizarea obligaţiilor subiecţilor care asigură funcţionarea sistemelor informaţionale de date cu caracter personal este efectuată prin intermediul învestirii cu drepturi/competenţe corespunzătoare de acces, prin dispoziția/ ordinul emis de conducătorul APM în acest sens. Utilizatorii sistemelor informaţionale de date cu caracter personal se învestesc doar cu acele drepturi/ competenţe, care sunt necesare pentru realizarea de către ei a obiectivelor stabilite acestora.

6.6. Înainte de acordarea accesului în sistem, utilizatorii sunt informaţi despre faptul că folosirea sistemelor informaţionale de date cu caracter personal este controlată şi că folosirea neautorizată a acestora se urmăreşte în conformitate cu legislaţia.

6.7. Sesiunea de lucru în sistemul informaţional, 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 şi autentificare.

6.8. Se efectuează controlul acţiunilor utilizatorului în vederea evaluării corectitudinii şi conformării operaţiunilor şi acţiunilor efectuate prin intermediul sistemelor informaţionale 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. PROTECŢIA SISTEMELOR INFORMAŢIONALE ŞI COMUNICAŢIILOR ÎN CARE SÎNT PRELUCRATE DATE CU CARACTER PERSONAL

7.1. Se asigură separarea posibilităţilor funcţionale ale utilizatorului de posibilităţile funcţionale de gestionare a sistemelor informaţionale de date cu caracter personal.

7.2. Se asigură izolarea funcţiilor de securitate de funcţiile care nu se atribuie la securitatea sistemelor informaţionale de date cu caracter personal.

7.3. Este asigurată posibilitatea limitării, cu ajutorul mecanismelor de stabilire a priorităţilor, a folosirii resurselor informaţionale în care sunt prelucrate date cu caracter personal.
7.4. Se efectuează monitorizarea permanentă şi controlul comunicaţiilor la perimetrul exterior al sistemelor informaţionale de date cu caracter personal, inclusiv la cele mai importante puncte de contact în interiorul perimetrului acestor sisteme informaţionale. Amplasarea resurselor general accesibile se asigură în spaţiile special destinate a rețelei. Este asigurată imposibilitatea accesului din exterior a utilizatorilor la reţeaua internă în care se prelucrează date cu caracter personal.
7.5. Se asigură confidenţialitatea datelor cu caracter personal transmise, utilizîndu-se mijloace de protecţie criptografică a informaţiei.

VIII. AUDITUL SECURITĂŢII ÎN SISTEMELE INFORMAŢIONALE DE DATE CU CARACTER PERSONAL

8.1. Înregistrările de audit a securităţii registrelor ţinute manual în care sunt prelucrate date cu caracter personal, trebuie să conţină: numele şi prenumele utilizatorului; numele fişei accesate (pagina şi inscripţia din registru); numărul înregistrărilor efectuate; tipul de acces; data accesului (an, lună, zi); timpul (ora, minuta) şi durata accesului.
8.2. Responsabilul de administrarea sistemelor informaționale este obligat să întocmească următoarele proceduri de audit al sistemului:

a) Înregistrarea tentativelor de intrare/ieşire a utilizatorului în sistem, conform datei şi timpului tentativei intrării/ ieşirii, ID-ul utilizatorului şi rezultatului tentativei de intrare/ieşire (pozitivă sau negativă).
b) Înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative şi proceselor, destinate prelucrării datelor cu caracter personal, înregistrarea modificărilor drepturilor de acces ale utilizatorilor şi statutul obiectelor de acces conform datei şi timpului tentativei de pornire, denumirii/ identificatorului programului aplicativ sau procesului, ID-ului utilizatorului, rezultatului tentativei de pornire (pozitivă sau negativă).
c) Înregistrarea tentativelor de obţinere a accesului (de executare a operaţiunilor) pentru aplicaţii şi procese destinate prelucrării datelor cu caracter personal, conform datei şi timpului tentativei de obţinere a accesului (executare a operaţiunii), denumirii (identificatorul) aplicaţiei sau procesului, ID-ul utilizatorului, specificaţiilor resursei protejate (identificator, nume logic, nume fişier, număr etc), tipului operaţiunii solicitate (citire, înregistrare, ştergere etc), rezultatului tentativei de obţinere a accesului (executare a operaţiunii) - pozitivă sau negativă.
d) Înregistrarea modificărilor drepturilor de acces (competenţelor) utilizatorului şi statutului obiectelor de acces, conform datei şi timpul modificării competenţelor, ID-ului administratorului care a efectuat modificările, ID-ul utilizatorului şi competenţele acestuia sau specificarea obiectelor de acces şi statutul nou al acestora.

