Anexa nr. 3
la Hotărîrea Guvernului nr.1236/2018

POLITICA DE SECURITATE A DATELOR CU CARACTER PERSONAL ÎN CADRUL PRIMĂRIEI ORAȘULUI NISPORENI

I. INTRODUCERE

1. Politica de securitate a datelor cu caracter personal este aprobată de către Consiliul orășenesc Nisporeni, conform denumirii oficiale, la forma gramaticală respectivă, în continuare după text], care acţionează în baza Legii privind administraţia publică locală nr. 436-XVI din 28.12.2006, şi are sediul înregistrat pe adresa: or.Nisporeni, str. Alexandru cel Bun nr.55.

2. Politica de securitate este aprobată în vederea conformării Primăriei orașului Nisporeni cu prevederile Legii nr.133/2011 privind protecţia datelor cu caracter personal şi ale Hotărîrii Guvernului nr.1123/2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal.

3. La prelucrarea datelor cu caracter personal în cadrul entităţii sînt aplicate principiile prevăzute în actele internaţionale: Declaraţia universală a drepturilor omului, Convenţia pentru apărarea drepturilor omului şi a libertăţilor fundamentale, Convenţia pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE, şi în cele naţionale: Constituţia Republicii Moldova, Legea nr.133/2011 privind protecţia datelor cu caracter personal, Legea nr.982/2000 privind accesul la informaţie, Hotărîrea Guvernului nr.1123/2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, Hotărîrea Guvernului nr.296/2012 privind aprobarea Regulamentului Registrului de evidenţă a operatorilor de date cu caracter personal, precum şi în alte acte normative de profil.

II. NOŢIUNI GENERALE

4. În prezenta Politică de securitate sînt utilizate următoarele noţiuni:

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

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

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

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

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

control de securitate – acţiuni întreprinse de către Primăria orașului Nisporeni în vederea asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaţionale şi/ sau registrelor ţinute;

fişiere temporare – ansamblu de date sau informaţii pe suport digital, creat pentru o perioadă de timp limitat, pînă 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;

mijloace de protecţie criptografică a informaţiei care conţine date cu caracter personal – mijloace tehnice, de program şi tehnico-aplicative, sisteme şi complexe de sisteme ce realizează algoritmi de conversie criptografică a informaţiei care conţine date cu caracter personal, destinate să asigure integritatea şi confidenţialitatea informaţiei în procesul de prelucrare, depozitare şi transmitere a acesteia prin canalele de comunicaţii;

nivel de protecţie – nivel de securitate proporţional riscului pe care îl comportă prelucrarea faţă de datele cu caracter personal respective, precum şi faţă de drepturile şi libertăţile persoanelor, elaborat şi actualizat corespunzător nivelului dezvoltării tehnologice şi costurilor implementării acestor măsuri;

politica de securitate a datelor cu caracter personal – document, elaborat de către operatorul de date [se indică localitatea], care oferă o descriere precisă a măsurilor de securitate şi trăsăturilor de protecţie selectate pentru securitatea datelor, ţinîndu-se cont de potenţialele pericole pentru datele cu caracter personal prelucrate şi riscurile la care sînt expuse acestea;

perimetru de securitate – zonă care reprezintă o barieră de trecere propriu-zisă, asigurată cu mijloace de control fizic şi/sau tehnic al accesului;

persoană responsabilă de politica de securitate a datelor cu caracter personal – persoană 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;

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 care 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 ce conţine date cu caracter personal;

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

restaurare a datelor – proceduri ce ţin de reconstituirea/restabilirea datelor cu caracter personal în starea în care se aflau pînă la momentul pierderii sau distrugerii acestora;

tehnologie informaţională – totalitatea metodelor, procedeelor şi mijloacelor de prelucrare şi transmitere a informaţiei care conţine date cu caracter personal şi regulile de aplicare a acesteia;

utilizator – persoană 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 pînă la momentul opririi acestora;

sistem informaţional de date cu caracter personal – totalitate de resurse şi tehnologii informaţionale interdependente, de metode şi de personal, destinată păstrării, prelucrării şi furnizării de informaţie care conţine date cu caracter personal;

prelucrare a 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;

