Anexa nr.1
la ordinul CNTS nr. 166-O din 16 august 2019

POLITICA DE SECURITATE PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL LA PRELUCRAREA ACESTORA ÎN CADRUL CENTRULUI NAȚIONAL DE TRANSFUZIE A SÎNGELUI

I. DISPOZIȚII GENERALE

1. Politica de securitate a datelor cu caracter personal reglementează prelucrarea datelor cu caracter personal de către subdiviziunile Centrului Național de Transfuzie a Sângelui (în continuare Politica) stabilește rapoartele juridice care apar în procesul de prelucrare a tuturor datelor cu caracter personal, inclusiv celor care constituie categorii speciale de date cu caracter personal, care fac parte dintr-un sistem de evidență sau care sunt destinate să fie incluse într-un asemenea sistem, efectuată în totalitate sau în parte prin mijloace automatizate, precum și prin alte mijloace decât cele automatizate.
2. Prezenta Politică se aplică activităților de prelucrare a datelor cu caracter personal efectuate de către Centrul Național de Transfuzie a Sîngelui (în continuare - CNTS), în calitate de operator, dar și în calitatea acestora de persoane împuternicite de către operator sau beneficiari ai datelor cu caracter personal.
3. CNTS are calitatea de operator, dacă:
1) stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal;
2) scopurile și mijloacele de prelucrare a datelor cu caracter personal sunt prevăzute în mod expres de legislația în vigoare.
4. Au calitatea de persoane împuternicite de către operator, subdiviziunile din subordinea CNTS care prelucrează date cu caracter personal în numele și pe seama operatorului, pe baza instrucțiunilor primite de la operator.
5. La nivelul CNTS, prelucrarea datelor cu caracter personal se realizează cu respectarea prevederilor Legii nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal, Hotărârii Guvernului nr.1123 din 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", Hotărârii Guvernului nr. 296 din 15 mai 2012 „Privind aprobarea Regulamentului Registrului de evidență a operatorilor de date cu caracter personal", ordinului Ministerului Sănătății, Muncii și Protecției Sociale nr. 791 din 01.07.2019 „Cu privire la unele măsuri pentru înregistrarea Ministerului și a prestatorilor de servicii medicale în calitate de operatori de date cu caracter personal, inclusiv a sistemelor de evidență a datelor cu caracter personal gestionate de către acestea", precum și a prevederilor prezentei Politici.
6. Termenii și expresiile utilizate în prezenta Politică au semnificațiile prevăzute în Legea nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal. Categoriile de date cu caracter personal prelucrate și categoriile operațiunilor de prelucrare efectuate asupra lor se specifică în anexele nr.1 și nr.2 la prezenta Politică.
7. În sensul prezentei Politici se definesc următoarele noțiuni:
politica de securitate a datelor cu caracter personal — document, elaborat de către deținătorul de date cu caracter personal, 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;
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;

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;

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;

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 in orice alt mod, alăturarea ori combinarea, blocarea, ștergerea sau distrugerea;

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;

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;

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;

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;

terț — persoană fizică sau persoană juridică de drept public ori de drept privat, alta decât subiectul datelor cu caracter personal, decât operatorul ori persoana împuternicită de către operator și decât persoana care sub autoritatea directă a operatorului sau a persoanei împuternicite este autorizată să prelucreze date cu caracter personal;

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;

restaurarea datelor — procedurile cu privire la reconstituirea datelor cu caracter personal

în starea în care se aflau până la momentul pierderii sau distrugerii acestora;
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;
control de securitate — acţiuni întreprinse de către deţinătorii de date cu caracter personal sau Centrul Naţional pentru Protecţia Datelor cu Caracter Personal în vederea verificării şi/sau asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaţionale şi/sau registrelor ţinute manual;
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;
destinatar — orice persoană fizică sau persoană juridică de drept public ori de drept privat, inclusiv autoritatea publică şi subdiviziunile ei teritoriale, căreia îi sunt dezvăluite date cu caracter personal, indiferent dacă este sau nu terţ. Nu sunt considerate destinatari organele din domeniul apărării naţionale, securităţii statului şi ordinii publice, organele de urmărire penală şi instanţele judecătoreşti cărora li se comunică date cu caracter personal în cadrul exercitării competenţelor stabilite de lege;
administrator — subdiviziunea responsabilă de gestionarea şi operarea resurselor informaţionale ale sistemelor de evidenţă a datelor cu caracter personal;
beneficiari ai datelor cu caracter personal — structurile ale căror atribuţii de serviciu presupun operaţiuni de prezentare, recepţionare, eliberare, păstrare şi utilizare a informaţiei documentate în sistemele de evidenţă automatizate, precum şi în sistemele de evidenţă automatizate ale altor operatori sau persoane împuternicite de aceştia;
colectarea — strângerea, adunarea ori primirea datelor cu caracter personal prin orice mijloace legale şi din orice sursă;
înregistrarea — consemnarea datelor cu caracter personal într-un sistem de evidenţă automat ori manuală, care poate fi registru, fişier automat, bază de date sau orice altă formă de evidenţă organizată, structurată ori ad-hoc sau într-un text, înşiruire de date ori document, indiferent de modalitatea în care se înscriu datele;
organizarea — ordonarea, structurarea sau sistematizarea datelor cu caracter personal, conform unor criterii prestabilite, potrivit atribuţiilor legale ale operatorului, în scopul eficientizării/optimizării activităţilor de prelucrare a acestora;
stocarea — păstrarea pe orice fel de suport a datelor cu caracter personal colectate, inclusiv prin efectuarea copiilor de siguranţă;
adaptarea — transformarea datelor cu caracter personal colectate iniţial, conform criteriilor prestabilite şi scopurilor pentru care au fost colectate;
modificarea — actualizarea, completarea, schimbarea, corectarea datelor cu caracter personal, în scopul menţinerii caracteristicilor de exactitate, realitate, actualitate;
extragerea — scoaterea unei părţi din categoria specifică de date cu caracter personal, în scopul utilizării acesteia, separat şi distinct de prelucrarea iniţială;
consultarea — examinarea, vizualizarea, interogarea ori cercetarea datelor cu caracter personal, fără a fi limitate la acestea, în scopul efectuării unei operaţiuni sau set de operaţiuni de prelucrare ulterioară;
utilizarea — folosirea datelor cu caracter personal, în tot sau în parte, de către şi în interiorul operatorului, persoanelor împuternicite de către operator ori destinatarului, după

