**pentru aprobarea Conceptului Sistemului informațional**

**„Registrul de stat al datelor genetice” și a** **Regulamentului privind modul de ținere a Sistemului informațional „Registrul de stat al datelor genetice”**

**------------------------------------------------------------**

În temeiul art. 7 alin. (1) din Legea nr. 235/2017 cu privire la înregistrarea genetică judiciară (Monitorul Oficial al Republicii Moldova, 2017, nr. 441–450, art. 740) și art.16 alin. (1) al Legii nr. 71/2007 cu privire la registre (Monitorul Oficial al Republicii Moldova, 2007, nr. 70–73, art. 314), cu modificările ulterioare, Guvernul HOTĂRĂŞTE:

**1.** Se instituie „Registrul de stat al datelor genetice”.

**2.** Se aprobă:

1) Conceptul Sistemului informațional „Registrul de stat al datelor genetice”, conform anexei nr. 1;

2) Regulamentul privind modul de ținere a „Registrului de stat al datelor genetice”, conform anexei nr. 2.

**3.** Ministerul Afacerilor Interne, în calitate de posesor al sistemului informațional respectiv, va asigura condițiile juridice, financiare și organizatorice pentru crearea, administrarea, mentenanța și dezvoltarea Sistemului informațional „Registrul de stat al datelor genetice”.

**4.** Prevederile prezentei hotărâri se vor realiza din mijloacele Proiectului „Îmbunătățirea eficienței și accesului la justiție în Republica Moldova”, implementat de către Programul Națiunilor Unite pentru Dezvoltare, cu sprijinul financiar al Suediei, în conformitate cu legislația.

**5.** Controlul asupra executării prezentei hotărâri se atribuie Ministerului Afacerilor Interne.

**6.** Prezenta hotărâre intră în vigoare la data publicării în Monitorul Oficial al Republicii Moldova.

**Prim-ministru DORIN RECEAN**

Contrasemnează:

Viceprim-ministru,

ministrul dezvoltării economice și digitalizării Dumitru Alaiba

Ministrul afacerilor interne Adrian Efros

Ministrul sănătății Ala Nemerenco

Anexa nr. 1

la Hotărârea Guvernului nr.\_\_\_\_\_\_

din \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023

**CONCEPTUL**

**Sistemului informațional „Registrul de stat al datelor genetice”**

**I. INTRODUCERE**

Conform Proiectului „Îmbunătățirea eficienței și accesului la justiție în Republica Moldova”, implementat de către Programul Națiunilor Unite pentru Dezvoltare, cu sprijinul financiar al Suediei, una dintre componentele de bază rezidă sporirea eficienței serviciilor de justiție și la îmbunătățirea accesului la justiție a bărbaților și a femeilor din Moldova, în special din categoriile vulnerabile și marginalizate, prin capacități fortificate ale instituțiilor criminalistice de a presta servicii de justiție de calitate, capacități consolidate ale actorilor din sectorul de justiție în domeniile-pilot selecte pentru a asigura un răspuns coordonat nevoilor de justiție ale bărbaților și femeilor și o societate civilă consolidată care este în stare să ceară respectarea drepturilor și să se implice într-un dialog constructiv cu actorii lanțului de justiție. Intervențiile proiectului vor oferi șanse egale și vor încuraja participarea bărbaților și a femeilor.

O bază de date criminalistice cu materiale biologice privind acidul dezoxiribonucleic (*în continuare – ADN*) este importantă prin faptul că poate contribui la cercetarea infracțiunilor prin corelarea profilurilor ADN recoltate din urmele biologice care au legătură cu infracțiunea și cu ale donatorilor posibili (sau rudele acestora). În ultimii 20 de ani, bazele de date criminalistice ADN și-au demonstrat utilitatea în acest sens.

La etapa actuală, bazele de date naționale ADN servesc drept bază pentru investigațiile de rutină desfășurate de organele de poliție. Prin urmare, strategiile tradiționale de investigare adoptate de poliție sunt abandonate tot mai frecvent în favoarea abordării bazate pe ADN, în special, în cazurile când sunt disponibile urme biologice. O bază de date ADN oferă informații operative importante și contribuie la eliminarea bănuiților inocenți la o etapă precoce a anchetei.

Potrivit experienței internaționale anterioare, bazele de date ADN au ajutat să fie excluse mai multe persoane din anchetele conduse de organele de poliție decât au fost condamnate – o abordare și un instrument unic în procedurile aplicate de poliție. Utilizarea bazelor de date ADN poate preveni risipa de resurse prin concentrarea cercetării desfășurate de poliție asupra problemelor relevante. În acest mod sunt identificați mai rapid recidiviștii, fiind asigurată protecția victimelor potențiale viitoare. Suplimentar, victimele infracțiunii și rudele acestora se pot bucura de dreptate chiar și peste perioade îndelungate, dat fiind faptul că multe cauze pot fi soluționate peste mulți ani după ce a fost comisă infracțiunea.

Există o mare diversitate între țări referitoare la normele de incluziune a bănuiților și/sau a condamnaților din cauza sistemelor juridice diferite. Mai mult, se observă tendințe de adaptare a bazelor de date și a noilor strategii de cercetare cum ar fi căutarea familiei sau generarea de caracteristici fenotipice. Totuși, baza pentru crearea unui registru național ADN ar trebui să păstreze un echilibru corect între interesele sistemului de justiție de a pune sub urmărire penală agresorii și dreptul persoanelor la confidențialitatea datelor genetice.

Deși în ultimii ani au fost depuse eforturi importante la nivel național cu scopul de a spori eficiența, transparența, echitatea și accesibilitatea sectorului de justiție, se impune o îmbunătățire suplimentară pentru a asigura o coordonare coerentă între organele de drept, organele de securitate și instituțiile de justiție pentru administrarea eficace a justiției, astfel încât bărbații și femeile, în special din grupurile marginalizate sau minoritare, să-și poată revendica efectiv drepturile și accesul la justiție.

**II. DISPOZIȚII GENERALE**

**1.** Sistemul informațional „Registrul de stat al datelor genetice” (în continuare *– SI RSDG*) reprezintă totalitatea de resurse şi tehnologii informaționale interdependente, de metode şi de personal, destinată ținerii resursei informaționale cu privire la datele genetice, concepute să gestioneze și să analizeze profilurile ADN recoltate la locul faptei, de la bănuiți și din alte surse.

**2.** Baza de date criminalistice ADN este utilizată în:

1) anchete penale – baza de date poate fi utilizată pentru a identifica concordanța probei de ADN prelevate la locul faptei cu bănuiții sau a elimina persoane inocente în calitate de bănuiți. Acest mod ajută organele de drept să identifice și să decidă reținerea bănuiților/învinuiților, precum și să excludă din anchetă persoanele acuzate pe nedrept;

2) cauzele persoanelor dispărute – baza de date poate fi utilizată pentru a identifica persoanele dispărute prin contrapunerea profilurilor ADN prelevate de la membrii de familie cu rămășițele umane neidentificate. Aceasta poate ajuta familiile să găsească o încheiere și o soluționare a cauzei lor;

3) cercetarea cauzelor nedescoperite – baza de date poate fi utilizată pentru a soluționa cauzele vechi nedescoperite prin analizarea repetată a probelor și compararea lor cu profilurile ADN din baza de date. Aceasta poate ajuta să fie adusă o încheiere și dreptate victimelor și familiei lor;

4) prelevarea mostrei de la infractorul condamnat – baza de date poate fi utilizată pentru a stoca profilurile ADN ale infractorilor condamnați, care pot fi comparate cu probele de ADN aferente infracțiunilor nedescoperite pentru a identifica potențiali bănuiți.

5) identificarea persoanei – baza de date poate fi utilizată pentru a identifica persoanele în cazurile când metodele tradiționale de identificare nu sunt posibile, în cazul anchetei dezastrelor în masă sau a infracțiunilor de război;

6) cercetare și dezvoltare – baza de date poate fi utilizată pentru cercetarea științifică și dezvoltare, precum identificarea unor marcheri ADN noi sau testarea corectitudinii și fiabilității metodelor de analiză ADN.

**3.** Obiectivul SI RSDG este digitalizarea fluxurilor de lucru în vederea stocării, gestionării și analizei profilurilor ADN generate din mostrele biologice colectate la locul faptei. Conceptul îi permite beneficiarului să conștientizeze modul în care vor fi îndeplinite necesitățile acestuia, iar dezvoltatorului soluției aplicative – ce componente urmează să fie dezvoltate și în conformitate cu ce principii.

**4.** La proiectarea, dezvoltarea și implementarea SI RSDG, în scopul asigurării realizării obiectivelor menționate, trebuie să se țină cont de următoarele principii:

1) *principiul legalității*, care presupune crearea și exploatarea SI RSDG în conformitate cu legislația națională, normele și standardele internaționale recunoscute în domeniu;

2) *principiul protecției datelor cu caracter personal*, care presupune că datele vor fi colectate, stocate și prelucrate în concordanță cu actele normative interne și cu tratatele internaționale la care Republica Moldova este parte în domeniul protecției datelor cu caracter personal;

3) *principiul accesibilității și partajării datelor* – care presupune că toți utilizatorii autorizați au acces la datele necesare pentru a-și îndeplini atribuțiile de serviciu – prin urmare, datele sunt partajate. Datele constituie fundamentul adoptării deciziei – procesului, prin urmare, acestea sunt gestionate în mod adecvat pentru ca să știm unde pot fi găsite, să fie corecte, fiind disponibile când și unde este nevoie;

4) *principiul autenticității datelor*, care presupune că obiectele informaționale ale SI RSDG corespund documentului original stocat în format digital sau pe suport de hârtie;

5) *principiul datelor sigure*, care presupune introducerea datelor în SI RSDG numai în baza înregistrărilor din documentele acceptate ca surse de informații de încredere și introducerea datelor în sistem doar prin canalele autorizate și autentificate;

6) *principiul identificării unice*, care presupune că oricărei copii a obiectului informațional îi este atribuit un cod unic de identificare la nivel de sistem, prin care acesta poate fi localizat și accesat;

7) *principiul aplicării bunelor practici și a standardelor din domeniu*, care asigură că soluția elaborată este modernă, are o fiabilitate ridicată deoarece se bazează pe experiența altor soluții similare și este compatibilă cu sistemele existente atât în țară, cât și peste hotare care respectă standardele din domeniu;

8) *principiul capabilității interoperabilității semantice*, care presupune că modelul de date al SI RSDG este aliniat din punct de vedere semantic și sintactic la nivel național și internațional. Sunt utilizate activele semantice comune promovate la nivel european și internațional pentru a defini vocabularul local;

9) *principiul alinierii cu TIC MAI la scară largă și arhitectura guvernamentală*, care presupune implicarea conformității fără rezerve cu principiile și arhitectura stabilite în cadrul arhitecturii la scară largă, precum arhitectura bazată pe servicii (SOA), interoperabilitatea, serviciile și componentele reutilizabile, portabilitatea, flexibilitatea etc.;

10) *independența tehnologiei*, care presupune că soluțiile aplicative trebuie să fie independente de opțiunile tehnologice specifice și, prin urmare, să poată opera pe o varietate de platforme tehnologice. Independența tehnologică permite dezvoltarea, actualizarea și operarea soluțiilor aplicative în cel mai eficient mod în timp util. În caz contrar, tehnologia, care este supusă îmbătrânirii continue și dependenței de furnizori, devine primordială în defavoarea cerințelor utilizatorilor;

11) *principiul extensibilității*, în conformitate cu care componentele SI RSDG oferă facilități pentru ajustarea și extinderea funcționalităților existente în vederea asigurării conformității cu necesitățile în permanentă schimbare;

12) *principiul dezvoltării progresive*, care presupune elaborarea sistemului și modificarea permanentă a componentelor acestuia sunt efectuate în concordanță cu TI avansate;

13) *principiul consecutivității*, care implică elaborarea și implementarea sistemului pe etape;

14) *principiul eficienței funcționării*, care implică optimizarea raportului calitate-cost;

15) *principiul auditului sistemului*, care implică înregistrarea informațiilor despre schimbările care au loc în sistem, pentru a fi posibil de reconstruit istoria unui document sau starea lui la o etapă anterioară;

16) *principiul simplității și comodității utilizării*, care presupune proiectarea și realizarea tuturor componentelor de program accesibile utilizatorilor SI RSDG, bazate pe principii exclusiv vizuale, ergonomice și logice de concepție;

17) *depozit exogen* – sistemul are capacitatea de a accesa și stoca date unice prin conectarea mai multor depozite de date. Conținutul este stocat și accesat din locul unde a fost creat. Modelul de date este gestionat în mod centralizat și există o singură politică de stocare. Nu există două date/depozite de date care să înregistreze aceleași informații și care nu comunică;

18) *principiul securității informaționale*, care presupune că informațiile sunt protejate pe baza integrității, disponibilității, confidențialității, incontestabilității și autenticității. Orice informații fac obiectul unei evaluări de securitate bazate pe acești 5 factori. Abordarea trasabilității în securitate include inițierea și aplicarea adecvată a sistemului de audit și a instrumentelor de monitorizare. Disponibilitatea schimbului de informații și dezvăluirea acestora ar trebui să fie echilibrată cu necesitatea de a limita disponibilitatea informațiilor confidențiale, brevetate și sensibile;

19) *principiul securității prin proiectare*, care este o abordare din dezvoltarea software și hardware care-și propune să facă sistemele cât mai libere posibil de vulnerabilități și impermeabile la atacuri cu ajutorul unor astfel de măsuri ca testarea continuă, garanții de autentificare și aderența la bunele practici de programare;

20) *principiul responsabilității personale*, care prevede răspunderea personală în concordanță cu legislația în vigoare a tuturor persoanelor care au acces la SI RSDG pentru acces, utilizare și diseminare neautorizată. În acest sens, accesul la date este personalizat și orice acțiune de utilizare a sistemului este jurnalizată cu aplicarea nerepudierii;

21) *principiul celor patru ochi* – cerința că 2 persoane aprobă unele acțiuni înainte de a fi desfășurate. Este aplicabil înregistrării datelor în SI RSDG.