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

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;

consimţământ al subiectului datelor cu caracter personal – orice manifestare de voinţă liberă, expresă şi necondiţionată, în formă scrisă sau electronică, conform cerinţelor documentului electronic, prin care subiectul datelor cu caracter personal acceptă să fie prelucrate datele care îl privesc;

depersonalizare a datelor – modificarea datelor cu caracter personal astfel încît detaliile privind circumstanţele personale sau materiale să nu mai permită atribuirea acestora unei persoane identificate sau identificabile ori să permită atribuirea doar în condiţiile unei investigaţii care necesită cheltuieli disproporţionate de timp, mijloace şi forţă de muncă.

III. OBIECTIVELE POLITICII DE SECURITATE A DATELOR CU CARACTER PERSONAL

5. Obiectivele principale ale Politicii de securitate sînt disponibilitatea, integritatea şi confidenţialitatea tuturor informaţiilor, inclusiv a datelor cu caracter personal prelucrate de [se indică localitatea], atît în cadrul prelucrării manuale, cît şi în cadrul sistemelor şi proceselor de tehnologie informaţională.

6. Securitatea reprezintă o componentă esenţială a derulării optime a proceselor bazate pe TI în cadrul Primăriei orașului Nisporen. Baza unei securităţi TI adecvate o constituie respectarea prezentei Politici de securitate. Aceasta cuprinde cerinţe şi reguli pentru protecţia tuturor informaţiilor, inclusiv a datelor cu caracter personal, a sistemelor şi proceselor TI împotriva influenţelor naturale, erorilor umane şi tehnice, precum şi împotriva acţiunilor deliberate care pot provoca pagube materiale, respectiv imateriale, sau care pot duce la încălcări ale legislaţiei.

7. Avînd în vedere că siguranţa TI nu poate fi garantată exclusiv cu ajutorul unor sisteme tehnice, prezenta Politică de securitate vizează, de asemenea, aspecte de ordin organizatorico-juridic şi de altă natură.

8 Primăria orașului Nisporeni va proteja datele cu caracter personal atît ale participanţilor la proces/ vizitatorilor, cît şi ale angajaţilor săi.

9. Reglementările prezentei Politici de securitate reprezintă un standard minim pentru Primăria orașului Nisporeni, inclusiv pentru toţi angajaţii Primăriei orașului Nisporeni, care vor respecta strict prevederile prezentei Politici de securitate şi regulile interne privind protecţia datelor cu caracter personal şi sistemelor TI.

IV. SCOPUL APLICĂRII MĂSURILOR DE PROTECŢIE A DATELOR CU CARACTER PERSONAL

10. Măsurile de protecţie a datelor cu caracter personal sînt asigurate în scopul:

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

2) preîntîmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în reţelele telecomunicaţionale şi resursele informaţionale;

3) neadmiterii dezvăluirii terţilor a informaţiei cu accesibilitate limitată;

4) eficientizării resurselor informaţionale atît pe suport de hîrtie, cît şi în format electronic.

V. METODELE DE PROTECŢIE A DATELOR CU CARACTER PERSONAL PRELUCRATE ÎN SISTEMELE INFORMAŢIONALE

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

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

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

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

4) preîntîmpinarea acţiunilor intenţionate şi/ sau neintenţionate ale utilizatorilor, precum şi ale altor membri ai operatorului/ persoanelor împuternicite de către operator, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program;

5) preîntîmpinarea scurgerii de informaţii care conţin date cu caracter personal, transmise prin canalele de legătură, care este asigurată prin folosirea metodelor de cifrare a acestei informaţii, precum şi utilizarea canalelor VPN;

6) preîntîmpinarea distrugerii, modificării datelor cu caracter personal sau defecţiunilor în funcţionarea softului destinat prelucrării datelor cu caracter personal, care 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 softului şi prin efectuarea periodice a copiilor de siguranţă;

7) preîntîmpinarea scurgerii de informaţii care conţin date cu caracter personal, asigurată prin auditul intern al sistemelor informaţionale, care se efectuează permanent;

8) stabilirea exactă a ordinii de acces la informaţia care conţine date cu caracter personal, prelucrate în cadrul sistemelor informaţionale şi de evidenţă instituite atît pentru utilizatorii interni, cît şi pentru cei externi.

