

Anexa nr. 1
la ordinul INN,,Diomid Gherman”

nr. 106 din 02.08 2019

**POLITICA DE SECURITATE
A DATELOR CU CARACTER PERSONAL A
IMSP INSTITUTUL DE NEUROLOGIE ȘI
NEUROCHIRURGIE,,DIOMID GHERMAN”**

Mun. Chișinău, str, Korolenko,2
Cod fiscal:1003600150602
MF Trezoreria de Stat
Cod TREZMD2X
IBAN: MD88AGPEBL518430A00077AA

I. DISPOZIȚII GENERALE

1. Politica de securitate a datelor cu caracter personal reglementează prelucrarea datelor cu caracter personal de către secțiile clinice și serviciile medicale, serviciile administrative și tehnice ale IMSP Institutului de Neurologie și Neurochirurgie „Diomid Gherman” (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 IMSP Institutul de Neurologie și Neurochirurgie „Diomid Gherman” (în continuare – IMSP INN „Diomid Gherman”), în calitate de operator; de către subdiviziunile IMSP INN „Diomid Gherman”, în calitatea acestora de persoane împuternicite de către operator sau beneficiari ai datelor cu caracter personal.

3. IMSP INN „Diomid Gherman” 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 IMSP INN „Diomid Gherman” care prelucrează date cu caracter personal în numele și pe seama operatorului, pe baza instrucțiunilor primite de la operator.

5. La nivelul IMSP INN „Diomid Gherman”, 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”, 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 în 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 și aplicației de utilizare a resursei informaționale sau din momentul pornirii resursei informaționale și până la momentul opririi acestora;

control de securitate — acțiuni întreprinse de către deținătorii de date cu caracter personal sau Centrul Național pentru Protecția Datelor cu Caracter Personal în vederea verificării și/sau asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaționale și/sau registrelor ținute manual;

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;

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;

destinatar — orice persoană fizică sau persoană juridică de drept public ori de drept privat, inclusiv autoritatea publică și subdiviziunile ei teritoriale, căreia îi sunt dezvăluite date cu caracter personal, indiferent dacă este sau nu terț. Nu sunt considerate destinatari organele din domeniul apărării naționale, securității statului și ordinii publice, organele de urmărire penală și instanțele judecătorești cărora li se comunică date cu caracter personal în cadrul exercitării competențelor stabilite de lege;

administrator — subdiviziunea responsabilă de gestionarea și operarea resurselor informaționale ale sistemelor de evidență a datelor cu caracter

personal;

beneficiari ai datelor cu caracter personal — structurile ale căror atribuții de serviciu presupun operațiuni de prezentare, recepționare, eliberare, păstrare și utilizare a informației documentate în sistemele de evidență automatizate, precum și în sistemele de evidență automatizate ale altor operatori sau persoane împuternicite de aceștia;

colectarea — strângerea, adunarea ori primirea datelor cu caracter personal prin orice mijloace legale și din orice sursă;

înregistrarea — consemnarea datelor cu caracter personal într-un sistem de evidență automat ori manuală, care poate fi registru, fișier automat, bază de date sau orice altă formă de evidență organizată, structurată ori ad-hoc sau într-un text, înșiruire 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 atribuțiilor legale ale operatorului, în scopul eficientizării/optimizării activităților de prelucrare a acestora;

stocarea — păstrarea pe orice fel de suport a datelor cu caracter personal colectate, inclusiv prin efectuarea copiilor de siguranță;

adaptarea — transformarea datelor cu caracter personal colectate inițial, conform criteriilor prestabilite și scopurilor pentru care au fost colectate;

modificarea — actualizarea, completarea, schimbarea, corectarea datelor cu caracter personal, în scopul menținerii caracteristicilor de exactitate, realitate, actualitate;

extragerea — scoaterea unei părți din categoria specifică de date cu caracter personal, în scopul utilizării acesteia, separat și distinct de prelucrarea inițială;

consultarea — examinarea, vizualizarea, interogarea ori cercetarea datelor cu caracter personal, fără a fi limitate la acestea, în scopul efectuării unei operațiuni sau set de operațiuni de prelucrare ulterioară;

utilizarea — folosirea datelor cu caracter personal, în tot sau în parte, de către și 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 aceștia și terților 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 inițial, într-o formă nouă, pe baza unor criterii prestabilite, pentru scopuri anume determinate;

blocarea — întreruperea prelucrării datelor cu caracter personal;

ștergerea — eliminarea sau înlăturarea, în tot sau în parte, a datelor cu caracter personal din evidențe sau înregistrări, prin împlinirea termenului de păstrare, la atingerea scopului pentru care au fost introduse, caducitatea, inexistența, inexactitatea;

transformarea — operațiunea efectuată asupra datelor cu caracter personal având ca scop depersonalizarea ori utilizarea acestora în scopuri exclusiv statistice;

distrugerea — aducerea la stare de neîntrebuințare, în condițiile legii, definitivă și 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 și beneficiarii datelor cu caracter personal utilizează sisteme de evidență și/sau mijloace automate și manuale de prelucrare a datelor cu caracter personal cu aplicarea principiilor respectării drepturilor și libertăților persoanei, legalității, oportunității, confidențialității și proporționalității și numai dacă, prin utilizarea acestora, este asigurată protecția datelor prelucrate.