**5.** Principiile care trebuie respectate atunci când se implementează confidențialitatea prin proiectare și confidențialitatea implicită:

1) minimizarea datelor, sistemele de prelucrare a datelor ar trebui să fie proiectate și selectate în concordanță cu scopul colectării și prelucrării a cât mai puține posibil date cu caracter personal;

2) capacitatea de control, sistemele informatice ar trebui să asigure subiecții datelor cu mijloace eficace de control în privința datelor cu caracter personal;

3) transparența, prin care dezvoltatorii și operatorii sistemelor informatice trebuie să asigure acele date;

4) sisteme ușor de folosit, funcțiile și facilitățile conexe confidențialității ar trebui să fie ușor de folosit, cu alte cuvinte, ar trebui să ofere asistență suficientă și interfețe simple de utilizat pentru utilizatorii cu mai puțină experiență;

5) confidențialitatea datelor, sistemele informatice ar trebui să fie concepute astfel încât numai entitățile autorizate să aibă acces la datele cu caracter personal;

6) calitatea datelor, controlorii datelor trebuie să susțină calitatea datelor prin mijloace tehnice. Date relevante ar trebui să fie accesibile, în funcție de necesitate, pentru scopuri legale;

7) limitarea utilizării, sistemele informatice care pot fi utilizate pentru diferite scopuri sau sunt operate într-un mediu cu mai mulți utilizatori trebuie să garanteze că datele și procesele ce servesc diferitor sarcini și scopuri pot fi segregate unele de celelalte într-un mod securizat.

**III. CADRUL NORMATIV AL SI RSDG**

**6.** Crearea și funcționarea SI RSDG este reglementat de actele normative din domeniul informatizării și al resurselor informaționale de stat, Regulamentul de organizare și funcționare a Centrului tehnico-criminalistic şi expertize judiciare al Inspectoratului General al Poliției al Ministerului Afacerilor Interne (în continuare – *CTCEJ*), inclusiv prevederile prezentei hotărâri, după cum urmează:

1) acte normative care reglementează domeniul expertizei genetice și judiciare:

a) Codul penal al Republicii Moldova nr. 985/2002;

b) Codul de procedură penală al Republicii Moldova nr. 122/2003;

c) Legea nr. 68/2016 cu privire la expertiza judiciară şi statutul expertului judiciar;

d) Legea nr. 235/2017 cu privire la înregistrarea genetică judiciară;

e) Legea nr. 77/2019 cu privire la ratificarea Acordului de implementare a Acordului dintre părțile Convenției privind cooperarea polițienească în Europa de Sud-est privind schimbul automatizat de date ADN, date dactiloscopice și date de înmatriculare a autovehiculelor;

f) Hotărârea Guvernului nr. 1310/2003 despre aprobarea Regulamentului cu privire la obținerea, evidența, păstrarea, sistematizarea şi utilizarea datelor dactiloscopice şi Listei funcțiilor deținute de persoanele supuse înregistrării dactiloscopice obligatorii.

g) Hotărârea Guvernului nr. 195/2017 privind aprobarea Nomenclatorului expertizelor judiciare;

h) Hotărârea Guvernului nr. 236/2020 pentru aprobarea Regulamentului privind gestionarea materialului biologic;

i) Regulamentul privind expertiza medico-legală a cadavrului, aprobat prin Ordinul Ministerului Sănătății din 24.02.1999.

2) acte normative care reglementează domeniul informatizării și al resurselor informaționale de stat:

a) Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat;

b) Legea nr. 71/2007 cu privire la registre;

c) Legea nr. 133/2011 privind protecția datelor cu caracter personal;

d) Legea nr. 305/2012 cu privire la reutilizarea informațiilor din sectorul public;

e) Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate;

f) Legea 124/2022 privind identificarea electronică și serviciile de încredere;

g) Hotărârea Guvernului nr. 562/2006 cu privire la crearea sistemelor şi resurselor informaționale automatizate de stat;

i) Hotărârea Guvernului nr. 1123/2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal;

j) Hotărârea Guvernului nr. 201/2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică;

k) Ordinul ministrului afacerilor interne nr. 247/2016 privind aplicarea practicilor de protecție a datelor cu caracter personal în cadrul implementării serviciilor de tehnologie a informației și comunicațiilor din cadrul MAI;

l) Ordinul ministrului afacerilor interne nr. 195/2016 privind implementarea practicilor centralizate de management al serviciilor de tehnologie a informației și comunicațiilor din cadrul MAI.

3) acte normative care reglementează activitatea Centrului tehnico-criminalistic şi expertize judiciare:

a) Legea nr. 320/2012 cu privire la activitatea Poliției și statutul polițistului;

b) Legea nr. 288/2016 privind funcționarul public cu statut special din cadrul Ministerului Afacerilor Interne;

c) Legea integrității nr. 82/2017;

d) Hotărârea Guvernului nr. 460/2017 pentru punerea în aplicare a prevederilor Legii nr. 288 din 16 decembrie 2016 privind funcționarul public cu statut special din cadrul Ministerului Afacerilor Interne;

e) Hotărârea Guvernului nr. 547/2019 cu privire la organizarea şi funcționarea Inspectoratului General al Poliției;

f) Ordinul ministrului afacerilor interne nr. 172/2020 privind aprobarea Regulamentului de organizarea şi funcționarea Centrului tehnico-criminalistic şi expertize judiciare al Inspectoratului General al Poliției;

**IV. SPAȚIUL FUNCȚIONAL AL SI RSDG**

**7.** Începând cu cerințele juridice cu privire la înregistrarea genetică, gestionarea registrului și aspectele specifice ale gestionării software, SI RSDG automatizează următoarele procese:

1) primirea și verificarea datelor din profilurile ADN de referință și a datelor cu caracter personal ale persoanei de la care a fost prelevat materialul biologic, în funcție de caz, profilul ADN neidentificat pentru înregistrare genetică;

2) activitatea de ținere a registrului include activități precum: înregistrarea inițială a obiectelor evidenței, operarea modificărilor în date și radierea obiectului din registru, de asemenea, furnizarea datelor;

3) arhivarea profilurilor ADN eliminate din SI RSDG și gestionarea arhivei;

4) compararea, căutarea și partajarea profilurilor ADN, a datelor privind persoanele și cauzele, inclusiv solicitarea de comparare a profilurilor ADN din partea partenerilor internaționali;

5) activități de administrare a soluției aplicative, inclusiv confidențialitatea datelor, rolul și gestionarea utilizatorului, auditul securității soluției aplicative.

**8.** În vederea automatizării proceselor de lucru, SI RSDG oferă următoarele funcții de bază:

1) formarea resursei informaționale – stocarea datelor, analiza datelor, căutarea datelor și radierea din evidență a obiectelor informaționale (schimbarea statutului profilurilor ADN). Acestea se realizează în funcție de îndeplinirea anumitor scenarii de bază, după cum urmează:

a) stocarea datelor – capacitatea de a stoca profiluri ADN, informații referitoare la mostre, informații referitoare la cauze și informații de identificare personală într-o manieră organizată și securizată;

b) analiza datelor – capacitatea de a analiza profiluri ADN și de a le compara pentru a identifica concordanțe potențiale între mostrele recoltate la locul faptei și bănuiți sau de a elimina persoanele inocente din categoria bănuiților;

c) căutarea datelor – capacitatea de a căuta în baza de date profiluri, cauze sau persoane concrete în baza criteriilor specificate;

d) radierea din evidență – înregistrările sunt radiate la solicitarea persoanei sau la expirarea termenului de păstrare. Solicitarea persoanei este verificată de registrator care ia decizia în conformitate cu cadrul normativ. Radierea automată este inițiată de sistem care notifică registratorul despre expirarea termenului de păstrare.

2) asigurarea multilaterală a funcționării SI RSDG – presupune interacțiunea și integrarea cu alte sisteme informaționale de stat sau servicii electronice guvernamentale, organe de drept și organizații autorizate, cum ar fi Sistemul combinat de index ADN al Biroului Federal de Investigații (FBI);

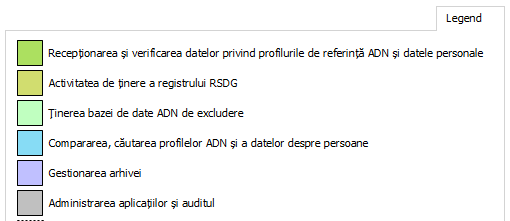
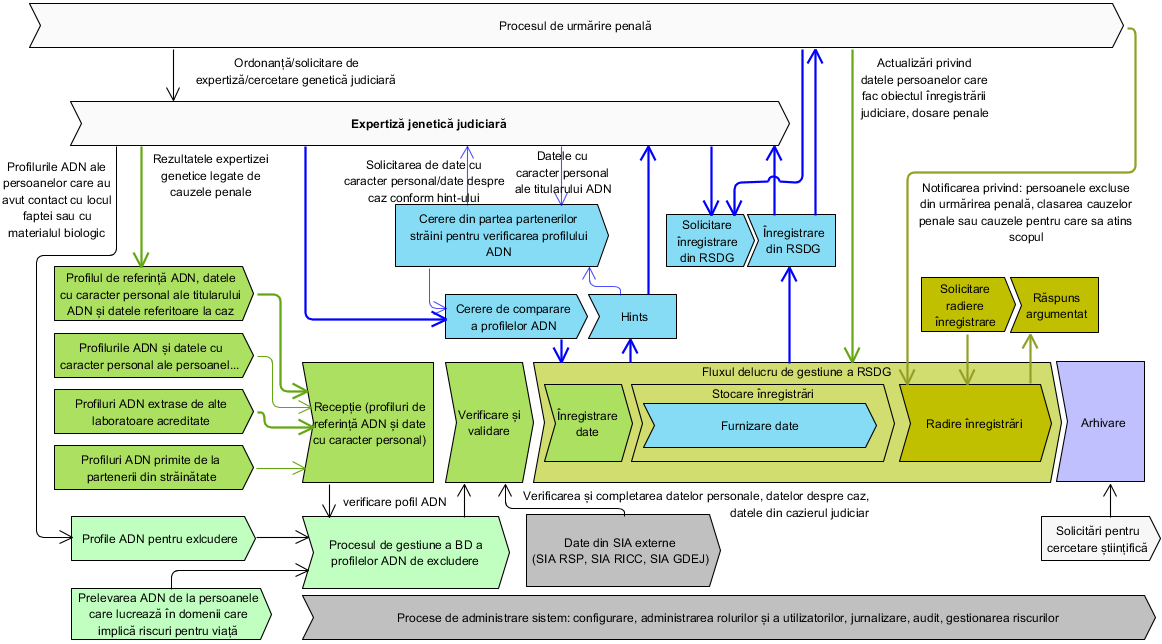
3) asigurarea securității și protecției informației – capacitatea de a proteja viața privată și confidențialitatea persoanelor ale căror profiluri ADN sunt stocate în baza de date, inclusiv utilizarea măsurilor de securitate precum controlul accesului, culoarele de audit și criptarea datelor sensibile;

4) raportarea – capacitatea de a generate rapoarte și analize statistice ale datelor stocate în baza de date, inclusiv numărul de profiluri, numărul de concordanțe și alte informații relevante;

5) arhivarea – capacitatea de a păstra profiluri ADN depersonalizate care au fost eliminate din RSDG;

6) asigurarea calității informației – se efectuează prin crearea și menținerea componentelor sistemului de calitate, bazate pe principul abordării de proces în conformitate cu cerințele standardului SM SR EN ISO 9001;

7) asigurarea multilaterală a funcționării SIGDEJ – presupune interacțiunea și integrarea cu alte sisteme informaționale de stat sau servicii electronice guvernamentale.