caz, inclusiv prin tipărire, copiere, multiplicare, scanare sau orice alte procedee similare;
dezvăluirea — a face disponibile date cu caracter personal operatorilor, persoanelor împuternicite de către aceşti şi terţilor prin comunicare, transmitere, diseminare sau în orice alt mod;
alăturarea — adăugarea, alipirea sau anexarea unor date cu caracter personal la cele deja existente, pe care nu le modifică;
combinarea — îmbinarea, unirea sau asamblarea unor date cu caracter personal separate iniţial, într-o formă nouă, pe baza unor criterii prestabilite, pentru scopuri anume determinate;
blocarea — întreruperea prelucrării datelor cu caracter personal;
ştergerea — eliminarea sau înlăturarea, în tot sau în parte, a datelor cu caracter personal din evidenţe sau înregistrări, prin împlinirea termenului de păstrare, la atingerea scopului pentru care au fost introduse, caducitatea, inexistenţa, inexactitatea;
transformarea — operaţiunea efectuată asupra datelor cu caracter personal având ca scop depersonalizarea ori utilizarea acestora în scopuri exclusiv statistice;
distrugerea — aducerea la stare de neîntrebuinţare, în condiţiile legii, definitivă şi irecuperabilă, prin mijloace mecanice sau termice, a suportului fizic pe care au fost prelucrate date cu caracter personal.
8. Operatorul, persoana împuternicită de către operator, utilizatorul şi beneficiarii datelor cu caracter personal utilizează sisteme de evidenţă şi/sau mijloace automate şi manuale de prelucrare a datelor cu caracter personal cu aplicarea principiilor respectării drepturilor şi libertăţilor persoanei, legalităţii, oportunităţii, confidenţialităţii şi proporţionalităţii şi numai dacă, prin utilizarea acestora, este asigurată protecţia datelor prelucrate.
9. Deţinătorul de date cu caracter personal numeşte o persoană responsabilă de elaborarea, implementarea şi monitorizarea respectări prevederilor politicii de securitate a datelor cu caracter personal, subordonată nemijlocit conducătorului instituţiei, care nu va avea alte responsabilităţi incompatibile cu sarcinile funcţiei de implementare a politicii.
1) Persoana responsabilă de politica de securitate a datelor cu caracter personal 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 acestei politici.
2) Persoana responsabilă de politica de securitate a datelor cu caracter personal asigură definirea clară a diferitelor responsabilităţi 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.
10.În cadrul activităţii de prelucrare a datelor cu caracter personal, operatorul, persoana împuternicită de către operator, utilizatorul şi beneficiarii datelor cu caracter personal se supun activităţilor de control a legalităţii prelucrărilor de date cu caracter personal efectuate de către Centru Naţional pentru Protecţia Datelor cu Caracter Personal (în continuare CNPDCP).

II. NOTIFICAREA PRELUCRĂRII DATELOR CU CARACTER PERSONAL

11.CNTS, în calitate de operator, notifică CNPDCP, despre prelucrarea datelor cu caracter personal, în condiţiile prevăzute de art. 23 din Legea nr. 133 din 08 iulie 2011 privind protecţia datelor cu caracter personal.

12.În situaţia în care CNIS efectuează mai multe categorii de prelucrări, iar acestea nu au acelaşi scop sau scopuri corelate, notificarea prevăzută la pct.l 1 se face separat pentru fiecare dintre aceste prelucrări.
13.Notificarea CNPDCP se realizează pe baza formularului tipizat al notificărilor aprobat prin Hotărârea Guvernului nr. 296 din 15 mai 2012.
14.La notificarea primară, CNIS primeşte un număr de înregistrare care se indică pe toate actele prin care datele cu caracter personal sunt colectate, stocate sau transmise, în conformitate cu prevederile Regulamentului Registrului de evidenţă a operatorilor de date cu caracter personal, aprobat prin Hotărârea Guvernului nr. 296 din 15 mai 2012.
15.Notificarea nu este necesară, în cazul în care prelucrarea are ca scop ţinerea unui registru destinat informării publicului larg şi deschis spre consultare publicului sau oricărei persoane care probează un interes legitim, cu condiţia ca prelucrarea să se limiteze la datele necesare ţinerii registrului menţionat.
16.Transferul de date cu caracter personal către un alt stat se face, în condiţiile legii, numai după notificarea CNPDCP şi recepţionarea autorizaţiei respective. Notificarea va cuprinde suplimentar:
1) categoriile de date care vor face obiectul transferului;
2) statul de destinaţie pentru fiecare categorie de date.
17.Notificarea CNPDCP prevăzută la pct.16 nu este necesară dacă transferul datelor cu caracter personal se face în baza prevederilor unei legi speciale sau ale unui tratat internaţional ratificat de Republica Moldova. Legea specială sau tratatul internaţional trebuie să conţină garanţii privind protecţia drepturilor subiectului datelor cu caracter personal.

III. PRELUCRAREA, STOCAREA ŞI UTILIZAREA DATELOR CU CARACTER PERSONAL

18.Datele cu caracter personal care fac obiectul prelucrării trebuie să fie:
1) prelucrate în mod corect şi conform prevederilor legii;
2) colectate în scopuri determinate, explicite şi legitime, iar ulterior să nu fie prelucrate într-un mod incompatibil cu aceste scopuri. Prelucrarea ulterioară a datelor cu caracter personal în scopuri statistice, de cercetare istorică sau ştiinţifică nu este considerată incompatibilă cu scopul colectării dacă se efectuează cu respectarea prevederilor prezentei legi, inclusiv privind notificarea către CNPDCP şi cu respectarea garanţiilor privind prelucrarea datelor cu caracter personal, prevăzute de normele ce reglementează activitatea statistică, cercetarea istorică şi cea ştiinţifică;
3) adecvate, pertinente şi neexcesive în ceea ce priveşte scopul pentru care sunt colectate şi/sau prelucrate ulterior;
4) exacte şi, dacă este necesar, actualizate. Datele inexacte sau incomplete din punctul de vedere al scopului pentru care sunt colectate şi ulterior prelucrate se şterg sau se rectifică;
5) stocate într-o formă care să permită identificarea subiecţilor datelor cu caracter personal pe o perioadă care nu va depăşi durata necesară atingerii scopurilor pentru care sunt colectate şi ulterior prelucrate.
19.Prelucrarea datelor cu caracter personal se poate realiza prin mijloace automatizate/sisteme informaţionale care conţin date cu caracter personal sau neautomatizate în cadrul unor operaţiuni ori seturi de operaţiuni, fără a fi limitate la acestea, cum ar fi: colectarea,

înregistrarea, organizarea, stocarea, adaptarea, modificarea, extragerea, consultarea, utilizarea, dezvăluirea, alăturarea, combinarea, blocarea, ştergerea, transformarea, distrugerea.
20.Prelucrarea datelor cu caracter personal se realizează de către subdiviziunile CNTS in exercitarea atribuţiilor stabilite printr-un act normativ sau atunci când acesta prevede constituirea unor sisteme de evidenţă la nivel naţional/interdepartamental/departamental, in scopul realizării unor activităţi/servicii de interes public.
21.Colectarea datelor cu caracter personal se poate face direct de la subiectul datelor cu caracter personal sau prin alte surse legale cu respectarea drepturilor subiectului datelor cu caracter personal şi instituirea unor măsuri adecvate de securitate a prelucrărilor.
22.Pentru realizarea activităţilor prevăzute în prezentul Politica, subdiviziunile CNTS colectează date cu caracter personal conform prevederilor art.5 al Legii nr. 133/2010 potrivit căreia:
1) Prelucrarea datelor cu caracter personal se efectuează cu consimţământul subiectului datelor cu caracter personal.
2) Consimţământul privind prelucrarea datelor cu caracter personal poate fi retras în orice moment de către subiectul datelor cu caracter personal. Retragerea consimţământului nu poate avea efect retroactiv.
3) În cazul incapacităţii de exercita sau al capacităţii de exerciţiu limitate a subiectului datelor cu caracter personal, consimţământul privind prelucrarea datelor cu caracter personal se acordă, în formă scrisă, de către reprezentantul lui legal.
4) În cazul decesului subiectului datelor cu caracter personal, consimţământul privind prelucrarea datelor sale se acordă, în formă scrisă, de către succesorii acestuia, dacă un astfel de consimţăminte nu a fost dat de subiectul datelor cu caracter personal în timpul vieţii.
5) Consimţământul subiectului datelor cu caracter personal nu este cerut în cazurile în care prelucrarea este necesară pentru:
a) executarea unui contract la care subiectul datelor cu caracter personal este parte sau pentru luarea unor măsuri înaintea încheierii contractului, la cererea acestuia;
b) îndeplinirea unei obligaţii care îi revine operatorului conform legii;
c) protejarea vieţii, integrităţii fizice sau a sănătăţii subiectului datelor cu caracter personal;
d) executarea sarcinilor de interes public sau care rezultă din exercitarea prerogativelor de autoritate publică cu care este învestit operatorul sau terţul căruia îi sunt dezvăluite datele cu caracter personal;
e) realizarea unui interes legitim al operatorului sau al terţului căruia îi sunt dezvăluite datele cu caracter personal, cu condiţia ca acest interes să nu prejudicieze interesele sau drepturile şi libertăţile fundamentale ale subiectului datelor cu caracter personal;
f) scopuri statistice, de cercetare istorică sau ştiinţifică, cu condiţia ca datele cu caracter personal să rămână anonime pe toată durata prelucrării.
23.Prelucrarea categoriilor speciale de date cu caracter personal este interzisă, cu excepţia cazurilor în care:
a) subiectul datelor cu caracter personal şi-a dat consimţământul. În cazul incapacităţii de exerciţiu sau al capacităţii de exerciţiu limitate a subiectului datelor cu caracter personal, prelucrarea categoriilor speciale de date cu caracter personal se efectuează numai cu obţinerea consimţământului în formă scrisă al reprezentantului lui legal;
b) prelucrarea este necesară pentru îndeplinirea obligaţiilor sau drepturilor specifice ale operatorului în domeniul dreptului muncii, cu respectarea garanţiilor prevăzute de lege şi