9. Deținătorul de date cu caracter personal numește o persoană responsabilă de elaborarea, implementarea și monitorizarea respectării prevederilor politicii de securitate a datelor cu caracter personal, subordonată nemijlocit conducătorului instituției, care nu va avea alte responsabilități incompatibile cu sarcinile funcției 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 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.

2) 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.

10. În cadrul activității de prelucrare a datelor cu caracter personal, operatorul, persoana împuternicită de către operator, utilizatorul și beneficiarii datelor cu caracter personal se supun activităților de control a legalității prelucrărilor de date cu caracter personal efectuate de către Centru Național pentru Protecția Datelor cu Caracter Personal (în continuare CNPDCP).

II. NOTIFICAREA PRELUCRĂRII DATELOR CU CARACTER PERSONAL

11. IMSP INN „Diomid Gherman”, în calitate de operator, notifică CNPDCP, despre prelucrarea datelor cu caracter personal, în condițiile prevăzute de art. 23 din Legea nr. 133 din 08 iulie 2011 privind protecția datelor cu caracter personal.

12. În situația în care IMSP INN „Diomid Gherman” efectuează mai multe categorii de prelucrări, iar acestea nu au același scop sau scopuri corelate, notificarea prevăzută la pct.11 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, IMSP INN „Diomid Gherman” primește 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 evidență 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 ținerea unui registru destinat informării publicului larg și deschis spre consultare publicului sau oricărei persoane care probează un interes legitim, cu condiția ca prelucrarea să se limiteze la datele necesare ținerii registrului menționat.

16. Transferul de date cu caracter personal către un alt stat se face, în condițiile legii, numai după notificarea CNPDCP și recepționarea autorizației respective. Notificarea va cuprinde suplimentar:

- 1) categoriile de date care vor face obiectul transferului;
- 2) statul de destinație 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 internațional ratificat de Republica Moldova. Legea specială sau tratatul internațional trebuie să conțină garanții privind protecția drepturilor subiectului datelor cu caracter personal.

III. PRELUCRAREA, STOCAREA SI UTILIZAREA DATELOR CU CARACTER PERSONAL

18. Datele cu caracter personal care fac obiectul prelucrării trebuie să fie:

- 1) prelucrate în mod corect și conform prevederilor legii;
- 2) colectate în scopuri determinate, explicite și 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 științifică nu este considerată incompatibilă cu scopul colectării dacă se efectuează cu respectarea prevederilor prezentei legi, inclusiv privind notificarea către CNPDCP și cu respectarea garanțiilor privind prelucrarea datelor cu caracter personal, prevăzute de normele ce reglementează activitatea statistică, cercetarea istorică și cea științifică;
- 3) adecvate, pertinente și neexcesive în ceea ce privește scopul pentru care sunt colectate și/sau prelucrate ulterior;
- 4) exacte și, dacă este necesar, actualizate. Datele inexacte sau incomplete din punctul de vedere al scopului pentru care sunt colectate și ulterior prelucrate

se șterg sau se rectifică;

5) stocate într-o formă care să permită identificarea subiecților datelor cu caracter personal pe o perioadă care nu va depăși durata necesară atingerii scopurilor pentru care sunt colectate și ulterior prelucrate.

19. Prelucrarea datelor cu caracter personal se poate realiza prin mijloace automatizate/sisteme informaționale care conțin date cu caracter personal sau neautomatizate în cadrul unor operațiuni ori seturi de operațiuni, fără a fi limitate la acestea, cum ar fi: colectarea, înregistrarea, organizarea, stocarea, adaptarea, modificarea, extragerea, consultarea, utilizarea, dezvăluirea, alăturarea, combinarea, blocarea, ștergerea, transformarea, distrugerea.

20. Prelucrarea datelor cu caracter personal se realizează de către subdiviziunile IMSP INN „Diomid Gherman” în exercitarea atribuțiilor stabilite printr-un act normativ sau atunci când acesta prevede constituirea unor sisteme de evidență la nivel național/interdepartamental/departamental, în scopul realizării unor activități/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 și instituirea unor măsuri adecvate de securitate a prelucrărilor.

22. Pentru realizarea activităților prevăzute în prezentul Politica, subdiviziunile IMSP INN „Diomid Gherman” 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 consimțământul subiectului datelor cu caracter personal.

2) consimțământul privind prelucrarea datelor cu caracter personal poate fi extras în orice moment de către subiectul datelor cu caracter personal. Retragera consimțământului nu poate avea efect retroactiv.

3) în cazul incapacității de exercita sau al capacității de exercițiu limitate a subiectului datelor cu caracter personal, consimțământul 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, consimțământul privind prelucrarea datelor sale se acordă, în formă scrisă, de către succesorii acestuia, dacă un astfel de consimțăminte nu a fost dat de subiectul datelor cu caracter personal în timpul vieții.

5) consimțământul 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 obligații care îi revine operatorului conform legii;

c) protejarea vieții, integrității fizice sau a sănătății subiectului datelor cu caracter personal;

d) executarea sarcinilor de interes public sau care rezultă din exercitarea prerogativelor de autoritate publică cu care este investit operatorul sau terțul căruia îi sunt dezvăluite datele cu caracter personal;

e) realizarea unui interes legitim al operatorului sau al terțului căruia îi sunt dezvăluite datele cu caracter personal, cu condiția ca acest interes să nu prejudicieze interesele sau drepturile și libertățile fundamentale ale subiectului datelor cu caracter personal;

f) scopuri statistice, de cercetare istorică sau științifică, cu condiția ca datele cu caracter personal să rămână anonime pe toată durata prelucrării.