VI. RESURSELE INFORMAŢIONALE SUPUSE PRINCIPIILOR DE PROTECŢIE A DATELOR CU CARACTER PERSONAL

12. Protecţia datelor cu caracter personal în cadrul Primăriei orașului Nisporeni în calitate de operator de date cu caracter personal este asigurată printr-un complex de măsuri tehnice şi organizatorice de preîntîmpinare a prelucrării ilicite a datelor cu caracter personal.

13. Se supun protecţiei prin mijloace/ procedee specifice toate resursele informaţionale ale operatorului de date cu caracter personal gestionate, care conţin date cu caracter personal, păstrate pe:

1) suporturi magnetice, optice, laser sau alte suporturi ale informaţiei electronice şi baze de date;

2) sisteme informaţionale, reţele, sisteme operaţionale, sisteme de date şi alte aplicaţii, sisteme de telecomunicaţii, inclusiv de multiplicare a documentelor, şi alte mijloace tehnice de prelucrare a informaţiei.

VII. DISPOZIŢII PRIVIND IERARHIA ŞI OBLIGAŢIILE PERSOANEI RESPONSABILE DE POLITICA DE SECURITATE A DATELOR CU CARACTER PERSONAL

14. Avînd în vedere specificul activităţii, operatorul de date cu caracter personal, prin prezenta Politică de securitate, transpune procedurile şi măsurile necesare în vederea asigurării nivelului adecvat de protecţie la prelucrarea datelor cu caracter personal în cadrul sistemelor de evidenţă gestionate.

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

16. Politica de securitate, în mod obligatoriu, va fi adusă la cunoştinţă, contra semnătură, tuturor angajaţilor responsabili de prelucrarea datelor cu caracter personal, înaintea acordării accesului la prelucrarea datelor cu caracter personal, inclusiv la operarea modificărilor odată cu necesitatea asigurării nivelului adecvat de protecţie a datelor cu caracter personal.

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

18. În cadrul monitorizării implementării/ respectării prevederilor Politicii de securitate, persoana responsabilă desemnată, indiferent de funcţiile exercitate, se va subordona nemijlocit conducătorului Primăriei orașului Nisporeni sau persoanei care îndeplineşte interimatul funcţiei.

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

20. Persoana responsabilă de politica de securitate a datelor cu caracter personal întreprinde următoarele acţiuni:

1) defineşte clar responsabilităţile şi procesele de management al securităţii datelor cu caracter personal, cu integrarea lor corespunzătoare în structura organizaţională şi de funcţionare generală;

2) asigură măsuri tehnice şi organizaţionale necesare organizării procesului de management al securităţii datelor cu caracter personal;

3) elaborează procedurile de clasificare a informaţiei care conţine date cu caracter personal, astfel încît să fie posibile întocmirea unui nomenclator şi localizarea tuturor datelor cu caracter personal care sînt prelucrate, indiferent de tipul purtătorului de date;

4) instruieşte persoanele implicate în procesul de prelucrare a datelor cu caracter personal în vederea îndeplinirii de către acestea a atribuţiilor funcţionale şi asumării responsabilităţilor de securitate a datelor cu caracter personal, inclusiv asupra confidenţialităţii acestora.