ţinându-se cont de faptul că o eventuală dezvăluire către un terţ a datelor cu caracter personal prelucrate în acest scop poate fi efectuată numai dacă există o obligaţie legală a operatorului în acest sens;
c) prelucrarea este necesară pentru protecţia vieţii, integrităţii fizice sau a sănătăţii subiectului datelor cu caracter personal ori a altei persoane, în cazul în care subiectul datelor cu caracter personal se află în incapacitate fizică sau juridică de a-şi da consimţământul;
d) prelucrarea este efectuată în contextul activităţilor legitime de către asociaţii obşteşti, partide şi alte organizaţii social-politice, de către sindicate, asociaţii de patronat, organizaţi filozofice sau religioase, organizaţii cooperatiste necomerciale, cu condiţia ca prelucrarea să se refere numai la membrii acestora sau la persoanele cu care acestea au contacte permanente în legătură cu scopurile lor şi cu condiţia ca datele să nu fie dezvăluite terţilor fără consimţământul subiecţilor datelor cu caracter personal;
e) prelucrarea se referă la date făcute publice în mod voluntar şi manifest de către subiectul datelor cu caracter personal;
f) prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în justiţie al subiectului datelor cu caracter personal;
g) prelucrarea este necesară în scopul asigurării securităţii statului, cu condiţia ca aceasta să se efectueze cu respectarea drepturilor subiectului datelor cu caracter personal şi a celorlalte garanţii prevăzute de prezenta lege.
24.Colectarea datelor cu caracter personal pentru realizarea activităţilor prevăzute la art. 8 al Legii nr. 133 din 08 iulie 2011 privind protecţia datelor cu caracter personal, se efectuează de către personalul subdiviziunilor CNIS (beneficiari ai datelor cu caracter personal) numai în scopul îndeplinirii atribuţiilor de serviciu.
25.Prelucrarea datelor cu caracter personal referitoare la măsuri procesuale de constrângere sau sancţiuni contravenţionale poate fi efectuată numai de către sau sub controlul autorităţilor publice, în limitele competentelor acordate şi în condiţiile stabilite prin legile ce reglementează aceste domenii.
26.Prelucrarea numărului de identificare de stat (IDNP) al persoanei fizice sau a altor date cu caracter personal având o funcţie de identificare de aplicabilitate generală poate fi efectuată în următoarele condiţii:
1) subiectul datelor cu caracter personal şi-a dat consimţământul;
2) prelucrarea este prevăzută în mod expres de legislaţie.
27.Informaţia ieşită din sistem, care conţine date cu caracter personal, se marchează, indicându-se prescripţii pentru prelucrarea ulterioară şi răspândirea acesteia, inclusiv indicându-se numărul de identificare unic al deţinătorului de date cu caracter personal.
28.Condiţiile şi termenele de stocare a datelor cu caracter personal se stabilesc de legislaţie ţinându-se cont de prevederile art. 4 alin. 1 lit. e) al Legii nr. 133 din 08 iulie 2011 privind protecţia datelor cu caracter personal.
29.La expirarea termenului de stocare, datele cu caracter personal urmează a fi distruse în modul stabilit de lege.
30.Datele cu caracter personal din registre, de la data încetării utilizării acestora, pot rămâne la păstrare primind statutul de document de arhivă.
31.La încheierea operaţiunilor de prelucrare a datelor cu caracter personal, dacă subiectul acestor date nu şi-a dat consimţământul pentru o altă destinaţie sau pentru o prelucrare ulterioară, acestea vor fi:

1) distruse;
2) transferate unui alt operator, cu condiția ca operatorul inițial să garanteze faptul că prelucrările ulterioare au scopuri similare celor în care s-a făcut prelucrarea inițială;
3) transformate în date anonime și stocate exclusiv în scopuri statistice, de cercetare istorică sau științifică.
32.După decesul subiectului datelor cu caracter personal, datele acestuia se pot utiliza, cu consimțământul succesorilor, în scop de arhivă sau în alte scopuri prevăzute de lege.

IV. DEZVĂLUIREA DATELOR CU CARACTER PERSONAL

33.Datele cu caracter personal se pot dezvălui între operatori și persoanele împuternicite de către operator sau între operatori sau persoanele împuternicite de către operator și alte instituții ori organisme publice sau entități de drept public sau privat în una dintre următoarele situații:
1) dacă subiectul datelor cu caracter personal și-a dat consimțământul expres și neechivoc pentru dezvăluirea datelor sale;
2) fără consimțământul subiectului datelor cu caracter personal în cazurile prevăzute de art. 5 alin. 5 din Legea nr. 133 din 08 iulie 2011 privind protecția datelor cu caracter personal;
3) în cazul prelucrării datelor cu caracter personal în activitățile de prevenire și investigare a infracțiunilor, punerii în executare a sentințelor de condamnare și al altor acțiuni din cadrul procedurii penale sau contravenționale în condițiile legii.
34.Dezvăluirea datelor cu caracter personal în situațiile prevăzute la pct. 33 se poate face dacă este îndeplinită una dintre următoarele condiții:
1) dezvăluirea se efectuează pe baza unui acord (contract) sau, după caz, a unui document de cooperare care trebuie să cuprindă cel puțin: numărul de înregistrare a notificării, temeiul legal al prelucrării și scopul acesteia, termenul maxim de prelucrare, drepturile și obligațiile părților, modalitățile de asigurare a securității prelucrărilor și de respectare a drepturilor persoanei vizate, precum și mențiunea că datele pot fi utilizate doar de beneficiar și numai în scopul pentru care au fost solicitate;
2) dezvăluirea se efectuează în baza unei solicitări scrise, care trebuie să cuprindă temeiul legal, scopul prelucrării și datele solicitate.
35.Dezvăluirea datelor cu caracter personal de către structurilor subdiviziunile MSMPS se poate face și on-line, cu respectarea Cerințelor 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 și dispozițiilor pct. 33 și pct. 34 ale prezentei Politici și asigurarea securității sistemelor de comunicații a datelor cu caracter personal.
36.Dezvăluirea prin transmitere a datelor cu caracter personal prin intermediul rețelelor de comunicații urmează a fi securizată, utilizându-se mijloace de criptare și cifrare cuvenite, utilizându-se poșta electronică guvernamentală și evitându-se transmiterea prin intermediul email-urilor personale de tip *@*gmail.com, *@*mail.ru, *@*yahoo.com, etc.
37.Documentele care conțin date cu caracter personal și corespondența electronică vor fi semnate la subsol cu conținutul corespunzător din anexa nr.3.
38.Datele cu caracter personal asupra cărora subiectul datelor cu caracter personal a exercitat și i s-a recunoscut dreptul de opoziție nu poate face obiectul prelucrării.
39.Cererile pentru dezvăluirea datelor cu caracter personal adresate CNTS, în calitatea sa de operator, în calitatea acestora de persoane împuternicite de către operator trebuie să conțină