23. Prelucrarea categoriilor speciale de date cu caracter personal este interzisă, cu excepția cazurilor în care:

a) subiectul datelor cu caracter personal și-a dat consimțământul. În cazul incapacității de exercițiu sau al capacității de exercițiu limitate a subiectului datelor cu caracter personal, prelucrarea categoriilor speciale de date cu caracter personal se efectuează numai cu obținerea consimțământului în formă scrisă al reprezentantului lui legal;

b) prelucrarea este necesară pentru îndeplinirea obligațiilor sau drepturilor specifice ale operatorului în domeniul dreptului muncii, cu respectarea garanțiilor prevăzute de lege și ținându-se cont de faptul că o eventuală dezvăluire către un terț a datelor cu caracter personal prelucrate în acest scop poate fi efectuată numai dacă există o obligație legală a operatorului în acest sens;

c) prelucrarea este necesară pentru protecția vieții, integrității fizice sau a sănătății 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-și da consimțământul;

d) prelucrarea este efectuată în contextul activităților legitime de către asociații obștești, partide și alte organizații social-politice, de către sindicate, asociații de patronat, organizații filozofice sau religioase, organizații cooperatiste necomerciale, cu condiția ca prelucrarea să se refere numai la membrii acestora sau la persoanele cu care acestea au contacte permanente în legătură cu scopurile lor și cu condiția ca datele să nu fie dezvăluite terților fără consimțământul subiecților datelor cu caracter personal;

e) prelucrarea se referă la date făcute publice în mod voluntar și manifest de către subiectul datelor cu caracter personal;

f) prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept injustiție al subiectului datelor cu caracter personal;

g) prelucrarea este necesară în scopul asigurării securității statului, cu condiția ca aceasta să se efectueze cu respectarea drepturilor subiectului datelor cu caracter personal și a celorlalte garanții prevăzute de prezenta lege.

24. Colectarea datelor cu caracter personal pentru realizarea activităților prevăzute la art. 8 al Legii nr. 133 din 08 iulie 2011 privind protecția datelor cu caracter personal, se efectuează de către personalul subdiviziunilor IMSP INN

„Diomid Gherman” (beneficiari ai datelor cu caracter personal) numai în scopul îndeplinirii atribuțiilor de serviciu.

25. Prelucrarea datelor cu caracter personal referitoare la măsuri procesuale de constrângere sau sancțiuni contravenționale poate fi efectuată numai de către sau sub controlul autorităților publice, în limitele competențelor acordate și în condițiile 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 funcție de identificare de aplicabilitate generală poate fi efectuată în următoarele condiții:

- 1) subiectul datelor cu caracter personal și-a dat consimțământul;
- 2) prelucrarea este prevăzută în mod expres de legislație.

27. Informația ieșită din sistem, care conține date cu caracter personal, se marchează, indicându-se prescripții pentru prelucrarea ulterioară și răspândirea acesteia, inclusiv indicându-se numărul de identificare unic al deținătorului de date cu caracter personal.

28. Condițiile și termenele de stocare a datelor cu caracter personal se stabilesc de legislație ținându-se cont de prevederile art. 4 alin. 1 lit. e) al Legii nr. 133 din 08 iulie 2011 privind protecția 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 operațiunilor de prelucrare a datelor cu caracter personal, dacă subiectul acestor date nu și-a dat consimțământul pentru o altă destinație sau pentru o prelucrare ulterioară, acestea vor fi:

- 1) distruse; 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;
- 2) 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, conform anexei nr.5 a prezentei Politici;

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 subdiviziunile IMSP INN „Diomid Gherman” 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 convenite, 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 IMSP INN, în calitate sa de operator și structurile IMSP INN „Diomid Gherman”, în calitate a acestora de persoane împuternicite de către operator trebuie să conțină datele de identificare a solicitantului, precum și motivarea și scopul cererii, conform prevederilor legale sau obligațiilor cuprinse în tratate la care Republica Moldova este parte.

40. Cererile care nu conțin elementele prevăzute la pct.39 se restituie pentru completare, iar cele care nu se încadrează în condițiile prevăzute de lege

sau de tratatele la care Republica Moldova este parte se resping, menționându-se motivele pentru care dezvăluirea datelor cu caracter personal nu este posibilă.

41. Înainte de dezvăluirea datelor cu caracter personal, subdiviziunile IMSP INN verifică dacă acestea sunt exacte și, dacă este cazul, actualizate.

42. În situația în care se constată că au fost transmise date incorecte sau neactualizate, subdiviziunile IMSP INN „Diomid Gherman” au obligația de a informa destinatarii respectivelor date asupra neconformității acestora, cu menționarea datelor care au fost modificate.

43. La dezvăluirea datelor cu caracter personal subdiviziunile IMSP INN „Diomid Gherman” atenționează destinatarii asupra interdicției de a prelucra datele pentru alte scopuri decât cele specificate în cererea de dezvăluire.