VIII. PROCEDURILE ORGANIZATORICE ŞI TEHNICE LA PRELUCRAREA DATELOR CU CARACTER PERSONAL

Secţiunea 1
Măsurile generale de administrare a securităţii informaţionale

21. Măsurile generale de administrare a securităţii informaţionale sînt următoarele:

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

2) computerele, terminalele de acces şi imprimantele sînt deconectate la terminarea sesiunilor de lucru;

3) este asigurată securitatea punctelor de primire/ expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele fax şi de copiere;

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

5) mijloacele de prelucrare a datelor cu caracter personal, informaţia care conţine date cu caracter personal sau softurile destinate prelucrării datelor cu caracter personal sînt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a conducerii;

6) toate programele utilizate în cadrul sistemului informatic respectă condiţiile de licenţiere;

7) este interzisă instalarea programelor de tip Shareware sau freeware fără aprobarea administratorului sistemului informatic.

Secţiunea a 2-a
Securitatea mediului fizic şi a tehnologiilor informaţionale folosite în procesul prelucrării datelor cu caracter personal

22. Accesul în sediile/ oficiile/ birourile ori spaţiile unde sînt amplasate sistemele informaţionale de date cu caracter personal este restricţionat, fiind permis doar persoanelor care au permisiunea necesară, conform listei sau însemnelor corespunzătoare (insigne, ecusoane, cartele de identificare).

23. Se asigură administrarea şi monitorizarea accesului fizic în toate punctele de acces la sistemele informaţionale de date cu caracter personal, inclusiv se reacţionează la încălcarea regimului de acces.

24. Perimetrul de securitate al Primăriei orașului Nisporeni, reprezintă perimetrul oficiilor în care se prelucrează/ stochează date cu caracter personal.

25. Perimetrul clădirii sau încăperilor în care sînt amplasate mijloacele de prelucrare a datelor cu caracter personal este integru din punct de vedere fizic, pereţii exteriori ai încăperilor sînt rezistenţi, intrările sînt echipate cu lacăte şi semnalizare.

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

27. În cazul în care în încăpere lipsesc persoanele desemnate, uşile şi ferestrele se încuie.

28. Computerele, serverele, alte terminale de acces sînt amplasate în locuri cu acces limitat pentru persoane străine.

29. Accesul în perimetrul de securitate al clădirii Primăriei orașului Nisporeni unde se prelucrează/ stochează date cu caracter personal cu utilaje foto/ video neautorizate este interzis, ţinînd cont de necesitatea asigurării regimului de confidenţialitate şi securitate a prelucrării datelor cu caracter personal, prevăzut la art.29 şi 30 din Legea nr.133/2011 privind protecţia datelor cu caracter personal, precum şi la pct.26 din 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.1123/2010.

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

Secţiunea a 3-a
Identificarea şi autentificarea utilizatorilor şi echipamentului. Administrarea identificatorilor utilizatorilor

31. Se efectuează identificarea şi autentificarea utilizatorilor sistemelor informaţionale de date cu caracter personal şi a proceselor executate în numele acestor utilizatori.

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

33. Pentru confirmarea ID-ului utilizatorului pot fi folosite: parole, mijloace fizice speciale de acces cu memorie (token), cartele cu microprocesoare, mijloace biometrice de autentificare bazate pe caracteristici unice şi individuale ale persoanei.

34. Codurile de identificare şi autentificare se revocă sau se suspendă de administratorul TI în cazul în care contractul de muncă/ raporturile de serviciu ale utilizatorului au fost încetate, suspendate sau modificate şi noile sarcini nu necesită accesul la date cu caracter personal ori drepturile de acces ale utilizatorului au fost modificate, ori utilizatorul a abuzat de codurile primite în scopul comiterii unei fapte prejudiciabile sau culpe, ori a absentat o perioadă îndelungată.

35. Administrarea identificatorilor utilizatorilor include:

1) identificarea univocă a fiecărui utilizator;

2) verificarea autenticităţii fiecărui utilizator.

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

Secţiunea a 4-a
Utilizarea parolelor în procesul asigurării securităţii informaţionale. Controlul administrării accesului

37. La utilizarea parolelor se respectă regulile de asigurare a securităţii informaţionale care prevăd:

1) păstrarea confidenţialităţii parolelor;

2) interzicerea înscrierii parolelor pe suport de hîrtie, în cazul în care nu se asigură securitatea păstrării acestuia;

3) modificarea parolelor de fiecare dată cînd sînt prezente indiciile eventualei compromiteri a sistemului sau parolei;

4) alegerea parolelor sigure, cu o mărime de minimum 8 simboluri, care nu sînt legate de informaţia cu caracter personal a utilizatorului, nu conţin simboluri identice consecutive şi nu sînt compuse integral din grupuri de cifre sau litere;

5) modificarea parolelor peste intervale de 3 luni;

6) dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate).