datele de identificare a solicitantului, precum şi motivarea şi scopul cererii, conform prevederilor legale sau obligaţiilor cuprinse în tratate la care Republica Moldova este parte.
40.Cererile care nu conţin elementele prevăzute la pct.38 se restituie pentru completare, iar cele care nu se încadrează în condiţiile prevăzute de lege sau de tratatele la care Republica Moldova este parte se resping, menţionându-se motivele pentru care dezvăluirea datelor cu caracter personal nu este posibilă.
41.Înainte de dezvăluirea datelor cu caracter personal, subdiviziunile CNTS verifică dacă acestea sunt exacte şi, dacă este cazul, actualizate.
42.În situaţia în care se constată că au fost transmise date incorecte sau neactualizate subdiviziunile CNTS au obligaţia de a informa destinatarii respectivelor date asupra neconformităţii acestora, cu menţionarea datelor care au fost modificate.
43.La dezvăluirea datelor cu caracter personal subdiviziunile CNTS atenţionează destinatarii asupra interdicţiei de a prelucra datele pentru alte scopuri decât cele specificate în cererea de dezvăluire.

V. DREPTURILE ŞI OBLIGAŢIILE UTILIZATORULUI/BENEFICIARULUI

44.Utilizatorul/beneficiarul este în drept:
1) să obţină acces la sistemele de evidenţă a datelor cu caracter personal necesare pentru exercitarea obligaţiilor;
2) să beneficieze de utilaj şi de asigurarea de program a accesului la sistemele de evidenţă a datelor cu caracter personal;
3) în caz de necesitate să se adreseze administratorului pentru acordarea asistentei metodice.
45.Utilizatorul/beneficiarul este obligat:
1) să cunoască şi să respecte prevederile actelor legislative şi normative din domeniul prelucrării datelor cu caracter personal, precum şi actele departamentale specializate emise la nivelul MSMPS şi CNTS;
2) să aplice nume login, care poartă un caracter secret şi nu poate fi divulgat;
3) să respecte 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 cu o mărime de minimum 8 simboluri, 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 intervale de maximum 3 luni;
f) dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate);
4) să întreprindă măsurile tehnice şi organizatorice necesare pentru protecţia datelor cu caracter personal împotriva accesului ilicit sau întâmplător, distrugerii, modificării, blocării, copierii, răspândirii, precum şi a altor acţiuni ilicite din partea unor terţe persoane;
5) să păstreze confidenţialitatea datelor prelucrate, a contului deutilizator, parolei/codului de acces la sistemele de evidenţă a datelor cu caracter personal;

6) să respecte măsurile de securitate prevăzute de legislaţia în vigoare, precum şi celelalte reguli stabilite de operatorul sau persoanele împuternicite de către operator, inclusiv cele stabilite de către administrator;
7) să informeze imediat conducătorul nemijlocit sau, după caz, administratorul despre circumstanţele ce prezintă semne a riscului de acces ilicit sau întâmplător, distrugere, modificare, blocare, copiere, răspândire, precum şi a altor acţiuni ilicite a datelor cu caracter personal sau despre orice situaţie în care a fost admisă prelucrarea, inclusiv accesarea/vizualizarea/imprimarea datelor cu caracter personal cu încălcarea normelor legale;
8) să informeze subiectul datelor cu caracter personal atunci când datele cu caracter personal sunt colectate direct de la acesta, în condiţiile legii cu privire la: identitatea operatorului, scopul în care se face prelucrarea datelor, destinatarii sau categoriile de destinatari ai datelor, obligativitatea furnizării tuturor datelor cerute şi consecinţele refuzului de a le pune la dispoziţie, drepturile prevăzute de lege, în special drepturile de acces, de intervenţie asupra datelor şi de opoziţie, condiţiile în care pot fi exercitate aceste drepturi, respectiv să ofere orice alte informaţii a căror furnizare este impusă prin normele Legii nr. 133 din 08 iulie 2011 privind protecţia datelor cu caracter personal;
9) să prelucreze numai datele cu caracter personal necesare îndeplinirii atribuţiilor de serviciu şi să acorde sprijin conform actelor normative persoanei/subdiviziunii de protecţie a datelor cu caracter personal din cadrul CNTS şi/sau reprezentanţilor CNPDCP, conform competentelor acestora.
46. Atribuţiile specifice ale utilizatorului/beneficiarului se stabilesc obligatoriu şi în fişa postului.
47. La acordarea accesului la sistemele de evidenţă a datelor cu caracter personal, utilizatorul semnează declaraţie de modelul stabilit pe proprie răspundere privind respectarea normelor de protecţie a acestor date, în două exemplare, modelul fiind aprobat prin ordin intern al instituţiei în corespundere cu prevederile actelor în vigoare. Un exemplar se pune la dispoziţia administratorului, al doilea exemplar se anexează la contractual individual de muncă şi este parte component a acestuia, păstrându-se în dosarul personal al angajatului.
48. La nivelul oricărui utilizator/beneficiar se instituie Registrul de evidenţă a interpelărilor (cusut, sigilat, numerotat şi înregistrat in cancelarie), unde se duce evidenta tuturor interpelărilor, care va conţine obligatoriu următoarele rubrici:
1) locul stocării purtătorilor de date cu caracter personal;
2) sistemul de evidenţă în care au fost prelucrate datele cu caracter personal, proprietarul/gestionarul/deţinătorul;
3) numărul de ordine a interpelării (raportului);
4) numărul şi data înregistrării (raportului) în registru;
5) subdiviziunea care a solicitat informaţia;
6) volumul concret al datelor cu caracter personal supuse prelucrării;
7) numele şi semnătura angajatorului care a executat interpelarea;
8) numele şi, în cazul ridicării răspunsului personal - semnătura colaboratorului care a recepţionat informaţia;
9) volumul documentului eliberat (numărul paginilor, filelor, copiilor) şi rezultatul eliberării pozitiv sau negativ;
10) adnotare.

49. Șefii de subdiviziuni ai CNTS, care dispun de personal ale căror atribuții de serviciu presupun operațiuni de prelucrare a datelor cu caracter personal poartă răspundere personală pentru nerespectarea de către utilizatori/beneficiari a prevederilor prezentei Politici.

VI. SECURITATEA DATELOR CU CARACTER PERSONAL

50. La prelucrarea datelor cu caracter personal CNTS (operator) și persoana împuternicită de către operator sunt obligate să ia măsurile organizatorice și tehnice necesare pentru protecția datelor cu caracter personal împotriva distrugerii, modificării, copierii, răspândirii, precum și împotriva altor acțiuni ilicite, măsuri menite să asigure un nivel de securitate adecvat în ceea ce privește riscurile prezentate de prelucrare și caracterul datelor prelucrate.

6.1. Autorizarea accesului fizic

51. Accesul în sedii/oficii/birouri ori spațiile unde sunt amplasate sistemele de prelucrare a datelor cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară în baza cartelelor de identificare.

6.2. Administrarea și monitorizarea accesului fizic

52. Datele monitorizării sistemelor de control al accesului și supraveghere video se păstrează în sistem timp de un an. Încăperile unde sunt instalate serverele sistemului, care prelucrează datele cu caracter personal, vor fi echipate cu mijloace automatizate ce asigură identificarea cazurilor de acces neautorizat și inițierea acțiunilor de blocare a accesului.