V.DREPTURILE ȘI OBLIGAȚIILE UTILIZATORULUI/BENEFICIARULUI

44. Utilizatorul/beneficiarul este în drept:

1) să obțină acces la sistemele de evidență a datelor cu caracter personal necesare pentru exercitarea obligațiilor;

2) să beneficieze de utilaj și de asigurarea de program a accesului la sistemele de evidență 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 și să respecte prevederile actelor legislative și normative din domeniul prelucrării datelor cu caracter personal, la nivelul IMSP INN „Diomid Gherman” ;

2) să aplice nume login, care poartă un caracter secret și nu poate fi divulgat;

3) să respecte 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 maximum 3 luni;

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

4) să întreprindă măsurile tehnice și organizatorice necesare pentru

protecția datelor cu caracter personal împotriva accesului ilicit sau întâmplător, distrugerii, modificării, blocării, copierii, răspândirii, precum și a altor acțiuni ilicite din partea unor terțe persoane;

5) să păstreze confidențialitatea datelor prelucrate, a contului de utilizator, parolei/codului de acces la sistemele de evidență a datelor cu caracter personal;

6) să respecte măsurile de securitate prevăzute de legislația în vigoare, precum și celelalte reguli stabilite de operatorul sau persoanele împuternicite de către operator, conducerea IMSP INN „Diomid Gherman”, inclusiv cele stabilite de către administrator;

7) să informeze imediat conducătorul nemijlocit sau, după caz, administratorul despre circumstanțele ce prezintă semne a riscului de acces ilicit sau întâmplător, distrugere, modificare, blocare, copiere, răspândire, precum și a altor acțiuni ilicite a datelor cu caracter personal sau despre orice situație 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 condițiile legii, cu privire la: identitatea operatorului, scopul în care se face prelucrarea datelor, destinarii sau categoriile de destinatari ai datelor, obligativitatea furnizării tuturor datelor cerute și consecințele refuzului de a le pune la dispoziție, drepturile prevăzute de lege, în special drepturile de acces, de intervenție asupra datelor și de opoziție, condițiile în care pot fi exercitate aceste drepturi, respectiv să ofere orice alte informații a căror furnizare este impusă prin normele Legii nr. 133 din 08 iulie 2011 privind protecția datelor cu caracter personal;

9) să prelucreze numai datele cu caracter personal necesare îndeplinirii atribuțiilor de serviciu și să acorde sprijin conform actelor normative persoanei/subdiviziunii de protecție a datelor cu caracter personal din cadrul IMSP INN „Diomid Gherman” și/sau reprezentanților CNPDCP, conform competențelor acestora.

46. Atribuțiile specifice ale utilizatorului/beneficiarului se stabilesc obligatoriu și în fișa postului.

47. La acordarea accesului la sistemele de evidență a datelor cu caracter personal, utilizatorul semnează declarație de modelul stabilit pe proprie răspundere privind respectarea normelor de protecție a acestor date, în două exemplare, anexa nr.4.

Un exemplar se înregistrează în serviciu proiecte, protocol și secretariat IMSP INN „Diomid Gherman” unde activează utilizatorul și se anexează la demersul adresat administratorului, al doilea exemplar se anexează în dosarul personal.

48. La nivelul oricărui utilizator/beneficiar se instituie Registrul de evidență a interpelărilor (cusut, sigilat, numerotat și înregistrat în serviciu proiecte, protocol și secretariat IMSP INN „Diomid Gherman”), unde se duce evidența tuturor interpelărilor, care va conține obligatoriu următoarele rubrici:

- 1) locul stocării purtătorilor de date cu caracter personal;
- 2) sistemul de evidență în care au fost prelucrate datele cu caracter personal, proprietarul/gestionarul/deținătorul;
- 3) numărul de ordine a interpelării (raportului);
- 4) numărul și data înregistrării (raportului) în registru;
- 5) subdiviziunea care a solicitat informația;
- 6) volumul concret al datelor cu caracter personal supuse prelucrării;
- 7) numele și semnătura angajatorului care a executat interpelarea;
- 8) numele și, în cazul ridicării răspunsului personal – semnătura colaboratorului care a recepționat informația;
- 9) volumul documentului eliberat (numărul paginilor, filelor, copiilor) și rezultatul eliberării pozitiv sau negativ;
- 10) adnotare.

49. Conducătorii subdiviziunilor IMSP INN „Diomid Gherman”, 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 IMSP INN „Diomid Gherman” (operator) și structurile IMSP INN „Diomid Gherman” (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 uşile exterioare şi ferestrele amplasate în locuri accesibile. Utilajul de rezervă şi suporturile copiilor de rezervă ale masivelor informaţionale se păstrează în locuri îndepărtate de utilajul principal şi care permit evitarea distrugerilor sau deteriorărilor ca rezultat al calamităţilor.

6.4 Controlul vizitatorilor

54. Datele sistemului automatizat de înregistrare a permiselor vizitatorilor institutului se păstrează timp de un an. Vizitatorii încăperilor în care se efectuează prelucrarea datelor cu caracter personal vor fi însoţiţi de către angajaţii institutului, desemnaţi 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 şi documentele ce se conţin în registrul supus lichidării se transmit în arhivă.

6.5 Securitatea electroenergetică

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

În cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, va fi asigurată posibilitatea deconectării electricităţii 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 reţea

56. Cablurile de reţea vor fi protejate contra conectărilor neautorizate pentru o perioadă îndelungată. Cablurile de reţea cu destinaţie 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 antiincendiară 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 incendiară, inclusiv sisteme automatizate de depistare/semnălizare 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

autorizați în conformitate cu Politica în vigoare.

Angajații subdiviziunii responsabile/administratorul responsabil de realizarea Politicii vor efectua controlul mijloacelor software, mijloacelor hardware și celor software/hardware, instalate la locurile de muncă (computerele) ale angajaților ministerului.