**Figura 1. Funcțiile de bază ale SI RSDG**

**9.** În cadrul funcționării SI RSDG se realizează funcții specifice, grupate în contururi funcționale speciale.

**10.** Conturul funcțional de interacțiune informațională a tuturor participanților sistemului „ADMINISTRAREA APLICAȚIEI” reprezintă un subsistem integrat de control și monitorizare a formării și utilizării resursei informaționale de gestiune a dosarelor de expertiză judiciară. Conturul include următoarele funcții:

1) asigurarea integrității logice a SI RSDG;

2) administrarea bazelor de date ale SI RSDG;

3) elaborarea și mentenanța ghidurilor de sistem și a clasificatoarelor;

4) delimitarea drepturilor de acces pentru utilizatori;

5) evidența rapoartelor de expertiză și a documentelor dosarelor;

6) asigurarea securității, protecției și integrității informației în SI RSDG conform cerințelor standardului național SM EN ISO/IEC 27001:2017 „Tehnologia informației. Tehnici de securitate. Sisteme de management al securității informației. Cerințe”;

7) asigurarea respectării cerințelor SI RSDG de protecție a datelor cu caracter personal.

**11.** Conturul funcțional „DOSAR DE EXPERTIZĂ” include funcții de evidență:

1) a solicitării de expertiză;

2) a obiectelor de expertizat;

3) a raportului de expertiză;

4) a notificării de refuz privind efectuarea expertizei;

5) a scrisorii de însoțire a raportului de expertiză;

6) a oricărei comunicări cu solicitantul sub formă de documente de intrare/ieșire;

7) a oricărui document care poate apărea pe parcursul desfășurării activității de expertiză.

**12.** Conturul funcțional „PARTICIPANȚI AI SISTEMULUI” include funcții de evidență:

1) a solicitanților de expertize;

2) a instituțiilor de expertiză judiciară;

3) a altor autorități/instituții implicate în activitatea de expertiză, după caz.

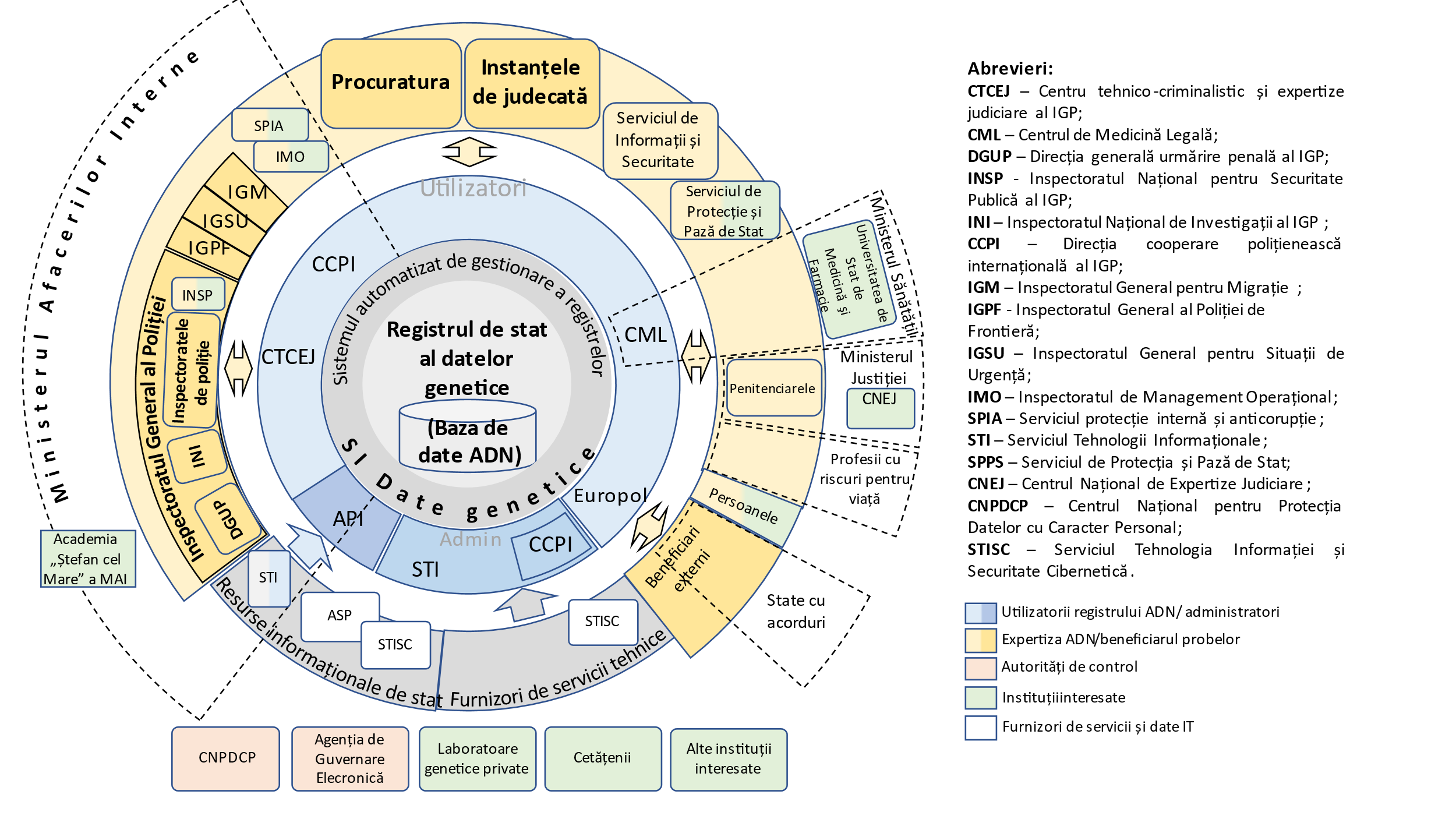
**13.** Conturul funcțional „DOCUMENTE” include funcții de evidență a documentelor care circulă în cadrul SI RSDG, după cum urmează:

1) documente de intrare;

2) documente tehnologice (inclusiv tehnice);

3) documente de ieșire.

**V. STRUCTURA ORGANIZAȚIONALĂ A SI RSDG**



**Figura 2. Părțile interesate ale SI RSDG**

**14.** Funcțiile de bază privind formarea și exploatarea SI RSDG sunt divizate între:

1) proprietarul sistemului;

2) posesorul sistemului;

3) deținătorul sistemului și administratorul tehnic al sistemului;

4) registratorii informației;

5) furnizorii de date;

6) utilizatorii datelor sistemului;

**15.** Proprietarul SI RSDG este statul, care își realizează dreptul de proprietate, gestionare și utilizare a datelor din acesta.

**16.** Posesorul SI RSDG este Ministerul Afacerilor Interne (în continuare – *MAI*) care:

1) asigură condițiile juridice, financiare și organizaționale pentru instituirea, administrarea, întreținerea și dezvoltarea sistemelor informaționale de stat;

2) desemnează și stabilește atribuțiile deținătorului, administratorului tehnic și ale destinatarilor sistemelor informaționale de stat și atribuțiile privind modul de ținere a SI RSDG.

**17.** Deținătorul și administratorul tehnic a SI RSDG este Serviciul Tehnologii Informaționale al MAI (în continuare – *STI*) care:

1) asigură totalitatea activităților de suport, mentenanță și dezvoltare continuă a SI RSDG;

2) administrează infrastructura tehnică (hardware și software), de întreținere și implementează politicile de securitate ale sistemului.

**18.** Utilizatorii datelor SI RSDG sunt:

1) registratorii;

2) furnizorii de date;

3) destinatarii.

**19.** Registratorii SI RSDG sunt:

1) Centrul tehnico-criminalistic şi expertize judiciare al Inspectoratului General al Poliției al MAI care dispune efectuarea expertizei genetice judiciare în cadrul laboratorului acreditat conform ISO 17025;

2) Centrul de Medicină Legală al Ministerului Sănătății în cadrul laboratorului acreditat conform ISO 17025, i se poate atribui rolul de sub-registrator, oferit de către posesor, pe bază contractuală, în vederea înregistrării rezultatelor investigațiilor genetice efectuate de acesta în SI RSDG;

3) punctele naționale de contact: Direcția cooperare polițienească internațională în calitate de Punct național de contact primar, care este responsabil de schimbul de date în lipsa conexiunii on-line, Centrul tehnico-criminalistic și expertize judiciare în calitate de Punct național de contact ADN, care este responsabil de confirmarea furnizării datelor personale pentru solicitări în cazul hit-urilor de contrapunere a pofilelor ADN, după caz de confirmarea hit-urilor.

**20.** În conformitate cu art. 8 din Legea nr. 235/2017 cu privire la înregistrarea genetică judiciară, persoanele și obiectele pasibile de înregistrarea genetică sunt:

1) Bază de date ADN a Interpol și portalul ADN – este un suport pentru transferul profilurilor ADN între două sau mai multe țări și pentru gestionarea profilurilor ADN proprii ale țării în baza de date ADN centrală. Accesul unei țări la portalul ADN este asigurat direct prin Birourile centrale naționale ale Interpol-ului, utilizând sistemul de comunicare securizat I-24/7.

2) Sistemul informațional Europol – este o bază de date centrală pentru informare în materie penală și pentru informații operative, care include toate domeniile infracționale acoperite de mandatul agenției. Acesta este un sistem de referință prin care se verifică dacă în alte state membre sunt disponibile informații privind o anumită persoană sau un anumit obiect de interes.

**21.** Furnizori de date pentru SI RSDG sunt instituțiile publice care livrează date în baza documentelor de reglementare pe domeniul de activitate, aferente obiectelor informaționale ale SI RSDG, care se realizează prin intermediul sistemului informațional deținut de ei, după cum urmează:

1) SIA al laboratoarelor acreditate conform ISO 17025 în domeniul expertizei genetice:

a) laboratorul CTCEJ;

b) Centrul de Medicină Legală al Ministerului Sănătății;

c) alte laboratoare acreditate conform ISO 17025.

2) SIA al autorităților abilitate să dispună înregistrarea genetică:

a) instanțele de judecată;

b) procuratura;

c) MAI și subdiviziunile din subordine abilitate cu competențe de urmărire penală (Inspectoratul General al Poliției, Inspectoratul General al Poliției de Frontieră, Serviciul protecție internă și anticorupție).

d) Administrația Națională a Penitenciarelor.