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

53. Încăperile unde sunt instalate mijloacele de prelucrare a datelor cu caracter personal vor fi echipate cu sisteme de constatare a tentativelor pentru ușile exterioare și ferestrele amplasate în locuri accesibile. Utilajul de rezervă și suporturile copiilor de rezervă ale masivelor informaționale se păstrează în locuri îndepărtate de utilajul principal și care permit evitarea distrugerilor sau deteriorărilor ca rezultat al calamităților.

6.4. Controlul vizitatorilor

54. Datele sistemului automatizat de înregistrare a permiselor vizitatorilor ministerului se păstrează timp de un an. Vizitatorii încăperilor în care se efectuează prelucrarea datelor cu caracter personal vor fi însoțiți de către angajații instituției, desemnați în aceste scopuri.

1) Accesul vizitatorilor se înregistrează în registre, care vor fi păstrate pe o perioadă de 1 an.

2) La expirarea termenului, registrele vor fi lichidate, iar datele și documentele ce se conțin în registrul supus lichidării se transmit în arhivă.

6.5. Securitatea electroenergetică

55. Se va asigura securitatea echipamentului electric, a cablurilor electrice, inclusiv protecția acestora contra deteriorărilor și conectărilor neautorizate.

În cazul apariției situațiilor excepționale, de avarie sau de forță majoră, va fi asigurată posibilitatea deconectării electricității la sistemele de prelucrare a datelor cu caracter personal sau la componentele acestora.

Pentru asemenea cazuri vor fi prevăzute surse autonome de alimentare (diesel generator) cu energie electrică, care vor fi folosite pentru o perioadă de timp cu durata de 24 de ore.

6.6. Securitatea cablurilor de rețea

56. Cablurile de rețea vor fi protejate contra conectărilor neautorizate pentru o perioadă îndelungată. Cablurile de rețea cu destinație diversă vor fi separate una de alta.

Controalele în scopul verificării cazurilor de conectare neautorizată la cablurile de reţea se vor efectua cel puţin o dată în lună.

6.7. Asigurarea securităţii anti incendiare a sistemelor informaţionale de date cu caracter personal

57. În sediile în care se efectuează prelucrarea datelor cu caracter personal vor fi prevăzute mijloace de asigurare a securităţii anti incendiare, inclusiv sisteme automatizate de depistare/semnalizare şi stingere a incendiilor.

6.8. Controlul instalării şi scoaterii componentelor IT

58. Instalarea şi scoaterea mijloacelor software, mijloacelor hardware şi celor software/hardware de prelucrare a datelor cu caracter personal, precum şi a mijloacele ce nu ţin de prelucrarea datelor se va efectua numai de către angajaţii autorizaţi în conformitate cu Politica în vigoare.

Angajaţii subdiviziunii/Administratorul responsabili de realizarea Politicii vor efectua controlul mijloacelor software, mijloacelor hardware şi celor software/hardware, instalate la locurile de muncă (computerele) ale angajaţilor instituţiei.

Informaţia, ce conţine date cu caracter personal, amplasată pe purtătorii de informaţie, se distrug împreună cu purtătorul sau se înlătură de pe purtător prin metode, care exclud restabilirea ulterioară.

6.9. Măsurile generale de administrare a securităţii informaţionale

59. Locurile de muncă (computerele) şi imprimantele vor fi deconectate la terminarea sesiunilor de lucru.

Se interzice accesul neautorizat la utilajul de primire/expediere a corespondenţei, precum şi la dispozitivele de fax şi de imprimare/scanare/fotocopiere a documentelor. Mijloacele de prelucrare a datelor cu caracter personal vor fi scoase din perimetrul de securitate al instituţiei de către persoane responsabile, conform cu Politica, care determină procedura de strămutare a mijloacelor în limitele perimetrului clădirii şi a edificiilor din teritoriu.

VII. AUDITUL SECURITĂŢII ÎN SISTEMELE DE EVIDENŢĂ A DATELOR CU CARACTER PERSONAL

60. Operatorul de date cu caracter personal/persoana împuternicită organizează generarea înregistrărilor de audit a securităţii în sistemele de evidentă a datelor cu caracter personal pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.

61. Lista evenimentelor înregistrate de sistemul de audit a securităţii în sistemele de evidentă a datelor cu caracter personal:

1) se efectuează înregistrarea tentativelor de intrare ieşire a utilizatorului beneficiarului în sistem, conform următorilor parametri:

a) data şi timpul tentativei;

b) ID-ul utilizatorului/beneficiarului;

c) rezultatul tentativei de intrare/ieşire pozitivă sau negativă.

2) este efectuată înregistrarea tentativelor de pornire/terminare asesiunii deluceru a programelor aplicative şi proceselor, destinate prelucrăriidatelor cu caracter personal, înregistrarea modificărilor drepturilor de acces ale utilizatorilor/beneficiarilor şi statutul obiectelor de acces conform următorilor parametri:

a) data şi timpul tentativei de pornire;

b) denumirea/identificatorul programului aplicativ sau procesului;

c) ID-ul utilizatorului/beneficiarului;
d) rezultatul tentativei de pornire pozitivă sau negativă.
3) se efectuează înregistrarea tentativelor de obţinere a accesului (deexecutare aoperaţiunilor) pentru aplicaţii şi procese destinate prelucrării datelorcu caracter personal, conform următorilor parametri:
a) data şi timpul tentativei de obţinere a accesului (executare a operaţiunii);
b) denumirea (identificatorul) aplicaţiei sau procesului;
c) ID-ul utilizatorului/beneficiarului;
d) specificaţiile resursei protejate (identificator, nume logic, nume fişier, număr etc.);
e) tipul operaţiunii solicitate (citire, înregistrare, ştergere etc.);
f) rezultatul tentativei de obţinere a accesului (executare a operaţiunii) — pozitivă sau negativă.
4) este efectuată înregistrarea modificărilor drepturilor de acces (competenţelor) utilizatorului beneficiarului şi statutului obiectelor de acces, conform următorilor parametri:
a) data şi timpul modificării competenţelor;
b) ID-ul administratorului care a efectuat modificările;
c) ID-ul utilizatorului/beneficiarului şi competentele acestuia sau specificarea obiectelor de acces şi statutul nou al acestora.
5) se efectuează înregistrarea ieşirii din sistem a informaţiei care conţine date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecţilor şi statutul obiectelor de acces, conform următorilor parametri:
a) data şi timpul eliberării;
b) denumirea informaţiei şi căile de acces la aceasta;
c) specificarea echipamentului (dispozitivului) care a eliberat informaţia (numele logic);
d) ID-ul utilizatorului/beneficiarului, care a solicitat informaţia;
e) volumul documentului eliberat (numarul paginilor, a filelor, copiilor) şi rezultatul eliberării pozitiv sau negativ.
62. Subdiviziunea/Persoana responsabilă de realizarea Politicii de securitate, precum şi alte subdiviziuni împuternicite cu funcţii corespunzătoare vor efectua monitorizarea permanentă şi analiza înregistrărilor de audit, în scopul:
a) depistării cazurilor de acces ilegal la datele cu caracter personal (încălcarea obligaţiunilor funcţionale sau a condiţiilor contractului);
b) depistării cazurilor de încălcare a procedurii de acces la datele cu caracter personal, inclusiv fără consimţământul subiectului;
c) depistării cazurilor de utilizare a sistemelor de prelucrare a datelor cu caracter personal în scopuri ilegale, inclusiv pentru colectarea ilegală a datelor cu caracter personal.
63. În cazul depistării acţiunilor menţionate va fi informată conducerea instituţiei, va fi desfăşurată cercetarea de serviciu şi vor fi întreprinse măsuri de preîntâmpinare a unor astfel de cazuri.
64. Potrivit rezultatelor monitorizării şi analizei înregistrărilor de audit, o dată pe semestru, se întocmeşte un raport privind funcţionarea sistemelor de prelucrare a datelor cu caracter personal şi, în caz de necesitate, vor fi întreprinse acţiuni de ameliorare a funcţionării sistemelor de prelucrare datelor cu caracter personal.