Informația, ce conține date cu caracter personal, amplasată pe purtătorii de informație, se distruge împreună cu purtătorul sau se înlătură de pe purtător prin metode, care exclud restabilirea ulterioară.

6.9 Măsurile generale de administrare a securității informaționale

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

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

VII. AUDITUL SECURITĂȚII ÎN SISTEMELE DE EVIDENȚĂ A DATELOR CU CARACTER PERSONAL

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

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

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

- a) data și timpul tentativei
- b) ID-ul utilizatorului/beneficiarului;
- c) rezultatul tentativei de intrare/ieșire pozitivă sau negativă.

2) este efectuată înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative și proceselor, destinate prelucrării datelor cu caracter personal, înregistrarea modificărilor drepturilor de acces ale utilizatorilor/beneficiarilor și statutul obiectelor de acces conform următorilor parametri:

- a) data și 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 obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:

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

4) este efectuată înregistrarea modificărilor drepturilor de acces (competențelor) utilizatorului/beneficiarului și statutului obiectelor de acces, conform următorilor parametri:

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

5) 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:

- a) data și timpul eliberării;
- b) denumirea informației și căile de acces la aceasta;
- c) specificarea echipamentului (dispozitivului) care a eliberat informația (numele logic);
- d) ID-ul utilizatorului/beneficiarului, care a solicitat informația;
- e) volumul documentului eliberat (numărul paginilor, a fișierelor, copiilor) și rezultatul eliberării — pozitiv sau negativ.

62. Subdiviziunea/Persoana responsabilă de realizarea Politicii de securitate, precum și alte subdiviziuni împuternicite cu funcții corespunzătoare vor efectua monitorizarea permanentă și analiza înregistrărilor de audit, în scopul:

- a) depistării cazurilor de acces ilegal la datele cu caracter personal (încălcarea obligațiilor funcționale sau a condițiilor contractului);
- b) depistarea cazurilor de încălcare a procedurii de acces la datele cu caracter personal, inclusiv fără consimțământul subiectului;
- c) depistarea 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 acțiunilor menționate va fi informată administrația INN, va fi desfășurată cercetarea de serviciu și vor fi întreprinse măsuri de preîntâmpinare a unor astfel de cazuri.

64. Potrivit rezultatelor monitorizării și analizei înregistrărilor de audit, o dată pe semestru, se întocmește un raport privind funcționarea sistemelor de prelucrare a datelor cu caracter personal și, în caz de necesitate, vor fi întreprinse acțiuni de ameliorare a funcționării sistemelor de prelucrare datelor cu caracter personal.

VIII. MODALITATEA DE CONECTARE /DECONECTARE A UTILIZATORILOR ȘI BENEFICIARILOR DATELOR CU CARACTER PERSONAL LA SISTEMELE DE EVIDENȚĂ A DATELOR CU CARACTER PERSONAL

65. Accesul la informația din sistemele de evidență a datelor cu caracter personal pentru utilizatorul datelor cu caracter personal (în continuare utilizator) se acordă de către administrator în baza demersului oficial, cu specificarea numărului necesar de locuri automatizate de muncă, categoriile de informații la care se permite accesul conform atribuțiilor de serviciu și a datelor personale ale utilizatorului (NPP, IDNP, data nașterii, funcția deținută și telefonul de contact).

66. Accesul beneficiarului datelor cu caracter personal (în continuare - beneficiar) la informația din sistemele de evidență a datelor cu caracter personal ale altor operatori sau persoane împuternicite de către operator se efectuează în baza contactului/acordului încheiat în care sunt specificate categoriile de informații la care se permite accesul între deținătorul sistemului de evidență a datelor cu caracter personal și IMSP INN „Diomid Gherman”. La solicitarea conducătorului subdiviziunii IMSP INN „Diomid Gherman”, accesul la informația din sistemele de evidență a datelor cu caracter personal pentru beneficiar se acordă de către subdiviziunea IMSP INN căreia conducerea IMSP INN „Diomid Gherman” i-a delegat atribuțiile corespunzătoare de administrator (Grupul tehnologii informaționale a Secției monitorizare, evaluare și integrare), pe baza demersului oficial, cu specificarea numărului necesar de locuri automatizate de muncă, categoriile de informații la care se permite accesul și a datelor personale ale utilizatorului (NPP, IDNP, data nașterii, funcția deținută și telefonul de contact).

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

68. Funcționarea sistemului de evidență este suspendată de către administrator în următoarele cazuri:

- 1) în timpul efectuării lucrărilor profilactice ale complexului de mijloace software și hardware ale Sistemului;
- 2) la apariția circumstanțelor de forță majoră;
- 3) la încălcarea sistemului securității de evidență, dacă aceasta prezintă

pericol pentru funcționarea sistemului;

4) în cazul suspendării serviciilor;

5) în caz de retragerea sistemului din exploatare.

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

70. În cazul apariției circumstanțelor de forță majoră, precum și al dificultăților tehnice în funcționarea complexului de mijloace software și hardware ale sistemului de evidență din vina terțelor persoane, este posibilă suspendarea funcționării sistemului de evidență cu notificarea ulterioară a utilizatorilor și beneficiarelor conectați.

