MINISTERUL SĂNĂTĂȚII, MUNCII ȘI PROTECȚIEI SOCIALE AL REPUBLICII MOLDOVA
AGENȚIA NAȚIONALĂ PENTRU SĂNĂTATE PUBLICĂ

MD 2028, mun. Chișinău, str. Gh. Asachi 67A, Tel. +373 22 574 501;Fax. +373 22 729 725,
http://www.ansp.md; e-mail:office@ansp.md IDNO:1018601000021

ORDIN

Nr. 415 din „ 16 „ august 2019

Cu privire la aprobarea Politicii de securitate și protecție a datelor cu caracter personal a Agenției Naționale pentru Sănătate Publică

În temeiul Legii nr.133 din 08.07.2011 privind protecția datelor cu caracter personal (Monitorul Oficial, 2011, nr. 170-175, art. 492) și 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 (Monitorul oficial, 2010, nr. 254-256, art. 1282) ,

ORDON:

1. Se aprobă Politica de securitate și protecție a datelor cu caracter personal a Agenției Naționale pentru Sănătate Publică (ANSP) conform anexei.
2. Șefii de Direcții și Centrelor de Sănătate Publică teritoriale:
   2.1 pînă la data de 10.09.2019, vor elabora și înainta spre aprobare Regulamente cu privire la protecția și securitatea datelor cu caracter personal, la prelucrarea lor în Direcții, secții, ghișeu unic și sisteme informaționale;
   2.2 vor propune persoane responsabile de protecția și securitatea datelor cu caracter personal.
3. Controlul realizării prezentului ordin mi-l asum.

Director interimar Nicolae FURTUNĂ

Anexa nr.1
la Ordinul intern al ANSP nr. 415
din „ 16 „ august 2019

POLITICA DE SECURITATE ȘI DE PROTECȚIE A DATELOR CU CARACTER PERSONAL ÎN CADRUL AGENȚIEI NAȚIONALE PENTRU SĂNĂTATE PUBLICĂ

I. PREAMBUL

La prelucrarea datelor cu caracter personal în cadrul Agenției Naționale pentru Sănătate Publică sunt aplicate principiile prevăzute de actele **internaționale** - Declarația universală a drepturilor omului, Convenția pentru apărarea drepturilor omului și a libertăților fundamentale, Convenția pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, Directiva 95/46/CE a Parlamentului European și a Consiliului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, și a celor **naționale** – Constituția Republicii Moldova, Legea privind protecția datelor cu caracter personal, Legea privind accesul la informație, Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr. 1123 din 14 decembrie 2010, Regulamentului Registrului de evidență al operatorilor de date cu caracter personal, aprobat prin Hotărârea Guvernului nr. 296 din 15 mai 2012 și alte acte legislative/normative de profil.

CUPRINS:

I. PREAMBUL

La prelucrarea datelor cu caracter personal în cadrul Agenției Naționale pentru Sănătate Publică sunt aplicate principiile prevăzute de actele **internaționale** - Declarația universală a drepturilor omului, Convenția pentru apărarea drepturilor omului și a libertăților fundamentale, Convenția pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, Directiva 95/46/CE a Parlamentului European și a Consiliului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, și a celor **naționale** – Constituția Republicii Moldova, Legea privind protecția datelor cu caracter personal, Legea privind accesul la informație, Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr. 1123 din 14 decembrie 2010, Regulamentului Registrului de evidență al operatorilor de date cu caracter personal, aprobat prin Hotărârea Guvernului nr. 296 din 15 mai 2012 și alte acte legislative/normative de profil.

II. INTRODUCERE

Agenția Națională pentru Sănătate Publică, (în continuare Agenția) este persoană juridică de drept public și are misiunea de a asigura implementarea politicii statului în domeniile de competență, în modul stabilit și în limitele atribuite de cadrul normativ.

Principalele domenii de competență ale Agenției sunt:

1) Supravegherea de stat, promovarea și protecția sănătății publice;
2) Controlul de stat (inspecția) în sănătate;
3) Monitorizarea și evaluarea stării de sănătate a populației;
4) Acreditarea activității instruiților medico-sanitare și farmaceutice;
5) Siguranța ocupațională.

Agenția este autoritate administrativă în subordinea Ministerului Sănătății, Muncii și Protecției Sociale și are următoarea adresă juridică: str. Gh. Asachi, 67A, mun. Chișinău Republica Moldova.