VIII. MODALITATEA DE CONECTARE /DECONECTARE A UTILIZATORILOR ŞI

BENEFICIARILOR DATELOR CU CARACTER PERSONAL LA SISTEMELE DE EVIDENŢĂ A DATELOR CU CARACTER PERSONAL

65. Accesul la informaţia din sistemele de evidenţă a datelor cu caracter personal pentru utilizatorul datelor cu caracter personal (în continuare utilizator) se acordă de către administrator in baza demersului oficial, cu specificarea numărului necesar de locuri automatizate de muncă, categoriile de informaţii la care se permite accesul conform atribuţiilor de serviciu şi a datelor personale ale utilizatorului (NPP, IDNP, data naşterii, funcţia deţinută şi telefonul de contact).

66. Accesul beneficiarului datelor cu caracter personal (în continuare - beneficiar) la informaţia din sistemele de evidentă a datelor cu caracter personal ale altor operatori sau persoane împuternicite de către operator se efectuează în baza contactului/acordului incheiat în care sunt specificate categoriile de informaţii la care se permite accesul între deţinătorul sistemului de evidentă a datelor cu caracter personal şi CNTS. La solicitarea conducătorului CNTS, accesul la informaţia din sistemele de evidentă a datelor cu caracter personal pentru beneficiar se acordă de către subdiviziunea CNTS căreia conducerea CNTS i-a delegat atribuţiile corespunzătoare de administrator (Secţia Tehnologii Informaţionale), pe baza demersului oficial, cu specificarea numărului necesar de locuri automatizate de muncă, categoriile de informaţii la care se permite accesul şi a datelor personale ale utilizatorului (NPP, IDNP, data naşterii, funcţia deţinută şi telefonul de contact).

67. Administratorul execută, după caz, lucrările necesare de instalare a mijloacelor software la locurile de muncă autorizate ale utilizatorilor/beneficiarilor, şi acordă suport la conectarea acestora la sistemele de evidentă a datelor cu caracter personal, cu semnarea între părţi a actului de instalare-primire a locurilor de muncă.

68. Funcţionarea sistemului de evidentă este suspendată de către administrator în următoarele cazuri:

1) în timpul efectuării lucrărilor profilactice ale complexului demijloace software şi hardware ale Sistemului;

2) la apariţia circumstanţelor de forţă majoră;

3) la încălcarea sistemului securităţii de evidentă, dacă aceasta prezintă pericol pentru funcţionarea sistemului;

4) încazul suspendării serviciilor;

5) în caz de retragerea sistemului din exploatare.

69. Lucrările profilactice în complexul de mijloace software şi hardware ale sistemului de evidentă se efectuează după notificarea în scris ale utilizatorilor şi beneficiarelor cu cel puţin 2 zile lucrătoare înainte de începerea lucrărilor, cu indicarea termenului de finalizare a acestora.

70. În cazul apariţiei circumstanţelor de forţă majoră, precum şi al dificultăţilor tehnice în funcţionarea complexului de mijloace software şi hardware ale sistemului de evidentă din vina terţelor persoane, este posibilă suspendarea funcţionării sistemului de evidentă cu notificarea ulterioară a utilizatorilor si beneficiarelor conectati.

71. Revocarea dreptului de acces la sistemul de evidenţă de date cu caracter personal pentru utilizatori şi beneficiari se efectuează în una dintre următoarele situatii:

1) în temeiul cererii (demersului) conducătorului acestuia;

2) la intervenirea modificărilor raporturilor de muncă/de serviciu, iar noile atribuţii nu

impun accesul la datele sistemului de evidenţă;
3) la încetarea raporturilor de muncă/de serviciu ale utilizatorului şi beneficiarului;
4) deconectarea se efectuează în mod automat, în cazul lipsei de activitate in decurs de 2 luni;
5) în cazul încetării sau rezilierii contractului/acordului;
6) la constatarea încălcării de către utilizator sau beneficiar a măsurilor securităţii informaţionale a sistemului de evidenţă.

IX. ASIGURAREA INTEGRITĂŢII INFORMAŢIEI ŞI SISTEMELOR DE PRELUCRARE A DATELOR CU CARACTER PERSONAL

9.1 Introducerea modificărilor de soft destinat prelucrării datelor cu caracter personal

72. Elaborarea şi introducerea modificărilor în soft-ul destinat prelucrării datelor cu caracter personal se va efectua în coordonare cu subdiviziunea/persoana responsabilă de realizarea Politicii de securitate.

9.2 Asigurarea protecţiei contra programelor dăunătoare (virușilor)

73. În sistemele de prelucrare a datelor cu caracter personal va fi asigurată protecţia împotriva infiltrării programelor dăunătoare (virușilor), precum şi reînnoirea automată şi la timp a mijloacelor de asigurare a protecţiei contra programelor dăunătoare şi a signaturilor de virus.

Va fi asigurată administrarea centralizată a mecanismelor de protecţie a sofît-urilor.

9.3 Tehnologiile şi mijloacele de constatare a tentativelor

74. Vor fi utilizate tehnologii şi mijloace de constatare a tentativelor, care ar permite monitorizarea evenimentelor în sistemele de prelucrare a datelor cu caracter personal şi constatarea atacurilor, inclusiv care ar asigura identificarea tentativelor folosirii neautorizate a sistemelor informaţionale.

9.4 Testarea posibilităţilor funcţionale de asigurare a securităţii sistemelor de prelucrare a datelor cu caracter personal

75. Va fi asigurată testarea funcţionării corecte a funcţiilor de securitate a sistemelor de prelucrare a datelor cu caracter personal (automat la pornirea sistemului şi lunar la solicitarea administratorului sistemului).

X. COPIILE DE REZERVĂ ŞI RESTABILIREA INFORMAŢIEI

10.1 Copiile de rezervă ale informaţiei care conţine date cu caracter personal

76. Copierea de rezervă a informaţiei care conţine date cu caracter personal va fi efectuată în conformitate cu regulile generale privind crearea, păstrarea şi utilizarea copiilor de rezervă a băncii centrale de date.

10.2 Serviciile telecomunicaţionale de rezervă

77. Vor fi identificate şi asigurate serviciile telecomunicaţionale de bază şi de rezervă ale sistemelor de prelucrare a datelor cu caracter personal.

Furnizorii serviciilor telecomunicaţionale de bază şi de rezervă vor fi diferiţi.

XI. CONTROLUL DE SECURITATE AL SISTEMELOR DE PRELUCRARE A DATELOR CU CARACTER PERSONAL

78. Controlul de securitate al sistemelor de prelucrare a datelor cu caracter personal va fi efectuat o dată pe an. Conform rezultatelor controalelor va fi întocmit raportul pentru fiecare sistem.

79. Rezultatele controalelor de securitate a sistemelor de prelucrare a datelor cu caracter personal servesc temei pentru introducerea modificărilor în Politica de securitate a datelor cu caracter personal.
80. Controalele de securitate a sistemelor de prelucrare a datelor cu caracter personal vor fi actualizate de fiecare dată în urma schimbării infrastructurii.