71. Revocarea dreptului de acces la sistemul de evidență de date cu caracter personal pentru utilizatori și beneficiari se efectuează în una dintre următoarele situații:

1) în temeiul cererii (demersului) conducătorului acestuia;

2) la intervenirea modificărilor raporturilor de muncă/de serviciu, iar noile atribuții nu impun accesul la datele sistemului de evidență;

3) la încetarea raporturilor de muncă/de serviciu ale utilizatorului și beneficiarului;

4) deconectarea se efectuează în mod automat, în cazul lipsei de activitate în decurs de 2 luni;

5) în cazul încetării sau rezilierii contractului/acordului;

6) la constatarea încălcării de către utilizator sau beneficiar a măsurilor securității informaționale a sistemului de evidență.

IX. ASIGURAREA INTEGRITĂȚII INFORMAȚIEI ȘI SISTEMELOR DE PRELUCRARE A DATELOR CU CARACTER PERSONAL

9.1 Introducerea modificărilor de soft destinat prelucrării datelor cu caracter personal

72. Elaborarea și 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 protecției contra programelor dăunătoare (virusurilor)

73. În sistemele de prelucrare a datelor cu caracter personal va fi asigurată protecția împotriva infiltrării programelor dăunătoare (virusurilor), precum și reînnoirea automată și la timp a mijloacelor de asigurare a protecției contra programelor dăunătoare și a signaturilor de virus.

Va fi asigurată administrarea centralizată a mecanismelor de protecție a soft-urilor.

9.3 Tehnologiile și mijloacele de constatare a tentativelor

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

9.4 Testarea posibilităților funcționale de asigurare a securității sistemelor de prelucrare a datelor cu caracter personal

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

X. COPIILE DE REZERVĂ ȘI RESTABILIREA INFORMAȚIEI

10.1 Copiile de rezervă ale informației care conține date cu caracter personal

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

10.2 Serviciile telecomunicaționale de rezervă

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

Furnizorii serviciilor telecomunicaționale de bază și de rezervă vor fi diferiți.

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 reorganizării IMSP INN „Diomid Gherman” sau a schimbării statelor de personal și a infrastructurii.

XII. MODUL DE ORGANIZARE ȘI REALIZARE A MĂSURILOR DE INFORMARE ASUPRA OPERAȚIUNILOR DE PRELUCRARE A DATELOR CU CARACTER PERSONAL

81. Structurile și subdiviziunile IMSP INN „Diomid Gherman” care efectuează operațiuni de prelucrare a datelor cu caracter personal în conformitate cu Legea nr.133 din 08 iulie 2011 privind protecția datelor cu caracter personal (în continuare — subdiviziunile IMSP INN „Diomid Gherman” abilitate) vor respecta prevederile și restricțiile stabilite în Lege, precum și 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, inclusiv:

art.4 alin.(1)

- 1) prelucrate în mod corect și conform a prevederilor legii;
- 2) colectate în scopuri determinate, explicite și 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 științifică nu este considerată incompatibilă cu scopul colectării dacă se efectuează cu respectarea prevederilor prezentei legi, inclusiv privind notificarea către Centrul Național pentru Protecția Datelor cu Caracter Personal, și cu respectarea garanțiilor privind prelucrarea datelor cu caracter personal, prevăzute de normele ce reglementează activitatea statistică, cercetarea istorică și cea științifică;
- 3) adecvate, pertinente și neexcesive în ceea ce privește scopul pentru care sunt colectate și/sau prelucrate ulterior;
- 4) exacte și, dacă este necesar, actualizate. Datele inexacte sau incomplete din punctul de vedere al scopului pentru care sunt colectate și ulterior prelucrate se șterg sau se rectifică;
- 5) stocate într-o formă care să permită identificarea subiecților datelor cu caracter personal pe o perioadă care nu va depăși durata necesară atingerii scopurilor pentru care sunt colectate și ulterior prelucrate.

art.12 alin.(1) și (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 informații, exceptând cazul în care acesta deține deja informațiile respective:

- a) identitatea operatorului sau, după caz, a persoanei împuternicite de către operator;
- b) scopul prelucrării datelor colectate;
- c) informații suplimentare, precum:
 - destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
 - existența drepturilor de acces la date, de intervenție asupra datelor și de opoziție, precum și condițiile în care acestea pot fi exercitate;

• dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sunt obligatorii sau voluntare, precum și consecințele 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 intenționează dezvăluirea acestora către terți, cel mai târziu în momentul primei dezvăluiri, să furnizeze subiectului datelor cu caracter personal informația privind categoriile de date care urmează a fi colectate sau dezvăluite, precum și informațiile indicate la alin.(1), cu excepția pct.3) lit.c).

art. 13

1) orice subiect al datelor cu caracter personal are dreptul să obțină de la operator, la cerere, fără întârziere și în mod gratuit:

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

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

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

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

e) informații privind modul de exercitare a dreptului de intervenție asupra datelor cu caracter personal.

art.14

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

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

b) notificarea terților cărora le-au fost dezvăluite datele cu caracter personal despre operațiunile efectuate conform lit.a), exceptând cazurile când această notificare se dovedește a fi imposibilă sau presupune un efort disproporționat față de interesul legitim care ar putea fi lezat.

art. 28

1) în scopul evidenței prelucrărilor de date cu caracter personal, CNPDCP instituie și administrează un registru de evidență al operatorilor de date cu caracter personal care trebuie să cuprindă informațiile stabilite la art. 23 alin. (2). Orice modificare a informațiilor respective va fi comunicată Centrului în termen

de 5 zile, care va efectua mențiunile corespunzătoare în registrul de evidență al operatorilor de date cu caracter personal.