8.3. În caz de deranjament al auditului securităţii în sistemele informaţionale 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 şi întreprinse măsuri în vederea restabilirii capacităţii de lucru a sistemului de audit.
8.4. Se efectuează monitorizarea permanentă şi analiza înregistrărilor de audit a securităţii în sistemele informaţionale de date cu caracter personal, în scopul depistării activităţilor neobişnuite sau

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

8.5. Rezultatele auditului securităţii în sistemele informaţionale de date cu caracter personal, care reprezintă operaţiuni de prelucrare a datelor cu caracter personal şi mijloacele de efectuare a auditului, se protejează contra accesului neautorizat prin instituirea măsurilor de securitate adecvate, inclusiv prin asigurarea confidenţialităţii şi integrităţii acestora.

8.6. Durata stocării rezultatelor auditului securităţii în sistemele informaţionale 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 investigaţii sau procese judiciare.

IX. ASIGURAREA INTEGRITĂŢII INFORMAŢIEI CARE CONŢINE DATE CU CARACTER PERSONAL ŞI A TEHNOLOGIILOR INFORMAŢIONALE

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

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

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

9.4. Se asigură protecţia şi posibilitatea depistării modificării neautorizate a soft-urilor destinate prelucrării datelor cu caracter personal şi informaţiei care conţine date cu caracter personal.

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

X. COPIILE DE REZERVĂ ŞI RESTABILIREA INFORMAŢIEI CARE CONŢINE DATE CU CARACTER PERSONAL ŞI IT

10.1. Copiile de rezervă ale informaţiei care conţine date cu caracter personal. Copiile de siguranţă a informaţiilor care conţin date cu caracter personal şi soft-urilor folosite pentru prelucrările automatizate a datelor cu caracter personal, sunt efectuate automatizat odată la 24 ore, fiind păstrate cel puţin 1 an în locuri sigure, cu acces limitat.

10.2. Copiile de siguranţă se testează în scopul verificării siguranţei purtătorilor de informaţii şi integrităţii informaţiei care conţine date cu caracter personal. 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 SISTEMELOR INFORMAŢIONALE 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 informaţionale de date cu caracter personal va trece, minimum o dată în an, instruirea referitor la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare 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 şi restabilirea securităţii iniţiale.

11.4. Incidentele de securitate a sistemelor informaţionale de date cu caracter personal se urmăresc şi 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 informaţionale de date cu caracter personal.

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

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

12.1. Categoria specială a datelor cu caracter personal o constituie informaţia care dezvăluie originea rasială sau etnică, convingerile politice, religioase, privind starea de sănătate sau viaţa intimă, precum şi 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 care caracter personal care constau în:

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

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

12.3.3. Utilajul de rezervă şi purtătorii de informaţii care conţin date cu caracter personal se păstrează în locuri care permit evitarea distrugerilor sau deteriorărilor ca rezultat al calamităţilor în sediul/ oficiul/ biroul de bază.

12.3.4. Se asigură administrarea centralizată a mecanismelor de protecţie contra programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal.

12.3.5. Copiile de siguranţă a datelor se păstrează în cutii metalice cu sigiliu aplicat şi stocate în afara zonei de amplasare a informaţiei care conţine date cu caracter personal de soft-urile de bază.

12.3.6. Sunt utilizate mijloace automatizate pentru urmărirea incidentelor de securitate a sistemelor informaţionale de date cu caracter personal, colectarea şi analiza informaţiei despre aceste incidente se efectuează de către persona desemnată pentru monitorizarea modului de aplicare a cerinţelor 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 CERINŢELOR DE SECURITATE ÎN CAZUL FORMEI MANUALE DE ŢINERE A REGISTRELOR ÎN CARE SUNT PRELUCRATE DATE CU CARACTER PERSONAL

13.1. Prevederile prezentelor Cerinţe, cu excepţia celor aplicabile în exclusivitate sistemelor de date/ programelor informatice, se aplică corespunzător de către deţinătorii de date cu caracter personal în cazul formei manuale de ţinere a registrelor în care sunt prelucrate seriile structurate de date cu caracter personal, accesibile conform criteriilor centralizate sau descentralizate, ori repartizate conform criteriilor funcţionale sau geografice.

SECRETAR INTERIMAR AL MUNICIPIULUI CHIŞINĂU

Adrian TALMACI