38. Controlul sistematic al acţiunilor utilizatorilor se efectuează în vederea evaluării corectitudinii şi conformării operaţiunilor şi acţiunilor efectuate prin intermediul sistemelor informaţionale de date cu caracter personal.

Secţiunea a 5-a
Accesul de la distanţă. Limitarea folosirii tehnologiilor fără fir

39. Toate metodele de acces de la distanţă la sistemele informaţionale de date cu caracter personal sînt securizate (utilizîndu-se VPN, criptarea, cifrarea etc.), precum şi sînt documentate, supuse monitorizării şi controlului.

40. Fiecare metodă de acces de la distanţă la sistemele informaţionale de date cu caracter personal este permisă de persoanele responsabile din cadrul Primăriei orașului Nisporeni doar utilizatorilor cărora aceasta le este necesară pentru îndeplinirea obiectivelor stabilite.

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

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

43. Folosirea tehnologiilor fără fir se permite de persoanele responsabile din cadrul [se indică localitatea].

Secţiunea a 6-a
Securitatea electroenergetică. Controlul instalării şi scoaterii componentelor TI

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

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

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

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

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

Secţiunea a 7-a
Dezvăluirea datelor cu caracter personal

49. La dezvăluirea datelor cu caracter personal conţinute în sistemele de evidenţă, prin reţele comunicaţionale ori pe alt suport digital de stocare şi păstrare, urmează a fi asigurată criptarea acestei informaţii sau examinarea posibilităţii utilizării unei conexiuni bilaterale prin canal securizat VPN.

50. Accesul fără fir la sistemele de evidenţă a datelor cu caracter personal este permis doar utilizatorilor autorizaţi. Fiecare caz de solicitare a dezvăluirii prin transmitere a datelor cu caracter personal pe cale electronică va fi examinat separat, ţinînd cont de posibilităţile tehnice asigurate de destinatar şi operator, precum şi în corespundere cu măsurile organizatorice şi tehnice implementate de părţi.

51. În cazul în care reţelele comunicaţionale prezintă riscuri pentru confidenţialitatea şi securitatea datelor cu caracter personal, vor fi utilizate metode tradiţionale de transmitere (expediere poştală cu aviz recomandat, înmînare personală etc.).

52. Este interzisă dezvăluirea prin transmitere a datelor cu caracter personal prin reţele comunicaţionale ce nu corespund cerinţelor (spre exemplu expedierea informaţiei prin intermediul e-mailurilor personale de tipul @gmail.com, @mail.ru, @yahoo.com etc.). O astfel de diseminare este posibilă în urma indicării de către deponent/ solicitant a adresei electronice în depunere/ solicitare/ cerere.

53. Sînt interzise operaţiunile de dezvăluire a datelor cu caracter personal între Primăria oraşului Nisporeni şi alte entităţi care sînt amplasate geografic în stînga Nistrului (regiunea transnistreană) şi care refuză să se supună juridic legislaţiei Republicii Moldova, avînd în vedere că în prezent nu există posibilitatea exercitării unui control efectiv asupra acestei părţi teritoriale, inclusiv în partea ce ţine de conformitatea prelucrării datelor cu caracter personal prevederilor Legii nr.133/2011 privind protecţia datelor cu caracter personal.

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

55. Transmiterea transfrontalieră a datelor cu caracter personal este efectuată în strictă corespundere cu prevederile art.32 din Legea nr.133/2011 privind protecţia datelor cu caracter personal, în special în cazurile cînd tratatul internaţional în baza căruia se efectuează transmiterea nu conţine garanţii privind protecţia drepturilor subiectului de date cu caracter personal.