3) Cooperarea polițienească transfrontalieră

a) Punctul național de contact ADN poate furniza profile ADN și/sau informații adiționale despre cetățenii Republicii Moldova care figurează într-un dosar penal gestionat de un stat partener dacă acesta este subiect al înregistrării în RSDG. În calitate de Punct național de contact ADN sunt:

- Direcția de Cooperare Polițienească Internațională a IGP (DCPI) ca punct național de contact – este responsabilă de schimbul de date în lipsa conexiunii online;

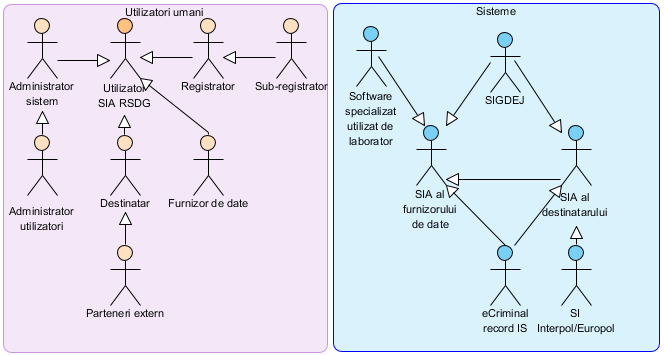
- CTCEJ în calitate de punct național de contact pentru ADN – este responsabilă cu confirmarea furnizării datelor detaliate (despre persoană, caz, etc.)în cazul hit-urilor și pentru confirmarea hit-urilor discutabile.

b) Instituțiile de poliție externă cu care Republica Moldova a semnat acorduri privind schimbul automat de date ADN vor avea acces la căutarea și compararea profilurilor ADN. Utilizatorii următoarelor canale de schimb stabilite conform acordurilor internaționale de cooperare polițienească pot fi utilizatori SI RSDG:

- Europol;

- Interpol.

**22.** Destinatarii SI RSDG sunt persoanele fizice și juridice mandatate conform legislației să primească datele conținute în RSDG.



**Figura 3. Utilizatorii SI RSDG**

**VI. DOCUMENTELE** **SI RSDG**

**24.** În cadrul SI RSDG se folosesc următoarele categorii de documente:

1) documente de intrare, care sunt fundamentale pentru introducerea datelor în sistem;

2) documente de ieșire, obținute în urma funcționării sistemului;

3) documente tehnologice.

**25.** Documentele de intrare ale SI RSDG sunt următoarele:

1) profilurile ADN, cunoscute, de asemenea, ca amprente digitale ADN, reprezintă componenta centrală a unei baze de date ADN. Acestea constau dintr-o serie de numere care reprezintă structura genetică unică a unei persoane și include rezultatele analizei ADN, precum repetările scurte în tandem (*Short Tandem Repeats (STRs))* sau polimorfisme uninucleotidice (*Single Nucleotide Polymorphisms (SNPs))*;

2) informații despre mostră, care includ informații despre mostra biologică utilizată pentru a genera profilul ADN, inclusiv tipul mostrei (de ex. sânge, saliva, fire de păr), data recoltării și sursa mostrei (de ex., locul faptei). Acestea includ informații despre mostră ca atare, inclusiv tipul mostrei, data recoltării și numărul de identificare a mostrei;

**26.** Documente de ieșire ale SI RSDG sunt următoarele:

1) rapoarte cu privire la cauză care includ informații în detaliu despre analiza ADN și interpretarea acesteia, inclusiv comparația rezultatelor profilului ADN și semnificația statistică a concordanței;

2) informații despre cauză asociată cu mostra ADN, inclusiv numărul cauzei, data comiterii infracțiunii și amplasarea locului faptei;

**27.** Documentele tehnologice ale SI RSDG sunt următoarele:

1) informații identificabile cu caracter personal care includ date despre persoana a cărui ADN a fost analizat, inclusiv numele, adresa, data nașterii, marcheri de identificare (de ex., cicatrice, tatuaje) și alte detalii cu caracter personal;

2) criterii de căutare care să permită personalului autorizat să caute profiluri ADN concrete, mostre, cauze sau persoane în baza unor criterii concrete, inclusiv tipul mostrei, data comiterii infracțiunii sau numele persoanei;

3) obiecte informaționale din arhiva profilurilor ADN depersonalizate;

4) informații despre utilizator, care includ informații despre utilizatorii bazei de date, inclusiv numele utilizatorului, rolul și nivelul de acces;

5) înscrieri de audit, care conțin informații cu privire la evidența tuturor modificărilor operate în baza de date, inclusiv completările, radierile și actualizările, precum și utilizatorul responsabil pentru modificare.

**VII. SPAȚIUL INFORMAȚIONAL al SI RSDG**

**28.** Profilurile ADN – Profilul ADN este un cod alcătuit din numere și/sau litere, care reprezintă un set de caracteristici de identificare a părții needificate a mostrei analizate de ADN uman, precum și structura moleculară specifică din diverse segmente (loci) ADN.

Identificatorul profilului ADN este un număr de referință alcătuit dintr-o combinație a următorilor itemi:

1) un cod care permite identificarea și extragerea datelor cu caracter personal și a altor informații din SIA RSDG;

2) un cod care indică originea națională a profilului ADN;

3) un cod care indică tipul profilului ADN.

**29.** Profilul ADN poate fi:

1) neidentificat – profil ADN obținut din urmele colectate în cursul anchetei unei infracțiuni care aparține unei persoane neidentificate;

2) de referință – profil ADN care aparține unei persoane identificate.

**30.** Persoana, care definește proprietarul uman al profilului ADN. Obiectul Persoana poate avea două instanțe diferite: Persoană identificată și Persoană neidentificată.

1) obiectul informațional Persoana identificată indică o persoană fizică identificată univoc. O caracteristică a persoanei identificate este prezența înregistrării acesteia în Registrul de Stat al Populației. Cazul prezenței a mai multor identități a unei persoane fizice în Registrul de Stat al Populației este tratat conform procedurii legale și procedurilor de ținere a registrului. SI RSDG trebuie să dispună de mecanisme de sincronizare a datelor cu Registrul de Stat al Populației pentru a asigura actualizarea datelor despre persoană.

Persoana este identificată prin codul IDNP. Identificatorul numeric personal (IDNP) este un cod numeric alcătuit din 13 cifre, unic, care este atribuit fiecărui cetățean al Republicii Moldova la naștere și persoanelor străine domiciliate în Republica Moldova sau care au solicitat o formă de protecție și se află pe teritoriul Republicii Moldova. Acest cod este utilizat pentru a identifica persoana în Registrul de Stat al Populației din Republica Moldova.

2) obiectul informațional Persoana neidentificată definește o persoană fizică proprietar uman al profilului ADN care la momentul înregistrării nu este cunoscută sau nu poate fi identificată univoc. Obiectul informațional Persoană neidentificată este identificat printr-un cod unic generat de SI RSDG care include informații ce pot permite identificarea acesteia:

a) numele, prenumele, patronimicul;

c) data nașterii;

d) porecla (pseudonim);

e) vârsta;

f) înălțimea;

g) culoarea ochilor;

h) culoare părului;

i) alte însemne distinctive (tatuaje, cicatrice).

**31.** În cazul identificării persoanei căreia îi aparține profilul ADN obiectul Persoană neidentificată urmează a fi înlocuită cu Persoana identificată.

**32.** Cauză penală – identificatorul cauzei este numărul de înregistrare al infracțiunii/semnalului în registrele R1 și R2 și identificatorul registrului. Numărul de înregistrare al cauzei este preluat din Registrul informațiilor criminalistice și criminologice. Cheia suplimentară pentru identificarea cauzei este codul alcătuit din: codul solicitantului și numărul de înregistrare a dosarului penal din registrele lor. Utilizarea cheii suplimentare este necesară deoarece numărul dosarului înregistrat de organul de urmărire penală nu corespunde numărului dosarului înregistrat de instanță.

**33.** Document – orice informație identificată în formă structurată (document) sau nestructurată (mesaj, fișier audio/video etc.) poate fi considerată document. Identificatorul documentului este numărul de ordine de înregistrare a documentului în SI RSDG. Cheia suplimentară pentru identificarea documentului include codul registratorului (sub-registratorului) și numărul de înregistrare al documentului în registrul documentelor de intrare al țării de intrare (sub-registratorul). Obiectul informațional al documentului include fără a se limita la:

1) identificatorul documentului;

2) emitentul documentului;

3) seria, numărul și data emiterii documentului;

4) tipul documentului;

5) indicele de identificare a formularului (in cazul documentelor de strictă evidență imprimate/perfectate);

6) conținutul documentului:

a) un document electronic structurat semnat electronic;

b) o copie scanată a documentului pe suport de hârtie semnat electronic de autor sau registrator.

**34.** Etichetele – sunt metadate care descriu obiectul informațional și pot fi asociate cu acesta. Unele etichete de acces restricționat pot semnala prelucrarea automatizată a obiectului informațional etichetat de sistemul informatic. Practica de etichetare prevede un mecanism flexibil și solid pentru clasificarea semantică a documentului.

**35.** Etichetele sistematizate sunt o categorie de etichete pe care soluția SI RSDG le poate recunoaște și prelucra automat. Etichetele sistematizate sunt utilizate atât pentru definirea categoriilor de date (de exemplu, pentru a identifica profilurile ADN care aparțin diferitor grupuri de persoane în baza de date de eliminare precum: "#lucrător de laborator", "#producător", "#anchetator", "#victimă" etc.),cât și pentru a organiza interfața utilizatorului (eticheta "#validat" poate fi utilizată pentru a grupa datele ce trebuie înregistrate în registru).

O categorie specifică de etichete sistematizate este reprezentată de tipul subiectului înregistrării genetice judiciare, iar pasibili de înregistrarea genetică sunt persoanele și obiectele prevăzute la art. 8 din Legea nr. 235/2017 cu privire la înregistrarea genetică judiciară.

**36.** Metadatele și datele pentru controlul calității – includ informații suplimentare asociate fiecărui profil ADN, precum data și ora colectării profilului, tipul mostrei utilizate (de ex., sânge, saliva, fire de păr) și orice alte informații relevante despre sursa ADN. Datele controlului calității includ informații despre calitatea și corectitudinea profilurilor ADN, inclusiv tehnicile și protocoalele utilizate pentru a genera profilurile, precum și informații despre orice verificare a controlului calității efectuate în cursul analizei. Aceste informații sunt importante pentru urmărirea și gestionarea profilurilor în baza de date.

**37.** Identificatorul furnizorului – un nomenclator local cu date de identificare a furnizorilor care au prezentat profilul ADN și informațiile suplimentare. Poate include date despre expertul/specialistul care a extras ADN-ul. Codul IDNO este utilizat în calitate de identificator pentru persoanele juridice, iar pentru persoanele fizice este utilizat IDNP. Pentru sursele din afara țării poate fi definit un cod local al țării.

**VIII. SPAȚIUL TEHNOLOGIC al SI RSDG**

**38.** Arhitectura generală a bazei de date criminalistice ADN se referă la proiectarea și structura sistemelor software utilizate pentru a gestiona și analiza date ADN în anchete penale. De regulă, printre componentele software ale unei baze de date comprehensive ADN sunt incluse următoarele:

1) componenta de gestionare a profilului ADN, care este responsabilă de stocarea și gestionarea profilurilor ADN, inclusiv a informațiilor demografice, informațiilor despre cauză și a rezultatelor ADN;

2) componenta de comparare ADN, care este responsabilă de compararea profilurilor ADN în baza de date pentru a identifica concordanțe și poate utiliza diverși algoritmi și modele statistice pentru a calcula probabilitatea unei concordanțe;

3) componenta de gestionare a fluxului de lucru, care este responsabilă de urmărirea și gestionarea procesului de colectare, analizare și stocare a probelor ADN și poate include astfel de trăsături precum urmărirea mostrei, gestionarea cauzei și controlul calității;

4) componenta de vizualizare și raportare a datelor, care este responsabilă de prezentarea rezultatelor ADN și a altor informații într-un format atractiv din punct de vedere vizual și ușor de înțeles și poate include astfel de caracteristici precum grafice, diagrame și rapoarte;