2) registrul de evidență al operatorilor de date cu caracter personal este deschis spre consultare publicului, cu excepția compartimentului care conține informații privind măsurile de securitate și de asigurare a confidențialității.

Înregistrarea operatorilor, precum și a modificărilor informațiilor înscrise în registrul de evidență al operatorilor de date cu caracter personal, se efectuează gratuit.

XIII. SISTEME DE EVIDENȚĂ ÎN CARE SUNT STOCATE INFORMAȚII CU DATE CU CARACTER PERSONAL

82. În cadrul IMSP INN „Diomid Gherman” informațiile care conțin date cu caracter personal se prelucrează manual, automat și mixt. Sistemele informaționale de date cu caracter personal sunt de evidență administrativă, economico-financiară, contabilă, de personal și petiții.

83. Sisteme informaționale automatizate de prelucrarea a informațiilor care conțin date cu caracter personal gestionate:

1) SIA Asistența Medicală Spitalicească conține date cu caracter personal, a pacienților care sunt examinați și tratați în secțiile clinice și serviciile medicale complementare în cadrul IMSP INN „Diomid Gherman”;

2) SIA „Manager transfuzii sânge” conține date cu caracter personal al pacienți din secțiile spitalicești și are ca scop înregistrarea primirii și administrării activităților de transfuzii a componentilor sanguini;

3) SIA „Transplant” conține date cu caracter personal a donatorilor potențiali de țesuturi și organe de origine umană;

4) Sistemul electronic „Programul automatizat de evidență contabilă IC”. Sistemul conține date cu caracter personal și are ca scop remunerarea personalului IMSP INN „Diomid Gherman”;

5) Sistemul electronic de evidență a resurselor umane „SIRIUS” conține date cu caracter personal a angajaților și are ca scop evidență a acestora în IMSP INN „Diomid Gherman” ;

84. Protecția datelor cu caracter personal în sistemele informaționale 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.

85. Sunt supuse protecției toate resursele informaționale ale deținătorilor de date cu caracter personal, care conțin date cu caracter personal, inclusiv:

1) suporturile magnetice, optice, laser sau alte suporturi ale informației electronice, masive informaționale și baze de date;

2) sistemele informaționale, rețelele, sistemele operaționale, sistemele de gestionare a bazelor de date și alte sistemele de telecomunicații, inclusiv mijloacele de confecționare și multiplicare a documentelor și alte mijloace tehnice de prelucrare a informației.

86. Protecția datelor cu caracter personal în sistemele informaționale de date cu caracter personal este asigurată în scopul:

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

2) preîntâmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în rețelele telecomunicaționale și resursele informaționale;

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

4) asigurării caracterului complet, integru, veridic al datelor cu caracter personal în rețelele telecomunicaționale și resurselor informaționale;

5) păstrării posibilităților de gestionare a procesului de prelucrare și păstrare a datelor cu caracter personal.

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

1) preîntâmpinarea conexiunilor neautorizate la rețelele telecomunicaționale și interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste rețele;

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

3) preîntâmpinarea acțiunilor speciale tehnice și de program, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program;

4) preîntâmpinarea acțiunilor intenționate și/sau neintenționate a utilizatorilor interni și/sau externi, precum și a altor angajați ai deținătorului de date cu caracter personal, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program.

88. Preîntâmpinarea scurgerii de informații care conțin date cu caracter personal, transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informații, inclusiv cu utilizarea măsurilor organizaționale, tehnice și de regim.

89. Preîntâmpinarea accesului neautorizat la informațiile care conțin date cu caracter personal și circulă sau se păstrează în mijloace tehnice este asigurată prin metoda folosirii mijloacelor speciale tehnice și de program, cifrării acestor informații, inclusiv prin măsurile organizaționale și de regim.

90. 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.

91. Ordinea de acces la informația care conține date cu caracter personal, prelucrată în cadrul sistemelor informaționale, se stabilește de către operator, în conformitate cu prevederile legislației.

XIV. RESPONSABILITĂȚI

92. Conducătorul utilizatorului/persoana împuternicită, de comun cu administratorul (Grupul tehnologii informaționale a Secției monitorizare, evaluare și integrare), care dispune de acces la sistemele de evidență a datelor cu caracter personal are următoarele responsabilități:

1) să asigure susținerea funcționării computerelor care fac parte din sistemele de evidență a datelor cu caracter personal;

2) să asigure mijloacele tehnice de blocare a fișierelor automatizate, dacă utilizatorul/beneficiarul nu acționează asupra datelor afișate pe ecran o perioadă de timp de până la 15 minute, stabilită în funcție de operațiile care trebuie executate;

3) să efectueze controlul plenitudinii și veridicității demersurilor (interpelărilor, rapoartelor) privind eliberarea informației din sistemele de evidență a datelor cu caracter personal.

93. Utilizatorul/beneficiarul și persoana care a interceptat informația din sistemele de evidență a datelor cu caracter personal poartă răspundere pentru asigurarea securității și protecției informației acumulate, neexecutarea sau executarea necorespunzătoare a obligatiilor prevăzute în prezenta Politică.