Agenția include în sine zece Centre de sănătate publică, care sunt subdiviziuni teritoriale ale Agenției, fără personalitate juridică. Centrele de Sănătate Publică teritoriale asigură coordonarea activităților la nivelul teritoriului deservit conform atribuțiilor stabilite în art. 17 din Legea nr.10-XVI din 3 februarie 2009 privind supravegherea de stat a sănătății publice și regulamentelor aprobate de directorul agenției.

Prezenta Politică este aprobată, inclusiv, în vederea conformării cu prevederile Hotărârii Guvernului Republicii Moldova nr.1123 din data de 14 decembrie 2010 "privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal" și Legii Republicii Moldova nr.133 din 08.07.2011 "privind protecția datelor cu caracter personal".

III. NOȚIUNI GENERALE

În prezenta Politică de Securitate, sunt definite/utilizate următoarele noțiuni:

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 - 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;

operator - persoana fizică sau persoana juridică de drept public sau de drept privat, inclusiv autoritatea publică, orice altă instituție ori organizație care, în mod individual sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal prevăzute în mod expres de legislația în vigoare;

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

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

control de securitate - acțiuni întreprinse de către Instituție în vederea asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaționale și/sau registrelor ținute;

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

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

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

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

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

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

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

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

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

purtător de date cu caracter personal - suport magnetic, optic, laser, de 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/prestabilirea datelor cu caracter personal în starea în care se aflau până la momentul pierderii sau distrugerii acestora;

tehnologie informațională - totalitatea metodelor, procedeelor și mijloacelor de prelucrare și transmitere a informației care conține date cu caracter personal și regulile de aplicare a acesteia;

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

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

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

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

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

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

consimțământul subiectului datelor cu caracter personal - orice manifestare de voință liberă, expresă și necondiționată, în formă scrisă sau electronică, conform cerințelor documentului electronic, prin care subiectul datelor cu caracter personal acceptă să fie prelucrate datele care îl privesc;

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

IV. OBIECTIVILE POLITICII DE SECURITATE

Obiectivele principale ale Politicii sunt disponibilitatea, integritatea și confidențialitatea tuturor informațiilor, inclusiv datelor cu caracter personal prelucrate de Instituție, atât în cadrul prelucrării manuale, cât și sistemelor și proceselor de tehnologie informațională. Securitatea reprezintă o componentă esențială a derulării optime a proceselor bazate pe IT în cadrul Agenției.

Baza unei securități IT adecvate o constituie respectarea prezentei Politici. Aceasta cuprinde cerințe și reguli pentru protecția tuturor informațiilor, inclusiv datele cu caracter personal, sistemelor și proceselor IT împotriva influențelor naturale, erorilor umane și tehnice, precum și împotriva acțiunilor deliberate care pot provoca pagube materiale, respectiv imateriale, sau care pot duce la încălcări ale legislației. Având în vedere că siguranța IT nu poate fi garantată exclusiv cu ajutorul unor sisteme tehnice, prezenta Politică vizează, de asemenea, aspecte de ordin organizatoric-juridic și de altă natură.

Agenția va proteja datele cu caracter personal atât a participanților la proces/vizitatori, cât și a angajaților săi.

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

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

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

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

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

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

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

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

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

VI. MIJLOACELE SUPUSE PRINCIPIILOR DE PROTECȚIE A DATELOR CU CARACTER PERSONAL

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

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

- suporturi magnetice, optice, laser sau alte suporturi ale informației electronice, masive informaționale și baze de date;
- sistemele informaționale, rețelele, sistemele operaționale, sistemele de gestionare a bazelor de date și alte aplicații, sistemele de telecomunicații, inclusiv mijloacele de confecționare și multiplicare a documentelor și alte mijloace tehnice de prelucrare a informației.

VII. SCOPUL IMPLEMENTĂRII MĂSURILOR DE PROTECȚIE A DATELOR CU CARACTER PERSONAL

Măsurile de protecția datelor cu caracter personal sunt asigurate în scopul:

- preîntâmpinării scurgerii informației care conține date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;
- preîntâmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în rețelele telecomunicaționale și resursele informaționale;
- neadmiterii dezvăluirii terților a informației cu accesibilitate limitată;
- eficientizării resurselor informaționale atât pe suport de hârtie cât și cel în format electronic.