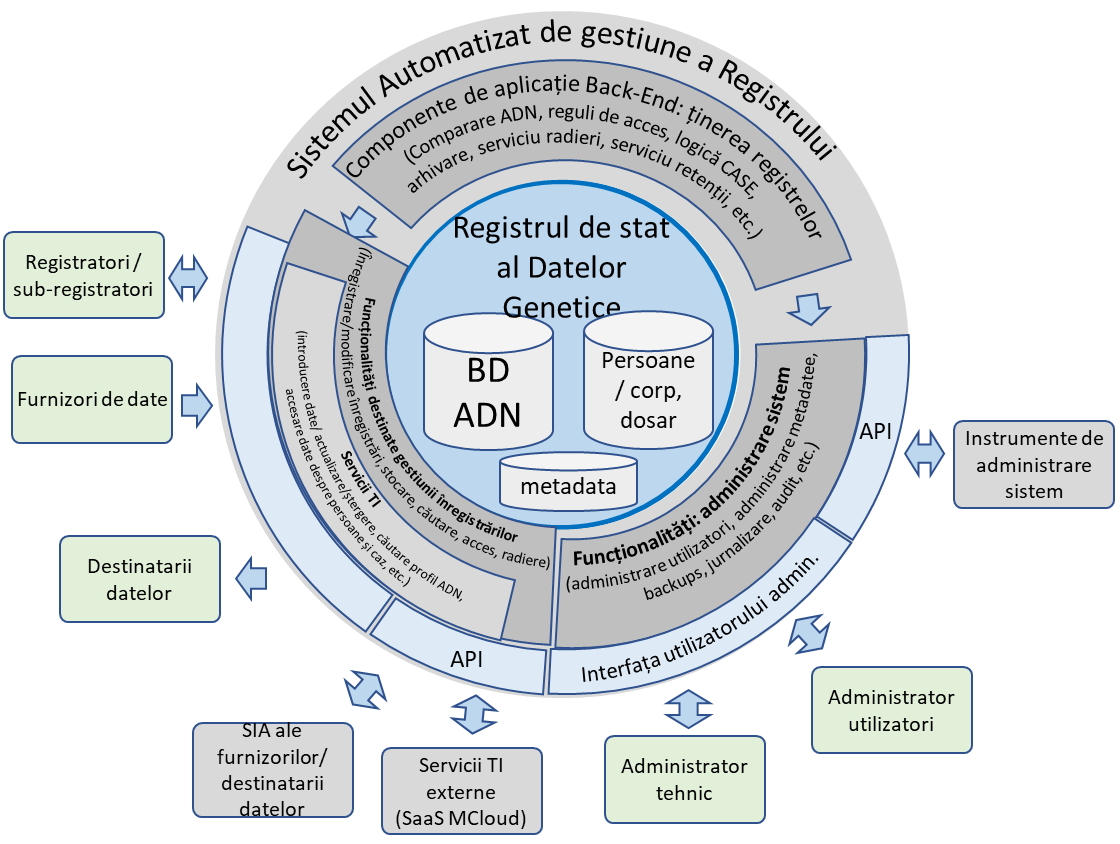
5) componenta de gestionare a utilizatorilor este responsabilă de gestionarea conturilor, controlul accesului și autentificarea utilizatorilor și poate include astfel de caracteristici precum protecția parolei, a rolurilor utilizatorilor și a culoarelor de audit;

6) componenta copiilor de rezervă și de restabilire a datelor, care este responsabilă cu asigurarea securității și fiabilității bazei de date ADN și poate include astfel de caracteristici precum copii de rezervă a datelor, restabilirea în urma unui dezastru și criptare a datelor.

**Secțiunea 1**

**Arhitectura și spațiul tehnologic a SI RSDG**

**Figura 4. Arhitectura SI RSDG**



**39.** Arhitectura tehnologică include toate aspectele conexe fiabilității și siguranței funcționării sistemului, precum zona geografică, locația și caracteristicile centrelor de date, rețelei de transfer al datelor, componentele tehnice și software de bază (sistemele operaționale, sistemele de administrare a bazei de date, serverele, soluțiile aplicative, mijloacele dezvoltatorilor, soluțiile aplicative pentru utilizatori).

**40.** Arhitectura tehnologică a SIA RDGS este conceputa cu aplicarea principiilor stabilite de documentul de arhitectură al STI al MAI și de viziunea-cadru guvernamentală în domeniul TIC. Arhitectura tehnologică necesară pentru RSDG include 3 dimensiuni principale:

1) infrastructura tehnologică a utilizatorului:

a) se preconizează utilizarea unui web browser pentru a accesa SIA RSDG. Administratorii tehnici pot utiliza o soluție aplicativă desktop dedicată administrării componentelor software;

b) soluția aplicativă web nu necesită resurse semnificative hardware și software de la stațiile de lucru ale utilizatorilor și poate fi utilizată în cadrul diferitor sisteme de operare

2) capacitatea de prelucrare (servere):

a) platforma tehnologică guvernamentală comună (MCloud) oferă toate beneficiile unei soluții cloud computing: scalabilitate, adaptabilitate și flexibilitate pentru datele găzduite de centrele virtuale;

b) platforma tehnologică guvernamentală comună MCloud este administrată de STISC, capabilă să asigure integritatea, disponibilitatea și securitatea serviciilor TIC;

c) MCloud este conectată la nodul central al rețelei guvernamentale, fapt ce asigură capacitatea de interconexiune cu SIA din posesia altor autorități publice. Platforma de interoperabilitate MConnect este amplasată în MCloud;

d) MAI optează pentru utilizarea platformei tehnologice MCloud pentru găzduirea informațiilor gestionate de sistemele informaționale;

e) existența normelor juridice care descurajează dezvoltarea centrelor locale de date de către autoritățile publice (Hotărârea Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat, Hotărârea Guvernului nr. 823/2020 cu privire la optimizarea și eficientizarea centrelor de date din sectorul public, precum și la aprobarea modificărilor ce se operează în unele hotărâri ale Guvernului).

3) infrastructura rețelei pentru funcționarea SI RSDG:

a) LAN a centrului de date;

b) rețeaua guvernamentală prin care se asigură accesul la serverele care găzduiesc SI RSDG;

c) punctul de contact cu rețelele străine / internaționale ale organelor de poliție;

d) LAN a utilizatorilor SI RSDG.

**41.** Furnizor de date în calitate de partener de interoperabilitate

1) Platforma tehnologică guvernamentală comună (MCloud) – pentru găzduirea sistemului;

2) Platforma de interoperabilitate (MConnect) – pentru schimbul de date cu alte sisteme informaționale şi registre;

3) Serviciul electronic guvernamental integrat de semnătură electronică (MSign) – pentru semnarea documentelor electronice;

4) Serviciul electronic guvernamental de autentificare şi control al accesului (MPass) – pentru autentificarea şi controlul accesului în cadrul sistemului;

5) Serviciul electronic guvernamental de jurnalizare (MLog) – pentru asigurarea evidenței operațiunilor (evenimentelor) produse în cadrul SI RSDG;

6) Serviciul electronic guvernamental de notificare (MNotify) – pentru notificarea furnizorilor de date, registratorilor și utilizatorilor;

7) Sistemul informațional automatizat „Registrul împuternicirilor de reprezentare în baza semnăturii electronice” (MPower) – pentru validarea împuternicirilor de reprezentare;

8) Serviciul guvernamental de livrare (MDelivery) – pentru oferirea unui mecanism unic de livrare fizică a rezultatelor din cadrul procesului de înregistrare genetică judiciară.

Dacă pentru efectuarea înregistrării genetice de stat legislația prevede deținerea unui document ale cărui date sunt disponibile în resursele informaționale ale altor instituții de stat, ele pot fi consumate sau furnizate prin intermediul Platformei de interoperabilitate (MConnect).

**Secțiunea 1**

**Obiectele informaționale**

**42.** Obiectele informaționale ale unei baze de date criminalistice comprehensive ADN sunt formele variate ale datelor și informațiilor care sunt produse sau stocate ca parte a procesului de analiză a ADN și sunt păstrate în baza de date, care includ:

1) profilurile ADN, cunoscute, de asemenea, ca amprente digitale ADN, care reprezintă componenta centrală a unei baze de date ADN. Acestea constau dintr-o serie de numere care reprezintă structura genetică unică a unei persoane. Acesta este obiectul informațional principal din baza de date ADN și include rezultatele analizei ADN, precum repetările scurte în tandem sau polimorfisme uninucleotidice;

2) datele profilului ADN sunt oferite în format digital de laboratoarele criminalistice acreditate conform ISO 17025. Este necesar de asigurat interoperabilitatea SI RSDG cu echipamentul utilizat de aceste laboratoare pentru digitalizarea profilurilor ADN. Introducerea manuală a profilului ADN se efectuată în cazuri excepționale și va fi aplicată o procedură de validare riguroasă.

3) datele despre persoana identificată vor fi extrase din Registrul de stat al populației. În cazul persoanelor, corpurilor sau mostrelor neidentificate, datele vor fi extrase din Sistemului informațional automatizat „Gestiunea Dosarelor de Expertiză Judiciară”. De regulă, în cazul unor persoane/mostre neidentificate prelevate la locul faptei, există o solicitare pentru efectuarea unei expertize genetice;

4) informații identificabile cu caracter personal, care includ informații despre persoana al cărui ADN a fost analizat, inclusiv numele, adresa, data nașterii, marcheri de identificare (ex., cicatrice, tatuaje) și alte detalii cu caracter personal;

5) informații despre cauză, care includ informații despre cauza asociată cu mostra ADN, inclusiv numărul cauzei, data comiterii infracțiunii și amplasarea locului faptei;

6) informații despre mostră, care includ informații despre mostra biologică utilizată pentru a genera profilul ADN, inclusiv tipul mostrei (de ex., sânge, saliva, fire de păr), data recoltării și sursa mostrei (ex., locul faptei). Acestea includ informații despre mostră ca atare, inclusiv tipul mostrei, data recoltării și numărul de identificare a mostrei;

7) criterii de căutare, baza de date trebuie să dispună de o funcție de căutare care să permită personalului autorizat să caute profiluri ADN concrete, mostre, cauze sau persoane în baza unor criterii concrete, inclusiv tipul mostrei, data comiterii infracțiunii sau numele persoanei;

8) rapoarte cu privire la cauză, care includ rapoarte în detaliu despre analiza ADN și interpretarea acesteia, inclusiv comparația rezultatelor profilului ADN și semnificația statistică a concordanței;

9) obiecte informaționale din arhiva profilurilor ADN depersonalizate;

10) informații despre utilizator, care includ informații despre utilizatorii bazei de date, inclusiv numele utilizatorului, rolul și nivelul de acces.

11) înscrieri de audit, care includ evidența tuturor modificărilor operate în baza de date, inclusiv completările, radierile și actualizările, precum și utilizatorul responsabil pentru modificare.

**43.** În SI RSDG se utilizează următoarele scenarii de bază:

1) *evidența înregistrărilor* – datele sunt introduse în registru pe baza datelor transmise de furnizorul de date pentru înregistrare în formă electronică prin intermediul platformei de interoperabilitate, iar înregistrarea este efectuată conform deciziei registratorului/sub-registratorului în baza actelor justificative prezentate. La introducerea unui obiect în registru, se înscrie in jurnal (log) datele privind înregistrarea, a documentele prezentate în baza cărora a fost efectuată inserarea și decizia de introducere a obiectului în registru.

2) *actualizarea înregistrărilor* – înregistrările nu sunt redactate – orice modificare lansează o nouă înregistrare. Modificările sunt efectuate numai pe baza documentelor justificative prezentate de furnizorul de date pentru înregistrare. Modificările sunt efectuate pe baza deciziei registratorului. Datele sunt păstrate în ordine cronologică. Modalitatea de evidență a datelor trebuie să asigure posibilitatea de a obține datele privind obiectul la un anumit timp.

3) *furnizarea de date* – furnizarea informației genetice din Registru se efectuează prin:

a) acordarea accesului omologat prin intermediul platformei de interoperabilitate;

b) emiterea documentelor în formă electronică sau, la solicitarea expresă a destinatarului, pe suport de hârtie;

c) acordarea informațiilor prin poșta electronică sau prin alte mijloace de comunicare.

**44.** Radierea automată din SI RSDG a informației genetice referitoare la persoanele prevăzute la art. 8 din Legea nr. 235/2017 cu privire la înregistrarea genetică judiciară, se realizează în conformitate cu art. 11 din aceeași lege.

**IX. ASIGURAREA SECURITĂȚII**

**INFORMAȚIONALE A SI RSDG**

**45.** Securitatea SI RSDG presupune starea de protecție a resurselor și infrastructurii informaționale, prin care se asigură veridicitatea, integritatea, confidențialitatea, disponibilitatea și autenticitatea resurselor informaționale. Sistemul securității informaționale reprezintă o totalitate a acțiunilor juridice, organizatorice, economice și tehnologice orientate spre prevenirea pericolelor asociate resurselor și infrastructurii informaționale. Pot fi delimitate următoarele probleme de asigurare a securității informaționale cu care se va confrunta sistemul informațional:

1) asigurarea confidențialității informației (prevenirea obținerii informațiilor de către persoanele care nu au drepturile și competențele respective);

2) asigurarea integrității logice a datelor (prevenirea introducerii, actualizării și ștergerii nesancționate a informației sau introducerea datelor denaturate);

3) asigurarea securității infrastructurii informaționale de tentative de a defecta sau de a modifica funcționarea acesteia.