94. Conducătorul structurilor/subdiviziunii IMSP INN „Diomid Gherman” care este conectată la sistemele de evidență a datelor cu caracter personal dispun măsurile necesare în vederea instituirii și menținerii unui nivel suficient de securitate a prelucrării datelor cu caracter personal, care vor consta cel puțin în:

1) interzicerea instalării de către personalul IMSP INN „Diomid Gherman” a altor programe software în afara celor configurate de personalul autorizat, pentru îndeplinirea atribuțiilor de serviciu;

2) configurarea porturilor de acces la mediile de stocare pentru fiecare stație de lucru și a comenzilor care permit salvarea documentelor, în mod adecvat, pentru categoriile de operațiuni efectuate de fiecare utilizator/beneficiar, în strictă legătură cu îndeplinirea atribuțiilor de serviciu ale acestuia;

3) implementarea unor aplicații automate de contracarare a vulnerabilităților și amenințărilor informatice și de securitate a sistemelor informatice.

95. Toate documentele care conțin date cu caracter personal se înregistrează și urmează regulile de păstrare, procesare, multiplicare, transportare, transmitere, distrugere și arhivare stabilite prin acte normative.

96. Structurile/subdiviziunile care prelucrează date cu caracter personal au obligația să transmită Administratorului (Grupul tehnologii informaționale a Secției monitorizare, evaluare și integrare), anual, către 31 decembrie, raportul despre incidentele de securitate a sistemelor de evidență a datelor cu caracter personal.

97. Anual, către 31 ianuarie, Administratorul prezintă Centrului Național

pentru Protecția Datelor cu Caracter Personal raportul generalizat despre
incidentele de securitate a sistemelor de evidență a datelor cu caracter personal
produse.

Director

A handwritten signature in black ink, consisting of several loops and a long, sweeping tail, positioned between the title 'Director' and the name 'Grigore ZAPUHLÎH'.

Grigore ZAPUHLÎH

Ex. Iurii Vacari

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 identității sale fizice, fiziologice, psihice, economice, culturale sau sociale, se împart în două categorii: **obișnuite și speciale**.

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

3. **Categoria obișnuită** o constituie informația care dezvăluie:

- 1) numele și prenumele;
- 2) sexul;
- 3) data și locul nașterii;
- 4) cetățenia;
- 5) IDNP;
- 6) imaginea;
- 7) situația familială;
- 8) situația militară;
- 9) datele personale ale membrilor de familie;
- 10) datele din certificatul de înmatriculare;
- 11) datele privind bunurile deținute;
- 12) datele bancare;
- 13) semnătura;
- 14) datele din actele de stare civilă;
- 15) codul personal de asigurării sociale (CPAS);
- 16) codul asigurării medicale (CPAM);
- 17) numărul de telefon/fax;
- 18) numărul de telefon mobil;
- 19) adresa (domiciliului/sediului);
- 20) adresa e-mail;
- 21) profesia și/sau locul de muncă;
- 22) formarea profesională — diplome studii;

**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.

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

Atenție! Documentul conține date cu caracter personal, prelucrate în conformitate cu prevederile Legii nr. 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 care nu va fi în nici un fel răspunzătoare pentru nici un fel de daune, indiferent de natura acestora, rezultând din erori de transmitere, viruși, influența externă, întârzieri sau alte cauze similare.

DECLARAȚIE DE CONFIDENȚIALITATE

din data de _____

În conformitate cu prevederile Legii nr.133 din 18.07.11 „Privind protecția datelor cu caracter personal”, 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, subsemnatul(ta) _____

(nume, prenume)

(funcția)

(secția/serviciul, instituția)

confirm, că sunt conștient de gradul de securitate a documentelor care conțin datele cu caracter personal, de riscurile aferente utilizării neadecvate acestora și mă angajez:

să respect condițiile impuse pentru protejarea informației primite de la IMSP Institutul de Neurologie și Neurochirurgie „Diomid Gherman”;

să păstrez în deplină confidențialitate respectiva informația;

să nu divulg către terți informația de care voi lua cunoștință în urma examinării documentelor vizate;

să nu utilizez această informație în alte scopuri decât cele anunțate la momentul solicitării.

Prezenta declarație este întocmită în 2(două) exemplare, câte un exemplar pentru fiecare parte.

(nume, prenume)

(semnătura)

Anexa nr.5
la ordinul INN,,”Diomid Gherman
nr. _____ din _____ 2019

**Consimțământul subiectului(pacientului)
pentru prelucrarea datelor cu caracter personal privind starea de sănătate, elaborat
conform art.7 din Legea privind protecția datelor cu caracter personal nr.133 din 08 iulie
2011.**

Eu, subsemnatul, _____ prin prezentul
îmi exprim consimțământul pentru ca **IMSP Institutul de Neurologie și Neurochirurgie** să prelucreze
datele mele cu caracter personal în scopul prestării serviciilor medicale, inclusiv stare mea de sănătate.

În caz de necesitate de a fi consultat de către medicii din instituție, sau de către medicii din alte
instituții medicale, consimt transmiterea datelor cu caracter personal privind starea mea de sănătate către
acești medici și aceste instituții în scopul consultului meu și în scopul examinării cererilor și petițiilor
depuse de mine.

**Și totodată menționez că am fost informat despre drepturile mele în calitate de subiect
de date cu caracter personal prevăzute de Legea nr.133 din 08 iulie 2011 privind protecția
datelor cu caracter personal.**

Semnat de mine personal (semnătura rudei sau tutelei).

Data _____

Semnătura _____

Data _____

Medicul curant _____