VIII. METODELE DE PROTECȚIE A DATELOR CU CARACTER PERSONAL PRELUCRATE ÎN SISTEMELE INFORMAȚIONALE

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

- preîntâmpinarea conexiunilor neautorizate la rețelele telecomunicaționale și interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste rețele;
- excluderea accesului neautorizat la datele cu caracter personal prelucrate;
- preîntâmpinarea acțiunilor speciale tehnice și de program, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program;
- preîntâmpinarea acțiunilor intenționate și/sau neintenționate a utilizatorilor interni și/sau externi, precum și a altor membri ai operatorului/persoanelor împuternicite de către operator, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program;
- preîntâmpinarea scurgerii de informații care conțin date cu caracter personal, transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informații, precum și utilizarea canalelor VPN;
- preîntâmpinarea distrugerii, modificării datelor cu caracter personal sau defecțiunilor în funcționarea soft-ului destinat prelucrării datelor cu caracter personal este asigurată prin metoda folosirii mijloacelor de protecție speciale tehnice și de program, inclusiv a programelor licențiate, programelor antivirus, organizării sistemului de control al securității soft-ului și efectuarea periodică a copiilor de siguranță;
- preîntâmpinarea scurgerii de informații care conțin date cu caracter personal, este asigurată prin auditul intern al sistemelor informaționale, care se efectuează permanent;

- stabilirea exactă a ordinii de acces la informația care conține date cu caracter personal, prelucrate în cadrul sistemelor informaționale și de evidență instituite atât pentru utilizatorii interni cât și pentru cei externi.

IX. PROCEDURILE ORGANIZATORICE ȘI TEHNICE CARE URMEAZĂ A FI RESPECTATE ÎN CADRUL INSTITUȚIEI LA PRELUCRAREA DATELOR CU CARACTER PERSONAL

1. Măsurile generale de administrare a securității informaționale

a) În cazul neutilizării temporare a purtătorilor de informație pe suport de hârtie sau electronici (digitali) care conțin date cu caracter personal, aceștia se păstrează în safeuri sau dulapuri metalice care se încuie;

b) Computerele, terminalele de acces și imprimantele sânt deconectate la terminarea sesiunilor de lucru;

c) Este asigurată securitatea punctelor de primire/expediere a corespondenței, precum și securitatea contra accesului neautorizat la aparatele fax și de copiere;

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

e) Mijloacele de prelucrare a datelor cu caracter personal, informația care conține date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal sunt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a conducerii;

f) Toate programele utilizate în cadrul sistemului informatic respectă condițiile de licențiere;

g) Este interzisă instalarea programelor de tip Hardware sau freeware, fără aprobarea administratorului sistemului informatic.

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

a) Accesul în sediile/oficiile/birourile ori spațiile unde sunt amplasate sistemele informaționale de date cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară, conform listei sau însemnelor corespunzătoare (insigne, ecusoane, cartele de identificare);

b) Se asigură administrarea și monitorizarea accesului fizic în toate punctele de acces la sistemele informaționale de date cu caracter personal, inclusiv se reacționează la încălcarea regimului de acces;

c) Perimetrul de securitate a Instituției reprezintă perimetru oficiilor în care se prelucrează/stochează date cu caracter personal;

d) Perimetrul clădirii sau încăperilor în care sunt amplasate mijloacele de prelucrare a datelor cu caracter personal este integru din punct de vedere fizic, pereții exteriori ai încăperilor sunt rezistenți, intrările sunt echipate cu lacăte și semnalizare;

e) Amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespund necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri;

f) Ușile și ferestrele se încuie în cazul în care în încăpere lipsesc membrii;

g) Computerele, serverele, alte terminale de acces sunt amplasate în locuri cu acces limitat pentru persoane străine;

h) Accesul în perimetrul de securitate a clădirii Instituție unde se prelucrează/stochează date cu caracter personal cu utilaje foto/video neautorizate este interzis, ținând cont de necesitatea asigurării regimului de confidențialitate și securitate a prelucrării datelor cu caracter personal, prevăzut de art. 29 și art. 30 ale Legii privind protecția datelor cu caracter personal, precum și pct. 26 din Cernițe;