**46.** Asigurarea securității informaționale va fi realizată în conformitate cu Cerințele minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr. 201/2017. Pentru gestiunea riscurilor de securitate va fi implementată o politică generală de securitate. Personalul implicat în utilizarea și administrarea SI RSDG va fi instruit în ceea ce privește riscurile de securitate la care poate fi expus. Politica de securitate va include prevederi referitoare la organizarea auditurilor periodice de securitate pentru a verifica politica și conformitatea cu regulile de securitate, precum și pentru a stabili domeniile care necesită îmbunătățiri.

**47.** Din motive criminalistice și în temeiul legislației privind protecția datelor cu caracter personal, profilurile ADN și informațiile asociate ar trebui introduse și stocate în mod corect, prin evitarea introducerii manuală a profilurilor ADN.

**48.** Accesul la baza de date ADN trebuie să fie limitat prin măsuri fizice și organizaționale numai la persoanele care solicită accesul. Periodic, trebuie să fie făcute copii de rezerva care să fie stocate într-un loc sigur și recuperate periodic pentru a simula restabilirea în urma unui dezastru.

**49.** Atunci când profilurile ADN și informațiile asociate acestora sunt prezente în sisteme diferite, aceste sisteme trebuie să fie comparate periodic pentru a verifica că sunt sincronizate în mod adecvat.

**50.** Mecanismele principale de securitate informațională utilizate vor fi:

1) autentificarea și autorizarea accesului la date;

2) administrarea accesului la date;

3) înregistrarea acțiunilor utilizatorilor SI RSDG;

4) criptarea datelor, după caz;

5) auditul informațional;

6) procedurile de restabilire, în caz de dezastru.

**51.** Pentru asigurarea unui nivel adecvat al securității informaționale a SI RSDG se consideră binevenită elaborarea și implementarea unei politici de asigurare a securității informaționale. Această politică va detalia totalitatea compartimentelor de securitate, rolurile, drepturile și obligațiile fiecărui actor al sistemului informațional. Politica de securitate va fi adusă la cunoștința fiecărui utilizator și semnată de către acesta. Fiecare utilizator va cunoaște obligațiile de serviciu în materie de respectare a securității informaționale și totalitatea procedurilor formale pe care trebuie să le respecte în strictă concordanță cu politica de securitate.

**52.** Posesorul, deținătorul și registratorii vor proteja SI RSDG de pericolul cauzării prejudiciilor resurselor sau infrastructurii informaționale în strânsă cooperare cu autoritățile publice competențele cărora sunt conexe dezvoltării de noi resurse informaționale de stat sau/și de date care se conțin în SI RSDG: Instituția publică Agenția de Guvernare Electronică, Serviciul Tehnologia Informației și Securitate Cibernetică, Centrul Național pentru Protecția Datelor cu Caracter Personal, STI al MAI în calitate de responsabil pentru arhitectura TIC a MAI și responsabil pentru implementarea securității cibernetice în cadrul MAI.

**X. ÎNCHEIERE**

Prezentul Concept descrie principalele aspecte organizaționale, metodologice și tehnologice în conformitate cu care este concepută și va fi implementată ideea realizării unei soluții informatice performante, care ar asigura suportul informațional actorilor implicați în procesele de prelevarea mostrelor și analiza ADN la gestionarea și partajarea datelor.

Este stabilit cadrul general și locul unui astfel de sistem în sistemul de guvernare electronică. A fost aleasă soluția optimă, care corespunde standardelor în domeniu și nivelului actual de dezvoltare a guvernării electronice în Republica Moldova.

Implementarea SI RSDG va permite implementarea unei soluții informatice care va furniza tot spectrul de prelevare/recoltarea a materialului biologic, care se vor introduce în SI RSDG și care se vor efectua prin metode noninvazive, prin recoltarea celulelor epiteliale prin periaj al mucoasei bucale, iar în situațiile în care nu se poate realiza această modalitate – prin recoltarea unor celule epiteliale din regiunea feței/cefei.

Neimplementarea SI RSDG poate avea un impact negativ substanțial asupra activității CTCEJ și a experților judiciari, dar și asupra aspectului de securitate, integritate și veridicitate a profilurile ADN și informațiile asociate colectate. Odată cu creșterea volumului de date, în lipsa unui sistem informațional automatizat, administrarea lor devine mai complicată și ineficientă, implicând și riscul pierderii complete a datelor.

Anexa nr. 2

la Hotărârea Guvernului nr.\_\_\_\_\_\_

din \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023

**REGULAMENTUL**

**privind modul de ținere a Sistemului informațional „Registrul de stat al datelor genetice”**

**I. DISPOZIȚII GENERALE**

**1.** Regulamentul privind modul de ținere a Registrului format din Sistemul informațional „Registrul de stat al datelor genetice” (în continuare – *Regulament*) stabilește modul de organizare şi mecanismul de funcționare a resursei informaționale destinate evidenței integrate şi sistematizate a informației aferente procesului de colectare, introducere şi administrare a materialului biologic şi a informației genetice judiciare, desfășurat de organele abilitate.

**2.** Sistemul informațional Registrul de stat al datelor genetice (în continuare – *SI* *RSDG*) este organizat astfel încât să asigure ca procesele de evidență şi acces la informația genetică judiciară să fie simple, eficiente, accesibile şi transparente.

**3.** Noțiunile utilizate în prezentul Regulament sunt corespunzătoare definițiilor din Legea nr. 235/2017 cu privire la înregistrarea genetică, Legea nr. 467/2003 cu privire la informatizare şi la resursele informaționale de stat, Legea nr. 71/2007 cu privire la registre și Regulamentul privind gestionarea materialului biologic, aprobat prin Hotărârea Guvernului nr. 236/2020.

**II. SUBIECŢII RAPORTURILOR JURIDICE ÎN DOMENIUL CREĂRII,**

**EXPLOATĂRII ŞI UTILIZĂRII SI RSDG**

**4.** Subiecții din domeniul creării, exploatării şi utilizării SI RSDG sunt:

1) proprietarul;

2) posesorul;

3) deținătorul și administratorul tehnic al sistemului;

4) registratorii;

5) furnizorii de date;

6) utilizatorii datelor sistemului.

**5.** Proprietarul SI RSDG este statul, care îşi realizează dreptul de proprietate, de gestionare şi de utilizare a datelor din SI RSDG. Proprietarul are atribuția de a asigura resursele financiare necesare pentru dezvoltarea, mentenanța şi exploatarea SI RSDG din bugetul statului şi/sau alte mijloace financiare, conform legislației.

**6.** Posesorul SI RSDG este Ministerul Afacerilor Interne (în continuare – *MAI*) care are următoarele atribuții:

1) asigură condițiile juridice, organizatorice şi financiare pentru crearea şi ținerea SI RSDG;

2) în comun cu alte instituții publice de profil, asigură elaborarea şi înaintarea proiectelor de acte normative privind înscrierea, acumularea, păstrarea, completarea, corectarea, sistematizarea şi utilizarea datelor, precum şi funcționarea SI RSDG şi le remite spre aprobare Guvernului;

3) asigură funcționarea, administrarea şi dezvoltarea continuă a SI RSDG în conformitate cu nivelul agreat de servicii şi în limitele bugetului alocat;

4) monitorizează procesul de înregistrare şi prelucrare a datelor în Registru;

5) asigură accesul registratorilor, furnizorilor de date și utilizatorilor în conformitate cu drepturile de acces stabilite şi atribuțiile delegate;

6) stabilește măsurile tehnice, organizatorice de protecție şi securitate a SI RSDG, monitorizează şi ajustează cerințele de securitate şi de conformitate a SIA REA în domeniul protecției datelor cu caracter personal;

7) asigură păstrarea SI RSDG până la adoptarea deciziei de lichidare a acestuia.

**7.** Deținătorul și administratorul tehnic este STI care își realizează atribuțiile în conformitate cu cadrul normativ privind administrarea tehnică şi menținerea sistemelor informaționale de stat și are următoarele atribuții:

1) asigură dezvoltarea, administrarea, mentenanța şi securitatea SI RSDG;

2) este responsabil de acordarea accesului securizat pentru utilizarea SI RSDG, la solicitarea posesorului;

3) asigură crearea, exploatarea, administrarea şi gestionarea SI RSDG în limitele reglementate de proprietar;

4) asigură integritatea, securitatea şi protecția datelor din SI RSDG, inclusiv protecția datelor cu caracter personal;

5) monitorizează activitatea subiecților sistemului informațional, procesul de înregistrare şi prelucrare a datelor în cadrul SI RSDG;

6) asigură modificările/rectificările/dezvoltările solicitate de către posesorul SI RSDG;

7) administrează infrastructura tehnică (hardware și software), de întreținere și implementează politicile de securitate ale sistemului.

**8.** Utilizatorii datelor sistemului sunt:

1) Registratori sunt experții judiciari ai CTCEJ responsabili de înregistrarea, modificarea, actualizarea și radierea datelor din SI RSDG.

**9.** În conformitate cu art. 8 din Legea nr. 235/2017 cu privire la înregistrarea genetică judiciară, persoanele și obiectele pasibile de înregistrarea genetică sunt:

1) *Bază de date ADN a Interpol și portalul ADN* – este un suport pentru transferul profilurilor ADN între două sau mai multe țări și pentru gestionarea profilurilor ADN proprii ale țării în baza de date ADN centrală. Accesul unei țări la portalul ADN este asigurat direct prin Birourile centrale naționale ale Interpol-ului, utilizând sistemul de comunicare securizat I-24/7.

2) *Sistemul informațional Europol* – este o bază de date centrală pentru informare în materie penală și pentru informații operative, care include toate domeniile infracționale acoperite de mandatul agenției. Acesta este un sistem de referință prin care se verifică dacă în alte state membre sunt disponibile informații privind o anumită persoană sau un anumit obiect de interes.

**10.** Furnizori de date sunt:

1) SIA al laboratoarelor acreditate conform ISO 17025 în domeniul expertizei genetice:

a) laboratorul CTCEJ;

b) Centrul de Medicină Legală al Ministerului Sănătății;

c) alte laboratoare acreditate conform ISO 17025.

2) SIA al autorităților abilitate să dispună înregistrarea genetică:

a) instanțele de judecată;

b) procuratura;

c) MAI și subdiviziunile din subordine abilitate cu competențe de urmărire penală (Inspectoratul General al Poliției, Inspectoratul General al Poliției de Frontieră, Serviciul protecție internă și anticorupție).

d) Administrația Națională a Penitenciarelor.

3) Cooperarea polițienească transfrontalieră

a) Punctul național de contact ADN poate furniza profile ADN și/sau informații adiționale despre cetățenii Republicii Moldova care figurează într-un dosar penal gestionat de un stat partener dacă acesta este subiect al înregistrării în RSDG. În calitate de Punct național de contact ADN sunt:

- Direcția de Cooperare Polițienească Internațională a IGP (DCPI) ca punct național de contact – este responsabilă de schimbul de date în lipsa conexiunii online;

- CTCEJ în calitate de punct național de contact pentru ADN – este responsabilă cu confirmarea furnizării datelor detaliate (despre persoană, caz, etc.)în cazul hit-urilor și pentru confirmarea hit-urilor discutabile.

b) Instituțiile de poliție externă cu care Republica Moldova a semnat acorduri privind schimbul automat de date ADN vor avea acces la căutarea și compararea profilurilor ADN. Utilizatorii următoarelor canale de schimb stabilite conform acordurilor internaționale de cooperare polițienească pot fi utilizatori SIA RSDG:

- Europol;

- Interpol.

**11.** Destinatarii SI RSDG sunt:

1) interni – persoanele de la care au fost prelevate probele biologice, instanțele de judecată, organele de urmărire penală, organele care efectuează activitatea specială de investigații în cazul cercetării infracțiunilor mai puțin grave, grave, deosebit de grave şi excepțional de grave, precum şi Serviciul de Informații şi Securitate în scopul îndeplinirii atribuțiilor sale legale privind asigurarea securității naționale;

2) externi – organele de urmărire penală ale altor state, precum şi organizațiile internaționale de securitate, în conformitate cu tratatele internaționale la care Republica Moldova este parte.