56. Volumul şi categoriile datelor cu caracter personal colectate în scopul ţinerii evidenţei activităţilor Primăriei oraşului Nisporeni sînt limitate la strictul necesar pentru realizarea scopurilor declarate.

57. Acces la datele cu caracter personal din sistemele informaţionale gestionate în cadrul Primăriei oraşului Nisporeni din partea organelor de drept sau altor persoane se va permite doar în cazurile şi condiţiile prevăzute le legislaţia în vigoare.

În conformitate cu prevederile art.157 din Codul de procedură penală al Republicii Moldova nr.122/2003, documentele în orice formă (scrisă, audio, video, electronică etc.) care provin de la persoane oficiale fizice sau juridice, dacă în ele sînt expuse ori adeverite circumstanţe care au importanţă pentru cauză (inclusiv informaţia stocată în auditul sistemelor informaţionale şi de evidenţă), pot fi solicitate printr-un demers al organului de urmărire penală

în cadrul urmăririi penale sau în procesul judecării cauzei. În acest caz, însă, urmează a fi respectate prevederile art.214 din Codul de procedură penală al Republicii Moldova nr.122/2003, care stipulează că în cursul procesului penal nu poate fi administrată, utilizată şi răspîndită fără necesitate informaţie oficială cu accesibilitate limitată. Persoanele cărora organul de urmărire penală sau instanţa le solicită să comunice sau să prezinte informaţie oficială cu accesibilitate limitată (inclusiv operatorii de date cu caracter personal) au dreptul să se convingă de faptul că aceste date se colectează pentru procesul penal respectiv, iar în caz contrar să refuze de a comunica sau de a prezenta date. Persoanele cărora organul de urmărire penală sau instanţa le solicită să comunice sau să prezinte informaţie oficială cu accesibilitate limitată au dreptul să primească în prealabil de la persoana care solicită informaţii o explicaţie în scris care ar confirma necesitatea furnizării datelor menţionate.

Urmează a se lua act de faptul că, în conformitate cu prevederile art.8 din Legea nr.982/2000 privind accesul la informaţie, datele cu caracter personal fac parte din categoria informaţiei oficiale cu accesibilitate limitată, accesul la aceasta realizîndu-se în conformitate cu prevederile legislaţiei privind protecţia datelor cu caracter personal.

58. În cazul în care avocatul sau persoana împuternicită solicită să ia cunoştinţă de fişa personală a clientului, acesta urmează a fi informat în scris despre obligaţiile ce îi revin în conformitate cu prevederile art.15 din Codul de procedură penală al Republicii Moldova nr.122/2003 şi art.29 şi 30 din Legea nr.133/2011 privind protecţia datelor cu caracter personal, inclusiv despre răspunderea prevăzută la art.74[1] din Codul contravenţional al Republicii Moldova nr.218/2008.

Secţiunea a 8-a
Drepturile subiecţilor de date cu caracter personal

59. În cazul în care datele cu caracter personal sînt colectate direct de la subiectul acestor date, în conformitate cu prevederile art.12 din Legea nr.133/2011 privind protecţia datelor cu caracter personal, acestuia i se furnizează următoarele informaţii, exceptînd cazul în care subiectul deţine deja informaţiile respective:

1) identitatea operatorului sau, după caz, a persoanei împuternicite de către operator (denumirea, adresa juridică, IDNO-ul, numărul de înregistrare în Registrul de evidenţă a operatorilor de date cu caracter personal);

2) scopul concret al prelucrării datelor cu caracter personal colectate;

3) destinatarii sau categoriile de destinatari ai datelor cu caracter personal;

4) dreptul la informare şi de acces la datele colectate, de intervenţie asupra datelor (în special de a rectifica, actualiza, bloca sau şterge datele cu caracter personal a căror prelucrare contravine legii din cauza caracterului incomplet sau inexact al acestora) şi de opoziţie, precum şi condiţiile în care aceste drepturi pot fi exercitate; dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sînt obligatorii sau voluntare, inclusiv consecinţele posibile ale refuzului de a răspunde la întrebările prin care se colectează informaţia;

5) dreptul de acces şi posibilitatea de a lua cunoştinţă de actele întocmite în scopul verificării corectitudinii întocmirii lor, contestării împotriva neincluderii sau includerii incorecte a unor date, precum şi împotriva altor erori comise la înscrierea datelor.