XII. MODUL DE ORGANIZARE ŞI REALIZARE A MĂSURILOR DE INFORMARE ASUPRA OPERAŢIUNILOR DE PRELUCRARE A DATELOR CU CARACTER PERSONAL

81. Subdiviziunile CNTS care efectuează operaţiuni de prelucrare a datelor cu caracter personal în conformitate cu Legea nr.133 din 08 iulie 2011 privind protecţia datelor cu caracter personal (în continuare — subdiviziunile CNTS abilitate) vor respecta prevederile şi restricţiilor stabilite în Lege, precum şi Cerinţele faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr. 1123 din 14 decembrie 2010, inclusiv:

art.4 alin.(1)

1) prelucrate în mod corect şi conform a prevederilor legii;
2) colectate în scopuri determinate, explicite şi legitime, iar ulterior să nu fie prelucrate într-un mod incompatibil cu aceste scopuri. Prelucrarea ulterioară a datelor cu caracter personal în scopuri statistice, de cercetare istorică sau ştiinţifică nu este considerată incompatibilă cu scopul colectării dacă se efectuează cu respectarea prevederilor prezentei legi, inclusiv privind notificarea către Centrul Naţional pentru Protecţia Datelor cu Caracter Personal, şi cu respectarea garanţiilor privind prelucrarea datelor cu caracter personal, prevăzute de normele ce reglementează activitatea statistică, cercetarea istorică şi cea ştiinţifică;
3) adecvate, pertinente şi neexcesive în ceea ce priveşte scopul pentru care sunt colectate şi/sau prelucrate ulterior;
4) exacte şi, dacă este necesar, actualizate. Datele inexacte sau incomplete din punctul de vedere al scopului pentru care sunt colectate şi ulterior prelucrate se şterg sau se rectifică;
5) stocate într-o formă care să permită identificarea subiecţilor datelor cu caracter personal pe o perioadă care nu va depăşi durata necesară atingerii scopurilor pentru care sunt colectate şi ulterior prelucrate.

art.12 alin.(1) şi (2)

1) în cazul în care datele cu caracter personal sunt colectate direct de la subiectul datelor, operatorul sau persoana împuternicită de către operator este obligată să-i furnizeze următoarele informaţii, exceptând cazul în care acesta deţine deja informaţiile respective:
a) identitatea operatorului sau, după caz, a persoanei împuternicite de către operator;
b) scopul prelucrării datelor colectate;
c) informaţii suplimentare, precum:

- destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
- existenţa drepturilor de acces la date, de intervenţie asupra datelor şi de opoziţie, precum şi condiţiile în care acestea pot fi exercitate;
- dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sunt obligatorii sau voluntare, precum şi consecinţele posibile ale refuzului de a răspunde.

2) în cazul în care datele cu caracter personal nu sunt colectate direct de la subiectul datelor, operatorul sau persoana împuternicită de către operator este obligată ca, în momentul colectării datelor sau, dacă se intenţionează dezvăluirea acestora către terţi, cel mai târziu în momentul primei dezvăluiri, să furnizeze subiectului datelor cu caracter personal informaţia privind categoriile de date care urmează a fi colectate sau dezvăluite, precum şi informaţiile indicate la alin.(1), cu excepţia pct.3) lit.c).

art. 13

1) Orice subiect al datelor cu caracter personal are dreptul să obţină de la operator, la cerere, fără întârziere şi în mod gratuit:

a) confirmarea faptului că datele care îl privesc sunt sau nu sunt prelucrate de acesta, de asemenea informaţii referitoare la scopurile prelucrării, categoriile de date avute în vedere şi destinatarii sau categoriile de destinatari cărora le sunt dezvăluite datele;

b) comunicarea, într-o formă inteligibilă şi într-un mod care nu necesită un echipament suplimentar, a datelor cu caracter personal care fac obiectul prelucrării, precum şi a oricărei informaţii disponibile privind originea acestor date;

c) informaţii privind principiile de funcţionare a mecanismului prin care se efectuează prelucrarea automatizată a datelor care vizează subiectul datelor cu caracter personal;

d) informaţii cu privire la consecinţele juridice generate de prelucrarea datelor cu caracter personal pentru subiectul acestor date;

e) informaţii privind modul de exercitare a dreptului de intervenţie asupra datelor cu caracter personal.

art.14

1) Orice subiect al datelor cu caracter personal are dreptul de a obţine de la operator sau persoana împuternicită de către acesta, la cerere şi în mod gratuit:

a) rectificarea, actualizarea, blocarea sau ştergerea datelor cu caracter personal a căror prelucrare contravine prezentei legi, în special datorită caracterului incomplet sau inexact al datelor;

b) notificarea terţilor cărora le-au fost dezvăluite datele cu caracter personal despre operaţiunile efectuate conform lit.a), excepând cazurile când această notificare se dovedeşte a fi imposibilă sau presupune un efort disproporţionat faţă de interesul legitim care ar putea fi lezat.

art. 28

1) în scopul evidenţei prelucrărilor de date cu caracter personal, CNPDCP instituie şi administrează un registru de evidenţă al operatorilor de date cu caracter personal care trebuie să cuprindă informaţiile stabilite la art. 23 alin. (2). Orice modificare a informaţiilor respective va fi comunicată Centrului în termen de 5 zile, care va efectua menţiunile corespunzătoare în registrul de evidenţă al operatorilor de date cu caracter personal.

2) Registrul de evidenţă al operatorilor de date cu caracter personal este deschis spre consultare publicului, cu excepţia compartimentului care conţine informaţii privind măsurile de securitate şi de asigurare a confidenţialităţii.

Înregistrarea operatorilor, precum şi a modificărilor informaţiilor înscrise în registrul de evidenţă al operatorilor de date cu caracter personal, se efectuează gratuit.

XIII. SISTEME DE EVIDENŢĂ ÎN CARE SUNT STOCATE INFORMAŢII CU

DATE CU CARACTER PERSONAL

82. În cadrul CNTS informaţiile care conţin date cu caracter personal se prelucrează manual, automat şi mixt. Sistemele informaţionale de date cu caracter personal sunt de evidenţă administrativă, economico-financiară, contabilă, de personal şi petiţii.

83. Sisteme informaţionale automatizate de prelucrarea a informaţiilor care conţin date cu caracter personal gestionate:

1) Sistemul informaţional automatizat Serviciul de Sânge „CTS Manager". Sistemul conţine date cu caracter personal şi are ca scop evidenta donatorilor de sânge/componente sanguine;

2) Sistemul electronic „Programul automatizat de evidenţă contabilă 1C". Sistemul conţine date cu caracter personal şi are ca scop evidenta contabilă a bunurilor material din gestiunea instituţiei, dar şi remunerarea personalului angajat al instituţiei;

3) Sistemul Informatic de Evidenţă a Resurselor Umane din Sistemul Sănătăţii al Republicii Moldova În cadrul Serviciul Resurse Umane;

84. Protecţia datelor cu caracter personal în sistemele informaţionale de date cu caracter personal este asigurată printr-un complex de măsuri tehnice şi organizatorice de preîntâmpinare a prelucrării ilicite a datelor cu caracter personal.

85. Sunt supuse protecţiei toate resursele informaţionale ale deţinătorilor de date cu caracter personal, care conţin date cu caracter personal, inclusiv:

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

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

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

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

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

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

4) asigurării caracterului complet, integru, veridic al datelor cu caracter personal în reţelele telecomunicaţionale şi resurselor informaţionale;

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

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

1) preîntâmpinarea 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) preîntâmpinarea acţiunilor speciale tehnice şi de program, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program;
4) 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.
88. 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.
89. Preîntâmpinarea accesului neautorizat la informaţiile care conţin date cu caracter personal şi circulă sau se păstrează în mijloace tehnice este asigurată prin metoda folosirii mijloacelor speciale tehnice şi de program, cifrării acestor informaţii, inclusiv prin măsurile organizaţionale şi de regim.
90. 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.
91. Ordinea de acces la informaţia care conţine date cu character personal, prelucrată în cadrul sistemelor informaţionale, se stabileşte de către operator, în conformitate cu prevederile legislaţiei.