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

3. Identificarea și autentificarea utilizatorilor

a) Este efectuată identificarea și autentificarea utilizatorilor sistemelor informaționale de date cu caracter personal și a proceselor executate în numele acestor utilizatori;

b) Toți utilizatorii (inclusiv personalul care asigură susținerea tehnică, administratorii de rețea, programatorii și administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu conține semnalmentele nivelului de accesibilitate al utilizatorului;

c) Pentru confirmarea ID-ului utilizatorului sunt utilizate parole, mijloace fizice speciale de acces cu memorie (token) sau cartele cu microprocesoare, mijloace biometrice de autentificare, bazate pe caracteristici unice și individuale ale persoanei;

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

4. Identificarea și autentificarea echipamentului

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

5. Administrarea identificatorilor utilizatorilor:

Administrarea identificatorilor utilizatorilor include:

a) identificarea univocă a fiecărui utilizator;

b) verificarea autenticității fiecărui utilizator.

6. Utilizarea parolelor în procesul asigurării securității informaționale

Sunt respectate 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 cu o mărime de minimum 8 simboluri, 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 intervale de 3 luni;

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

7. Controlul administrării accesului

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

8. Accesul de la distanță

a) Toate metodele de acces de la distanță la sistemele informaționale de date cu caracter personal sunt securizate (utilizându-se VPN, criptarea, cifrarea etc.), precum și sunt documentate, supuse monitorizării și controlului;

b) Fiecare metodă de acces de la distanță la sistemele informaționale de date cu caracter personal este autorizată de persoanele responsabile ale Instituției și permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

9. Limitarea folosirii tehnologiilor fără fir

a) Accesul fără fir la sistemele informaționale de date cu caracter personal este limitat la maximum, este documentat, supus monitorizării și controlului;

b) Accesul fără fir la sistemele informaționale de date cu caracter personal este permis doar în cazul utilizării mijloacelor criptografice de protecție a informației;

c) Folosirea tehnologiilor fără fir se autorizează de persoanele responsabile ale Instituției.

10. Securitatea electroenergetică

a) Echipamentul electric utilizat pentru menținerea funcționalității sistemelor informaționale de date cu caracter personal, a cablurilor electrice, este asigurat contra deteriorărilor și conectărilor nesancționate, prin montarea lor în nișe speciale;

b) În cazul apariției situațiilor excepționale, de avarie sau de forță majoră, este asigurată posibilitatea deconectării electricității la sistemele informaționale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component TI;

c) Sunt implementate sisteme automatizate de depistare și semnalizare a incendiilor în birourile unde sunt amplasate sistemele informaționale de date cu caracter personal și mijloacele de prelucrare a datelor cu caracter personal.

11. Controlul instalării și scoaterii componentelor TI.

a) Este exercitat controlul și evidența instalării și scoaterii mijloacelor de program, mijloacelor tehnice și celor tehnice de program, utilizate în cadrul sistemelor informaționale de date cu caracter personal;

b) Informațiile, care conțin date cu caracter personal și care se conțin pe purtătorii de informații, se distrug fizic sau se transcriu și se nimicesc prin metode sigure, evitându-se folosirea funcțiilor standarde de nimicire.

12. Dezvăluirea datelor cu caracter personal

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

datelor cu caracter personal, vor fi utilizate metode tradiționale de transmitere *(expediere poștală cu aviz recomandat, înmânarea personală, etc.)*;

b) Dezvăluirea prin transmitere a datelor cu caracter personal prin rețele comunicaționale ce nu corespund Cerințelor, *(spre exemplu: expedierea informației prin intermediul e-mail-urilor personale de tipul @gmail.com, @mail.ru, @yahoo.com, etc.)* sunt interzise;

c) Sunt interzise operațiunile de dezvăluire a datelor cu caracter personal între Instituție și alte entități care sunt amplasate geografic în stânga Nistrului care refuză să se supună juridic legislației Republicii Moldova, reieșind din considerentul că la moment nu există posibilitatea exercitării unui control efectiv asupra acestei părți teritoriale, inclusiv în partea ce ține de conformitatea prelucrării datelor cu caracter personal prevederilor Legii privind protecția datelor cu caracter personal;

d) Procedura dezvăluirii prin transmitere a datelor cu caracter personal stocate pe suport de hârtie și/sau suport digital, peste hotarele Republicii Moldova, urmează a fi reglementată prin act normativ instituțional/acord bilateral luându-se în considerare necesitatea asigurării unui nivel adecvat de protecție a datelor cu caracter personal;