60. Persoanele responsabile de prelucrarea datelor cu caracter personal vor asigura accesul persoanei doar la datele cu caracter personal care o vizează nemijlocit, fiind exclusă posibilitatea consultării datelor cu caracter personal ce vizează alţi subiecţi, conţinute în fişele personale (alte materiale), cu excepţia cazurilor în care solicitanţii îşi realizează un interes legitim care nu prejudiciază interesele sau drepturile şi libertăţile fundamentale ale subiectului datelor cu caracter personal.

61. Dreptul de informare este asigurat de către operatorul datelor cu caracter personal (sau entităţile ce asigură mentenanţa sistemului şi/ sau prestează servicii externalizate ale operatorului) tuturor persoanelor supuse prelucrării.

62. În cazul realizării de către subiectul de date cu caracter personal a dreptului de intervenţie, datele inexacte vor fi actualizate prin rectificare sau ştergere, ca bază servind doar surse legale (acte de identitate, de stare civilă, resurse informaţionale principale de stat etc.), modificarea urmînd a fi efectuată în toate sistemele informaţionale şi de evidenţă gestionate.

Secţiunea a 9-a
Stocarea, păstrarea şi distrugerea datelor cu caracter personal prelucrate

63. Accesul în spaţiile/ perimetrul unde sînt amplasate sistemele informaţionale şi de evidenţă a datelor cu caracter personal este restricţionat, fiind permis doar persoanelor care au permisiunea necesară conform politicii de securitate instituţionale/ regulamentelor departamentale aprobate.

64. Sînt interzise stocarea şi păstrarea formatului electronic al datelor cu caracter personal, structurate în sisteme de evidenţă, în computere care sînt conectate la internet, nu sînt echipate cu mijloace de protecţie speciale tehnice şi de program şi nu au instalate programe licenţiate, programe antivirus, sisteme de control al securităţii softului, de asigurare a efectuării periodice a copiilor de siguranţă şi de efectuare a auditului.

65. Introducerea în perimetrul de securitate instituţional şi utilizarea calculatoarelor personale ori a purtătorilor de informaţii în scopuri de serviciu este interzisă.

66. Accesul la computerele din dotare sînt protejate/ restricţionate prin crearea profilurilor de utilizatori, iar drepturile de administrator sînt încredinţate doar persoanei responsabile desemnate pentru implementarea Politicii de securitate din cadrul Primăriei orașului Nisporeni

67. Stocarea datelor cu caracter personal pe suport magnetic, optic, laser, de hîrtie sau alt suport al informaţiei, pe care se creează, se fixează, se transmite, se recepţionează, se păstrează sau, în alt mod, se utilizează documentul şi care permite reproducerea acestuia este asigurată prin plasarea acestora în seifuri sau dulapuri metalice care se încuie.

68. Scoaterea fără autorizare a purtătorilor de date cu caracter personal din perimetrul de securitate al operatorului este interzisă.

Secţiunea a 10-a
Auditul sistemelor informaţionale gestionate

69. Înregistrarea tentativelor de intrare/ ieşire a utilizatorului în/ din sistem se efectuează conform următorilor parametri:

1) data şi timpul tentativei intrării/ ieşirii;

2) ID-ul utilizatorului;

3) rezultatul tentativei de intrare/ ieşire – pozitiv sau negativ.

70. Înregistrarea tentativelor de obţinere a accesului (de executare a operaţiunilor) pentru aplicaţii şi procese destinate prelucrării datelor cu caracter personal se efectuează conform următorilor parametri:

1) data şi timpul tentativei de obţinere a accesului (de executare a operaţiunii);

2) denumirea (identificatorul) aplicaţiei sau procesului ori ID-ul utilizatorului;

3) specificaţiile resursei protejate (identificator, nume logic, nume fişier, număr etc.);

4) tipul operaţiunii solicitate (citire, înregistrare, ştergere etc.);

5) rezultatul tentativei de obţinere a accesului (de executare a operaţiunii) – pozitiv sau negativ.