XIV. RESPONSABILITĂŢI

92. Conducătorul utilizatorului persoana împuternicită, de comun cu administratorul (Secţia Tehnologii Informaţionale), care dispune de acces la sistemele de evidenţă a datelor cu caracter personal are următoarele responsabilităţi:
1) să asigure susţinerea funcţionării computerelor care fac parte din sistemele de evidenţă a datelor cu caracter personal;
2) să asigure mijloacele tehnice de blocare a fişierelor automatizate, dacă utilizatorul/beneficiarul nu acţionează asupra datelor afişate pe ecran o perioadă de timp de până la 15 minute, stabilită in funcţie de operaţiile care trebuie executate;
3) să efectueze controlul plenitudinii şi veridicităţii demersurilor (interpelărilor, rapoartelor) privind eliberarea informaţiei din sistemele de evidenţă a datelor cu caracter personal.
93. Utilizatorul/beneficiarul şi persoana care a interceptat informaţia din sistemele de evidenţă a datelor cu caracter personal poartă răspundere pentru asigurarea securităţii şi protecţiei informaţiei acumulate, neexecutarea sau executarea necorespunzătoare a obligatelor prevăzute în prezenta Politică.
94. Şefii de subdiviziuni care sunt conectate la sistemele de evidenţă a datelor cu caracter personal dispun măsurile necesare în vederea instituirii şi menţinerii unui nivel suficient

de securitate a prelucrării datelor cu caracter personal, care vor consta cel puţin în:
1) interzicerea instalării de către personalul CNTS a altor programe software în afara celor configurate de personalul autorizat, pentru îndeplinirea atribuţiilor de serviciu;
2) configurarea porturilor de acces la mediile de stocare pentru fiecare staţie de lucru şi a comenzilor care permit salvarea documentelor, în mod adecvat, pentru categoriile de operaţiuni efectuate de fiecare utilizator/beneficiar, în strictă legătură cu îndeplinirea atribuţiilor de serviciu ale acestuia;
3) implementarea unor aplicaţii automate de contracarare a vulnerabilităţilor si ameninţărilor informatice si de securitate a sistemelor informatice.
95. Toate documentele care conţin date cu caracter personal se înregistrează şi urmează regulile de păstrare, procesare, multiplicare, transportare, transmitere, distrugere şi arhivare stabilite prin acte normative.
96. Subdiviziunile care prelucrează date cu caracter personal au obligaţia să transmită Administratorului (Secţia Tehnologii Informaţionale), anual, către 31 decembrie, raportul despre incidentele de securitate a sistemelor de evidenţă a datelor cu caracter personal.
97. Anual, către 31 ianuarie, Administratorul prezintă Centrului Naţional pentru Protecţia Datelor cu Caracter Personal raportul generalizat despre incidentele de securitate a sistemelor de evidenţă a datelor cu caracter personal produse.

Anexa nr.1
la Politica de securitate a datelor cu character personal în cadrul CNTS

CATEGORIILE DE DATE CU CARACTER PERSONAL

1. Datele cu caracter personal, care direct sau indirect identifică o persoană, fizică, în special prin referire la un număr de identificare (cod personal), la unul sau mai multe elemente specifice proprii identităţii sale fizice, fiziologice, psihice, economice, culturale sau sociale, se împart în două categorii: obişnuite şi speciale.
2. ***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.
3. ***Categoria obişnuită*** o constituie informaţia care dezvăluie:
1) numele şi prenumele;
2) sexul;
3) data şi locul naşterii;
4) cetăţenia;
5) IDNP;
6) imaginea;
7) situaţia familială;
8) situaţia militară;
9) datele personale ale membrilor de familie;
10) datele din certificatul de înmatriculare;
11) datele bancare;
12) semnătura;
13) datele din actele de stare civilă;
14) codul personal de asigurării sociale (CPAS);
15) codul asigurării medicale (CPAM);
16) numărul de telefon/fax;
17) numărul de telefon mobil;
18) adresa (domiciliului/sediului);
19) adresa e-mail;
20) profesia şi/sau locul de muncă;
21) formarea profesională — diplome studii.

Anexa nr.2
la Politica de securitate a datelor cu caracter personal în cadrul CNTS

CATEGORIILE OPERAȚIUNILOR DE PRELUCRARE A DATELOR CU CARACTER PERSONAL, SUSCEPTIBILE DE A PREZENTA RISCURI SPECIALE PENTRU DREPTURILE ȘI LIBERTĂȚILE PERSOANELOR

Prezintă riscuri speciale pentru drepturile și libertățile persoanelor următoarele categorii ale operațiunilor de prelucrare a datelor cu caracter personal:

1) adaptarea, modificarea, dezvăluirea prin transmitere, difuzare sau în orice alt mod, a datelor cu caracter personal legate de originea rasială sau etnică, de convingerile politice, religioase, de apartenența la un partid politic sau o organizație religioasă, a datelor cu caracter personal privind starea de sănătate sau viață intimă, precum și a datelor cu caracter personal referitoare la condamnările penale, măsurile de constrângere, sancțiunile disciplinare sau contravenționale;

2) operațiunile de prelucrare a datelor care permit localizarea geografică a persoanelor prin intermediul rețelelor de comunicații electronice;

3) operațiunile de prelucrare a datelor cu caracter personal prin mijloace electronice, având ca scop evaluarea unor aspecte de personalitate, precum competența profesională, credibilitatea, comportamentul etc.;

4) operațiunile de prelucrare a datelor cu caracter personal prin mijloace electronice în cadrul unor sisteme de evidență, având ca scop analizarea situației economico-financiare, a faptelor susceptibile de a atrage răspunderea disciplinară, contravențională sau penală a persoanelor fizice;

5) operațiunile de prelucrare a datelor cu caracter personal ale minorilor în scopuri comerciale (activităților de marketing direct);

6) operațiunile de prelucrare a datelor cu caracter personal menționate la subpunctele 1) și 2) din prezenta anexă, precum și datele cu caracter personal ale minorilor, colectate prin intermediul Internetului sau mesageriei electronice.

Anexa nr.3
la Politica de securitate a datelor cu caracter personal în cadrul CNTS

Conținutul textului
care se va include la subsolul documentelor care conțin date cu caracter personal

Atenție! Documentul conține date cu caracter personal **prelucrate în sistemul de evidență nr. 000002[illegible]001, înregistrat în Registru de evidență al operatorilor de date cu caracter personal** www.registru.datepersonale.md, în conformitate cu prevederile Legii nr. [illegible]133 din 08.07.2011 privind protecția datelor cu caracter personal. Acest document este destinat numai pentru uzul organelor abilitate de lege și nu poate fi dat publicității. Prelucrarea ulterioară a acestor date poate fi efectuată numai în condițiile Legii nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal. Operațiunile efectuate fără drept în legătură cu **acest document sunt pedepsite conform legislației Republicii Moldova**.

Conținutul textului care se va include la subsolul corespondenței electronice

Acest mesaj este confidențial și este adresat exclusiv destinatarului, pentru uzul acestuia din urmă. Dacă primiți acest mesaj din eroare, vă rugăm să informați imediat pe cel care l-a trimis și să ștergeți mesajul și orice atașamente ale mesajului. Vă mulțumim.
În măsura permisă de lege, se indică denumirea instituției, nu va fi în nici un fel răspunzătoare pentru nici un fel de daune, indiferent de natura acestora rezultând din erori de transmitere, virusi, influența externă, întârzieri sau alte cauze similare.