e) Transmiterea transfrontalieră a datelor cu caracter personal este efectuată în strictă corespundere cu prevederile art. 32 al Legii privind protecția datelor cu caracter personal, în special în cazurile când tratatul internațional în baza căruia se efectuează transmiterea nu conține garanții privind protecția drepturilor subiectului de date cu caracter personal;

f) Volumul și categoriile datelor cu caracter personal colectate în scopul ținerii evidenței, este limitat la strictul necesar pentru realizarea scopurilor declarate;

g) Acces la sistemele informaționale gestionate în cadrul Instituției, din partea Procuraturii Generale *(după caz procuraturile teritoriale/specializate)*, Ministerului Afacerilor Interne, Centrului Național Anticorupție etc., va fi permis doar în cazul în care solicitarea va corespunde prevederilor art. 15 și art. 212 Cod de procedură penală.

Se explică că în conformitate cu prevederile art.157 Cod de procedură penală, documentele în orice formă *(scrisă, audio, video, electronică etc.)* care provin de la persoane oficiale fizice sau juridice dacă în ele sunt expuse ori adeverite circumstanțe care au importanță pentru cauză, *(inclusiv informația stocată în auditul sistemelor informaționale și de evidență)*, pot fi solicitate printr-un demers al organului de urmărire penală în cadrul urmăririi penale sau în procesul judecării cauzei. În acest caz, însă, urmează a fi respectate prevederile art.214 Cod de procedură penală, care stipulează că în cursul procesului penal nu pot fi administrate, utilizate și răspândite fără necesitate informație oficială cu accesibilitate limitată. Persoanele cărora organul de urmărire penală sau instanța le solicită să comunice sau să prezinte informație oficială cu accesibilitate limitată *(inclusiv operatorii de date cu caracter personal)* au dreptul să se convingă de faptul că aceste date se colectează pentru procesul penal respectiv, iar în caz contrar să refuze de a comunica sau de a prezenta date. Persoanele cărora organul de urmărire penală sau instanța le solicită să comunice sau să prezinte informație oficială cu accesibilitate limitată au dreptul să primească în prealabil de la persoana care solicită informații o explicație în scris care ar confirma necesitatea furnizării datelor menționate.

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

În cazul în care, avocatul sau persoana împuternicită solicită să ia cunoștință cu fișa personală a clientului, aceștia urmează a fi informați în scris despre obligațiile ce le revin în conformitate cu prevederile art. 15 Cod de procedură penală, art. 29 și 30 ale Legii privind protecția datelor cu caracter personal, inclusiv despre răspunderea prevăzută de art. 74^1 Cod contravențional.

13. Drepturile subiecților de date cu caracter personal

a) În cazul în care datele cu caracter personal sunt colectate direct de la subiectul acestor date, în conformitate cu prevederile art.12 al Legii privind protecția datelor cu caracter personal, persoanei necesită a-i fi furnizate următoarele informații, exceptând cazul în care el deține deja informațiile respective:

- privind identitatea operatorului sau, după caz, a persoanei împuternicite de către operator *(denumirea, adresa juridică, IDNO-ul, numărul de înregistrare în Registrul de evidență al operatorilor de date cu caracter personal);*
- privind scopul concret al prelucrării datelor cu caracter personal colectate;
- privind destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
- existența drepturilor la informare și de acces la datele colectate; de intervenție asupra datelor *(în special de a rectifica, actualiza, bloca sau șterge datele cu caracter personal a căror prelucrare contravine legii datorită caracterului incomplet sau inexact al acestora)* și de opoziție, precum și condițiile în care aceste drepturi pot fi exercitate; dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sunt obligatorii sau voluntare, inclusiv consecințele posibile ale refuzului de a răspunde la întrebările prin care se colectează informația.

b) Subiecților de date cu caracter personal le este asigurat dreptul de acces și posibilitatea de a lua cunoștință cu actele întocmite în scopul verificării corectitudinii întocmirii lor, contestării împotriva neincluderii sau includerii incorecte a unor date, precum și împotriva altor erori comise la înscrierea datelor despre sine. În acest sens, persoanele responsabile de prelucrarea datelor cu caracter personal, vor asigura accesul persoanei doar la datele cu caracter personal care-o vizează nemijlocit, fiind exclusă posibilitatea consultării datelor cu caracter personal ce vizează alți subiecți, conținute în fișele personale *(alte materiale)*, cu excepția cazurilor în care solicitanții își realizează un interes legitim care nu prejudiciază interesele sau drepturile și libertățile fundamentale ale subiectului datelor cu caracter personal;