Utilizatorii interni și externi au dreptul doar de vizualizare a informației genetică judiciară din SI RSDG.

**III. DREPTURILE ȘI OBLIGAŢIILE SUBIECŢILOR**

**LA CREAREA, EXPLOATAREA ŞI UTILIZAREA SI RSDG**

**Secțiunea 1.**

**Drepturile și obligațiile posesorului** **SI RSDG**

**12.** Posesorul are dreptul:

1) să elaboreze şi să amendeze, în limitele competenței funcționale, cadrul normativ cu privire la SI RSDG;

2) să propună soluții de perfecționare şi eficientizare a procesului de funcționare a SI RSDG, precum şi să le pună în aplicare;

3) să supravegheze respectarea cerințelor de securitate a informației;

4) să solicite suspendarea/lichidarea SI RSDG;

5) să verifice autenticitatea şi veridicitatea datelor introduse în SI RSDG.

12. Posesorul este obligat:

1) să dezvolte şi să propună, în funcție de competența sa, modificări la cadrul normativ cu privire la SI RSDG;

2) să propună soluții pentru perfecționarea şi eficientizarea procesului de funcționare a SI RSDG, precum şi să le pună în aplicare;

3) să supravegheze respectarea cerințelor de securitate a informației și să fixeze cazurile şi tentativele de încălcare a acestora;

4) să inițieze procedura de suspendare a drepturilor de acces la SI RSDG pentru nerespectarea regulilor, standardele şi normele general acceptate în domeniul securității informaționale;

5) să verifice autenticitatea şi veridicitatea datelor înscrise de registratori, furnizorii de date și utilizatori la SI RSDG;

6) să solicite de la registratori, furnizorii de date și utilizatori actualizarea sau corectarea datelor din baza de date a SI RSDG în caz de depistare a omiterilor şi erorilor;

7) să solicite de la organul ierarhic superior finanțarea anuală pentru dezvoltarea şi administrarea SI RSDG;

8) să asigure coordonarea şi monitorizarea procesului de implementare a SI RSDG cu autoritățile publice (instituțiile publice) participante, în conformitate cu cadrul normativ;

9) să efectueze monitorizarea şi supravegherea accesărilor informației din SI RSDG, să identifice încălcările comise şi să întocmească rapoarte privind datele accesate;

10) să asigure susținerea metodologică şi practică prin elaborarea de proceduri, reguli şi instrucțiuni în ceea ce privește înscrierea, acumularea, păstrarea, completarea, corectarea, sistematizarea şi utilizarea datelor, precum şi să asigure funcționarea SI RSDG;

11) să asigure funcționarea şi ținerea SI RSDG în conformitate cu cadrul normativ;

12) să asigure funcționarea neîntreruptă a SI RSDG;

13) să acorde suportul necesar persoanelor autorizate care au acces la SI RSDG privind utilizarea complexului de mijloace software aferente acestuia;

14) să asigure, prin intermediul deținătorului, accesul securizat la informația conținută în SI RSDG, respectarea condițiilor de securitate şi regulilor de exploatare a acestuia;

15) să utilizeze informația obținută din baza de date a SI RSDG doar în scopurile stabilite de cadrul normativ;

16) să asigure atribuirea rolurilor şi drepturilor de acces la datele SI RSDG;

17) să stabilească condițiile juridice, financiare şi organizatorice pentru administrarea şi mentenanța SI RSDG de către deținătorul acestuia;

18) să efectueze, prin intermediul deținătorului SI RSDG, măsurile organizatorico-tehnice necesare pentru asigurarea protecției şi confidențialității informației stocate în SI RSDG, inclusiv împotriva distrugerii, modificării, blocării, copierii, răspândirii, precum şi împotriva altor acțiuni ilicite, menite să asigure un nivel de securitate adecvat în ceea ce privește riscurile prezentate de prelucrare şi caracterul datelor prelucrate;

19) să informeze registratorii, furnizorii de date și utilizatorii SI RSDG despre modificările condițiilor tehnice de funcționare ale acestuia;

20) să efectueze auditul SI RSDG şi al sistemelor conexe pentru asigurarea protecției complexului de date şi bunei funcționări a acestuia.

**Secțiunea a 2-a.**

**Drepturile și obligațiile deținătorului și administratorului tehnic**

**al** **SI RSDG**

**13.** Deținătorul și administratorul tehnic are dreptul:

1) să supravegheze respectarea cerințelor de securitate a informației;

2) să acorde/revoce accesul la SI RSDG în cazurile de nerespectare a regulilor, standardelor şi normelor în domeniul securității informaționale;

3) să determine obiectele informaționale ale SI RSDG;

4) să asigure măsurile tehnice şi organizatorice de protecție şi securitate;

5) să ajusteze cerințele de securitate şi conformitate ale SI RSDG la cerințele cadrului normativ în domeniul protecției datelor cu caracter personal;

6) să gestioneze furnizarea de informații, registratorii și utilizatorii şi angajații din subordinea acestora, dar şi accesul la sistem, prin crearea, modificarea, eliminarea şi setarea drepturilor acestora;

7) să suspende funcționarea SI RSDG la solicitarea posesorului;

8) să organizeze seminare şi instruiri de utilizare a SI RSDG;

9) să monitorizeze şi să supravegheze accesările informației şi să identifice încălcările comise;

**14.** Deținătorul și administratorul tehnic este obligat:

1) să asigure administrarea tehnică, mentenanța şi dezvoltarea SI RSDG, precum şi implementarea cerințelor de securitate stabilite de actele normative în domeniu;

2) să asigure funcționarea SI RSDG în conformitate cu regulile privind reglementarea resurselor informaționale;

3) să asigură implementarea măsurilor necesare pentru asigurarea regimului de confidențialitate şi securitate a informației şi a datelor cu caracter personal;

4) să garanteze utilizarea informației obținute din SI RSDG doar în scopurile stabilite conform cadrului normativ;

5) să asigure securitatea sistemului de infrastructură şi infrastructura de comunicare;

6) să dețină alte obligații stabilite în conformitate cu cadrul normativ.

**Secțiunea a 3-a.**

**Drepturile și obligațiile registratorului** **SI RSDG**

**15.** Registratorul are dreptul:

1) să vizualizeze şi să editeze informațiile conținute în SI RSDG conform rolului atribuit;

2) să acceseze spațiul informațional al SI RSDG în limitele rolului atribuit;

3) să acceseze informațiile care se conțin în SI RSDG şi care au fost prezentate de către acesta;

4) să înainteze posesorului propuneri privind modificarea actelor normative care reglementează funcționarea SI RSDG;

5) să solicite şi să primească de la posesor sau deținător susținere practică privind funcționarea SI RSDG;

6) să înainteze posesorului propuneri privind îmbunătățirea şi sporirea eficacității funcționării SI RSDG;

**16.** Registratorul este obligat:

1) să acceseze SI RSDG în limitele rolului atribuit;

2) să asigure înregistrarea şi actualizarea datelor, în termenele stabilite de legislație;

3) să vizualizeze şi să modifice informațiile din SI RSDG, conform rolului atribuit;

4) să înainteze posesorului propuneri privind modificarea actelor normative care reglementează funcționarea SI RSDG;

5) să solicite şi să primească de la posesor/deținător susținere metodologică şi practică privind funcționarea SI RSDG;

6) să înainteze posesorului propuneri privind îmbunătățirea şi sporirea eficacității funcționării SI RSDG;

7) să asigure corectitudinea, autenticitatea şi veridicitatea datelor înscrise în SI RSDG;

8) să corecteze erorile ca urmare a înscrierii eronată a datelor, precum şi orice alte erori constatate;

9) să dețină semnătură electronică validă, obținută conform reglementărilor stabilite de către prestatorii de servicii de certificare;

10) să semneze formularele electronice cu semnătura electronică prevăzută de legislație, în scopul confirmării veridicității datelor;

11) să întreprindă măsuri pentru evitarea accesului neautorizat al persoanelor terțe;

12) să utilizeze funcționalitățile SI RSDG în exclusivitate, conform destinației acestora şi în conformitate cu cadrul normativ;

13) să radieze automat informația genetică în conformitate cu art. 11 din Legea nr. 235/2017 cu privire la înregistrarea genetică judiciară.

14) să radieze la solicitare informația genetică în conformitate cu art.12 Legea nr. 235/2017 cu privire la înregistrarea genetică judiciară.

**Secțiunea a 4-a.**

**Drepturile și obligațiile furnizorului de date ale** **SI RSDG**

**17.** Furnizorul de date are dreptul:

1) să vizualizeze şi să modifice informațiile din Registru, conform rolului atribuit;

2) să acceseze SI RSDG în limitele rolului atribuit;

3) să acceseze informațiile care se conțin în SI RSDG;

4) să solicite şi să primească de la posesor sau deținător suport metodologic şi practic privind funcționarea SI RSDG;

e) să înainteze posesorului propuneri privind modificarea actelor normative care reglementează funcționarea SI RSDG;

**18.** Furnizorul de date este obligat:

1) să consume informațiile din SI RSDG în conformitate cu prevederile legislației cu privire la schimbul de date şi interoperabilitate;

2) să înainteze posesorului SI RSDG propuneri privind modificarea şi/sau completarea actelor normative care reglementează funcționarea SI RSDG;

3) să solicite şi să primească de la posesorul Registrului ajutor metodologic şi practic privind funcționarea acestuia;

4) să prezinte propuneri posesorului SI RSDG privind perfecționarea şi eficientizarea funcționării acestuia;

5) să asigure schimbul de informații şi/sau integrarea sistemelor informaționale proprii cu SI RSDG;

6) să colaboreze cu deținătorul SI RSDG pentru asigurarea securității accesului la SI RSDG şi să informeze despre orice acțiune suspicioasă de care are cunoștință şi care ar putea să reprezinte un atentat la securitatea accesului la sistem;

7) să asigure corectitudinea, autenticitatea şi veridicitatea datelor furnizate în limitele competenței;

8) să utilizeze informația doar în scopurile stabilite de legislație;

9) să efectueze măsurile organizatorice şi tehnice interne necesare asigurării protecției şi confidențialității informației transmise către SI RSDG.

**Secțiunea a 5-a.**

**Drepturile și obligațiile destinatarului SI RSDG**

**19.** Destinatarul are dreptul:

1) să solicite şi să primească de la posesorul sau deținătorul SI RSDG ajutor metodologic şi practic privind funcționarea acestuia;

2) să solicite şi să primească de la posesor sau deținător accesul la datele/informațiile din SI RSDG în conformitate cu scopul prelucrării şi rolul atribuit;

3) să participe la implementarea şi dezvoltarea SI RSDG;

4) să vizualizeze datele/informațiile/documentele din SI RSDG în conformitate cu drepturile de acces stabilite, pornind de la atribuțiile şi funcțiile deținute, fără dreptul de a modifica aceste date/informații/documente;

**20.** Destinatarul este obligat:

1) să utilizeze funcționalitățile SI RSDG conform rolurilor şi permisiunilor atribuite;

2) să solicite şi să primească de la posesorul SI RSDG suport metodologic şi practic privind funcționarea acestuia;

3) să înainteze posesorului SI RSDG propuneri privind modificarea şi/sau completarea actelor normative care reglementează funcționarea SI RSDG;

4) să prezinte propuneri posesorului SI RSDG privind perfecționarea şi eficientizarea funcționării acestuia;

5) să utilizeze informația obținută din baza de date a SI RSDG doar în scopurile stabilite de legislație;

6) să întreprindă toate măsurile necesare pentru asigurarea regimului de confidențialitate şi securitate a datelor cu caracter personal în conformitate cu instrucțiunile deținătorului SI RSDG şi Legii nr.133/2011 privind protecția datelor cu caracter personal;

7) să raporteze imediat, în formă verbală şi scrisă, posesorului SI RSDG şi/sau administratorului tehnic despre incidentele de securitate;

8) să nu întreprindă anumite acțiuni în vederea obținerii accesului neautorizat la informații, indiferent de metodă.

**IV. ŢINEREA ŞI ASIGURAREA FUNCŢIONĂRII SI RSDG**

**21.** SI RSDG se ține în limba română în formă electronică.

**22.** Posesorul SI RSDG efectuează administrarea acestuia cu ajutorul complexului de mijloace software şi hardware, în corespundere cu prezentul Regulament.