71. Înregistrarea modificărilor drepturilor de acces (competenţelor) ale utilizatorului şi statutului obiectelor de acces se efectuează conform următorilor parametri:

1) data şi timpul modificării competenţelor;

2) ID-ul administratorului care a efectuat modificările;

3) ID-ul utilizatorului şi competenţele acestuia sau specificarea obiectelor de acces şi statutul nou al acestora.

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

1) data şi timpul eliberării;

2) denumirea informaţiei şi căile de acces la aceasta;

3) specificarea echipamentului (dispozitivului) care a eliberat informaţia (nume logic);

4) ID-ul utilizatorului care a solicitat informaţia.

Secţiunea a 11-a
Asigurarea protecţiei contra programelor dăunătoare (virusilor). Testarea posibilităţilor funcţionale de asigurare a securităţii sistemelor informaţionale de date cu caracter personal

73. Protecţia contra infiltrării programelor dăunătoare în softurile destinate prelucrării datelor cu caracter personal este asigurată prin existenţa programelor licenţiate antivirus.

74. 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).

Secţiunea a 12-a
Gestionarea incidentelor de securitate

75. Personalul/ angajaţii Primăriei oraşului Nisporeni care asigură exploatarea sistemelor informaţionale de date cu caracter personal trec(e), minimum o dată în an, instruirea privind responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate.

76. Personalul/ angajaţii Primăriei oraşului Nisporeni informează neîntîrziat conducerea despre incidentele care încalcă securitatea sistemelor informaţionale de date cu caracter personal.

77. Prelucrarea incidentelor include: depistarea, analiza, preîntîmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii.

78. Anual, pînă la data de 31 ianuarie, operatorul de date cu caracter personal informează în scris Centrul Naţional pentru Protecţia Datelor cu Caracter Personal despre incidentele de securitate constatate.

79. În cazul producerii incidentelor de securitate în cadrul Primăriei oraşului Nisporeni persoana responsabilă din cadrul Primăriei oraşului Nisporeni va întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia şi va înlătura cauzele incidentului de securitate, cu informarea Centrului Naţional pentru Protecţia Datelor cu Caracter Personal în termen de 72 de ore de la momentul producerii incidentului de securitate.

80. În cadrul controalelor efectuate, Centrului Naţional pentru Protecţia Datelor cu Caracter Personal i se va acorda sprijinul necesar şi i se va asigura accesul la informaţiile necesare relevante obiectului controlului.

Secţiunea a 13-a
Marcarea documentelor. Responsabilitatea pentru asigurarea securităţii datelor cu caracter personal şi a informaţiilor cu accesibilitate limitată

81. Toată informaţia care se intenţionează a fi dezvăluită şi care conţine date cu caracter personal urmează a fi marcată prin includerea numărului de înregistrare din Registrul de evidenţă a operatorilor de date cu caracter personal.

Model: „Atenţie! Documentul conţine date cu caracter personal, prelucrate în cadrul sistemului de evidenţă nr.0000YYY-00X, înregistrat în Registrul de evidenţă a operatorilor de date cu caracter personal www.registru.datepersonale.md. Prelucrarea ulterioară a acestor date poate fi efectuată numai în condiţiile prevăzute de Legea nr.133/2011 privind protecţia datelor cu caracter personal”.

82. Pentru nerespectarea dispoziţiilor Politicii de securitate, operatorul de date cu caracter personal, persoana împuternicită de către operator, persoanele terţe, după caz, poartă răspundere civilă (Codul civil al Republicii Moldova nr.1107/2002), contravenţională (art.74[1] din Codul contravenţional al Republicii Moldova nr.218/2008) şi penală (art.177, 178, 180 din Codul penal al Republicii Moldova nr.985/2002).