c) Dreptul de informare este asigurat de către operatorul datelor cu caracter personal *(sau entitățile ce asigură mentenanța sistemului și sau prestează servicii de externalizare ale operatorului)* tuturor persoanelor supuse prelucrării;

d) În cazul realizării de către subiectul de date cu caracter personal a dreptului de intervenție, datele inexacte vor fi actualizate prin rectificare sau ștergere, ca bază servind doar surse legale *(acte de identitate, de stare civilă, resurse informaționale principale de stat etc.)*, modificarea urmând a fi efectuată în toate sistemele informaționale și de evidență gestionate.

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

a) Accesul în spațiile/perimetrul unde sunt amplasate sistemele informaționale și de evidență a datelor cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară conform politicii de securitate instituționale/regulamentelor departamentale aprobate;

b) Stocarea și păstrarea formatului electronic al datelor cu caracter personal, structurate în sisteme de evidență, în computere care sunt conectate la internet, nu sunt echipate cu mijloace de protecție speciale tehnice și de program și nu au instalate programe licențiate, programe antivirus, sisteme de control al securității soft-ului, de asigurare a efectuării periodice a copiilor de siguranță și de efectuare a auditului - este interzisă;

c) Introducerea în perimetrul de securitate instituțional și utilizarea calculatoarelor personale ori a purtătorilor de informații în scopuri de serviciu este interzisă. Mai mult, accesul la computerele din dotare sunt protejate/restricționate prin crearea profilurilor de

utilizatori, iar drepturile de administrator sunt încredințate doar persoanei responsabile pentru implementarea politicii de securitate desemnate din cadrul Instituției;

d) Stocarea datelor cu caracter personal pe 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, este asigurat prin plasarea acestora în safeuri sau dulapuri metalice care se încuie. Scoaterea, fără autorizare, a purtătorilor de date cu caracter personal din perimetrul de securitate al operatorului este interzisă.

15. Auditul sistemelor informaționale gestionate

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

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

b) Se efectuează înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:

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

c) Este efectuată înregistrarea modificărilor drepturilor de acces (competențelor) utilizatorului și statutului obiectelor de acces, conform următorilor parametri:

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

d) Se efectuează înregistrarea ieșirii din sistem a informației care conține date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecților și statutul obiectelor de acces, conform următorilor parametri:

- data și timpul eliberării;
- denumirea informației și căile de acces la aceasta;
- specificarea echipamentului (dispozitivului) care a eliberat informația (numele logic);
- ID-ul utilizatorului, care a solicitat informația.

16. Asigurarea protecției contra programelor dăunătoare (virușilor)

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

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

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

18. Gestionarea incidentelor de securitate

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

b) Personalul Instituției informează neîntârziat conducerea despre incidentele care încalcă securitatea sistemelor informaționale de date cu caracter personal;

c) Prelucrarea incidentelor include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor și restabilirea securității;

d) Până la 31 ianuarie a fiecărui an, operatorul de date cu caracter personal informează în scris Autoritatea națională pentru protecția datelor cu caracter personal despre incidentele de securitate constatate.

e) În cazul producerii incidentelor de securitate în cadrul CSPM Chișinău, persoana responsabilă va întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia și va înlătura cauzele incidentului de securitate cu informarea, în termen de 72 ore din momentul producerii incidentului de securitate, a Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova.

19. Marcarea documentelor

Toată informația care se intenționează a fi dezvăluită, și care conține date cu caracter personal, urmează a fi marcată prin includerea numărului de înregistrare din Registrul de evidență al operatorilor de date cu caracter personal.

Model Atenție! Documentul conține date cu caracter personal, prelucrate în cadrul sistemului de evidență nr. 000000X-00X, înregistrat în Registrul de evidență al operatorilor de date cu caracter personal www.registru.datepersonale.md. Prelucrarea ulterioară a acestor date poate fi efectuată numai în condițiile prevăzute de Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal

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

Operatorul de date cu caracter personal, persoana împuternicită de către operator, persoanele terțe după caz, pentru nerespectarea dispozițiilor Politicii de securitate - poartă răspundere civilă (Codul civil), contravențională (art. 74^1 Cod contravențional) și penală (art. art. 177, 178, 180 Cod penal).