**23.** Păstrarea şi dezvoltarea SI RSDG sunt asigurate de către posesor până la adoptarea deciziei de scoatere a acestuia din exploatare. În cazul în care sistemul este scos din exploatare, datele şi documentele conținute în acesta se transmit în arhivă conform legislației.

**24.** Răspunderea pentru veridicitatea şi corectitudinea datelor şi a informațiilor incluse, precum şi pentru respectarea obligației de înregistrare a datelor le revine furnizorilor de date, registratorilor și utilizatori.

**25.** Toate înregistrările şi modificările operate în SI RSDG se păstrează în ordine cronologică.

**26.** Obiectele informaționale şi scenariile de bază ale SI RSDG sunt descrise la pct. 42 din Anexa nr.1 la prezenta hotărâre.

**V. REGIMUL JURIDIC DE UTILIZARE A DATELOR DIN SI RSDG**

**Secțiunea 1**

**Accesul la datele Registrului**

**27.** Registratorii, furnizorii de date și utilizatorii beneficiază de drepturi de acces la informația din SI RSDG conform atribuțiilor şi funcțiilor deținute şi regimul juridic al informației accesate.

**28.** Nivelul de acces la informație pentru fiecare participant corespunde funcției de serviciu şi profilului de acces. Informația conținută în SI RSDG se accesează în conformitate cu Legea nr. 982/2000 privind accesul la informație şi în limitele stabilite de aceasta, precum şi în conformitate cu alte acte normative.

**29.** Dreptul de acces la resursele informaționale ale SI RSDG este segmentat pe unități de conținut, atribuind prerogative partajate, şi anume: înregistrarea, vizualizare, modificare (corectare, completări, schimbarea datelor. etc.) şi radiere.

**30.** Punerea la dispoziție a datelor din SI RSDG se realizează prin:

1) acordarea accesului autorizat la sistem;

2) eliberarea documentelor pe suport de hârtie, conform prevederilor normative;

3) acordarea informației prin intermediul poștei electronice sau al altor mijloace de comunicații electronice/aplicații web, conform prevederilor normative.

**31.** Datele cu caracter personal ale persoanelor fizice se utilizează în conformitate cu prevederile Legii nr. 133/2011 privind protecția datelor cu caracter personal.

**32.** Datele recepționate din SI RSDG nu pot fi transmise persoanelor terțe, dacă legislația sau tratatele internaționale la care Republica Moldova este parte nu prevede acest lucru.

**33.** Dreptul de acces nu este unul permanent, acesta poate fi suspendat sau revocat. Introducerea şi/sau modificarea datelor de pe un nume sau profil de registrator, furnizor de date și utilizator este interzisă, urmând a fi considerată ca acces neautorizat. Registratorul, furnizorul de date și utilizatorul urmează să se asigure de faptul că profilul acestora, precum şi semnătura electronică sunt confidențiale.

**34.** Revocarea/suspendarea dreptului de acces se efectuează la cerere de către deținător, în una dintre următoarele situații:

1) la încetarea/suspendarea raporturilor de serviciu/de muncă ale registratorului, furnizorului de date și utilizatorului;

2) la intervenirea modificărilor raporturilor de serviciu/de muncă, când noile atribuții nu impun accesul la datele din SI RSDG;

3) la constatarea de către posesor sau deținător a încălcării securității informaționale;

4) în alte cazuri, în limitele legislației.

**Secțiunea a 2-a**

**Înregistrarea și utilizarea informației în SI RSDG**

**35.** Înregistrarea datelor cu privire la obiectele informaționale în SI RSDG se efectuează de către registratori.

**36.** Înregistrarea se efectuează în ordine cronologică, fiecărei înregistrări fiindu-i atribuită data efectuării înscrierii în SI RSDG.

**37.** Fiecărui obiect informațional i se atribuie un cod unic de identificare generat de SI RSDG, după introducerea completă sau parțială a datelor cu privire la obiectul informațional.

**38.** Codul de identificare a înregistrării este unic, invariabil şi nu poate fi atribuit altor înregistrări, inclusiv după radierea acestuia din SI RSDG.

**39.** Înregistrarea se face prin utilizarea datelor de referință ADN.

**40.** Se interzice utilizarea datelor în scopuri care contravin legii.

**41.** Orice modificare şi completare în SI RSDG a obiectelor informaționale, precum şi scoaterea din evidență a acestora se efectuează doar în baza documentelor justificative, cu indicarea motivului ce confirmă veridicitatea acțiunilor efectuate în sistem.

**42.** Toate modificările operate în SI RSDG se păstrează în ordine cronologică, cu păstrarea nemijlocită a istoricului acestora. Modificarea sau completarea datelor nu afectează accesarea şi vizualizarea informației din sistem.

**43.** Pentru modificarea datelor se impun următoarele restricții:

1) registratorii pot modifica datele doar în conformitate cu atribuțiile pe care le au în cadrul SI RSDG în temeiul unor motive și/sau documentelor justificative;

2) utilizatorii nu sunt în drept să modifice datele obținute din SI RSDG, iar la utilizarea acestora sunt obligați să indice sursa lor;

3) alte categorii de subiecți sunt restricționați în utilizarea datelor din SI RSDG în conformitate cu prevederile Legii nr.133/2011 privind protecția datelor cu caracter personal.

**44.** Actualizarea informațiilor de către furnizorii de date nu este considerată corectare a acestora. Furnizorii de date sunt obligați să asigure corectitudinea şi autenticitatea datelor prezentate pentru a fi înscrise în SI RSDG, precum şi să asigure actualizarea acestora în modul stabilit de legislație sau în baza acordurilor cu privire la schimbul de informații şi interoperabilitate.

**45.** SI RSDG utilizează datele până la atingerea scopului, ulterior permite arhivarea datelor şi a documentelor în format electronic, în vederea eficientizării procesului de prelucrare şi furnizare către utilizator al informației documentate.

**46.** Radierea automată a informației genetice din registru se efectuează în conformitate cu art. 11 din Legea nr. 235/2017 cu privire la înregistrarea genetică.

**47.** Radierea imediată a informației genetice se efectuează la solicitarea persoanei conform prevederilor art. 13 din Legea nr. 235/2017 cu privire la înregistrarea genetică.

**48.** În cazul radierii informației genetice, este nimicit şi materialul biologic corespunzător.

**49.** Datele cu caracter personal sunt șterse din SI RSDG odată cu profilele ADN.

**50.** Termenul de păstrare a documentelor electronice este identic cu termenul prevăzut de legislație pentru păstrarea documentelor echivalente pe suport de hârtie.

**Secțiunea a 3-a**

**Căutarea şi compararea automatizată a pofilelor genetice**

**51.** Solicitările internaționale, privind căutarea şi compararea profilelor genetice se efectuează prin intermediul punctului național de contact – Direcția cooperare polițienească internațională a Inspectoratului General al Poliției al MAI sau prin alte căi de contact stabilite oficial.

**52.** Căutarea şi compararea profilelor genetice se poate realiza în baza cererilor de asistență polițienească primite în condițiile Legii nr. 371/2006 cu privire la asistența juridică internațională în materie penală.

**53.** Compararea a două profile genetice se efectuează, pe baza locilor pentru care, în ambele profile genetice, este disponibilă o pereche de valori ale alelelor.

**54.** În cazul în care, în urma unei căutări şi contrapunerii unui profil genetic identificat sau neidentificat, nu s-a obținut nici o concordanță în SI RSDG, sau s-a obținut o concordanță corespunzând unui profil genetic neidentificat, acest profil, poate fi transmis ulterior pentru verificarea în bazele de date ale altor state, la solicitarea organului competent.

**55.** În cazul în care, în urma unei căutări potrivit pct. 52 se obțin concordanțe cu profiluri genetice de referință şi/sau profiluri genetice neidentificate din bazele de date ale altor state, aceste concordanțe sunt comunicate utilizatorului extern, cu transmiterea datelor de referință.

**56.** Dacă nu pot fi obținute concordanțe în bazele de date ale altor state, acest fapt se comunică utilizatorului extern (statului solicitant).

**57.** În cazul în care, în urma unei căutări cu ajutorul unui profil genetic neidentificat, se obține o concordanță în bazele de date ale altor state, registratorul adaugă o notă explicativă, în acest sens, în sistem.

**58.** În cazul în care se indică o concordanță între profilele genetice, furnizarea de date suplimentare cu caracter personal şi alte informații în legătură cu datele de referință se realizează, după caz, în condițiile Legii nr. 371/2006 cu privire la asistența juridică internațională în materie penală.

**Secțiunea a 4-a**

**Activitatea de ținere a bazei de date ADN de eliminare**

**59.** Baza de date ADN de eliminare are menirea să păstreze profilurile ADN ale persoanelor care potențial ar putea contamina probele de ADN. Informațiile stocate în această bază de date au cicluri de viață diferite comparativ cu baza de date ADN criminalistică. Acesta este determinat de faptul că obiectele informaționale aparțin procesului de extragere a profilurilor ADN și nu sunt în mod necesar conexe cauzei anchetate.

**60.** Cu toate că fluxurile de lucru din cadrul bazei de date ADN de eliminare sunt relativ simple, ar trebui examinate următoarele aspecte:

1) gestionarea personalului care prezintă risc de contaminare.

2) identificarea terților care au putut contamina probele biologice este esențială pentru investigațiile criminalistice. Se recomandă definirea grupurilor de persoane în conformitate cu riscul de contaminare și instituirea unor proceduri de lucru standard pentru fiecare grup. Vor fi examinate, cel puțin, următoare grupuri:

a) profiluri ale personalului de poliție;

b) personal suplimentar care nu face parte din organele de poliție;

c) medici legiști;

d) personal implicat în sfera de producție;

e) personalul de laborator /al furnizorilor de servicii de expertiză criminalistică;

f) contaminanți dintr-o sursă necunoscută.

3) Organizarea bazelor de date de eliminare.

**61.** Principalele părți interesate în materie de politici și standarde ar trebui să agreeze la nivel național o abordare unificată pentru organizarea și utilizarea bazelor de date ADN de eliminare care cuprind baze de date ADN de eliminare gestionate la nivel local, național (central)și internațional. Scopul exclusiv al acestei abordări este depistarea contaminării potențiale din partea personalului implicat în fabricarea consumabilelor (tampoane, tuburi etc.) și colectarea și prelucrarea mostrelor ADN.

**62.** Vor fi stabilite și menținute seturile de date de profil de eliminare în cadrul cărora vor fi păstrate profilurile următoarelor grupuri și comparate cu urmele/petele și profilurile ADN de referință în vederea identificării potențialelor evenimente de contaminare a ADN (ISO/IEC 17025):

a) personalul de laborator /al furnizorilor de servicii de expertiză criminalistică care prelucrează mostrele probatorii și orice vizitatori ai facilității care prezintă risc de contaminare a probelor de ADN prelucrate în cadrul organizației, de exemplu, setul de date de eliminare ale personalului de laborator (SED);

b) personalul de poliție, atât ofițerii, cât și personalul civil, de exemplu, setul de date de eliminare ale personalului național (central), de exemplu, baza de date pentru eliminarea contaminării (CED);

c) toți medicii legiști, personalul centrului de specialitate în domeniul abuzurilor sexuale, patologii și medicii implicați direct sau indirect în recuperarea probelor de la victimele infracțiunii, supraviețuitoare și decedate, sau bănuiții arestați, de exemplu, setul de date de eliminare ale personalului național (central), de exemplu, baza de date pentru eliminarea contaminării (CED);

d) personalul implicat direct în procesul de producție și asamblare a consumabilelor utilizate pentru colectarea, păstrarea și prelucrarea materialului în vederea generării profilurilor ADN, de exemplu, seturi de date de eliminare ale personalului național (central) sau internațional, de exemplu, baza de date pentru eliminarea contaminării (CED), baza de date de eliminare a producătorilor (MED) și/sau baza de date de excludere a ICMP (Comisiei internaționale pentru persoane dispărute);

e) contaminanți dintr-o sursă necunoscută, baza de date ADN de contaminare (CDD).

**63.** La cererea donatorului, poate fi examinată posibilitatea de a oferi copii legalizate (semnate electronic) ale profilurilor ADN din baza de date ADN de eliminare. Această copie legalizată poate fi utilizată în calitate de „pașaport biometric”, eliminând necesitatea de a fi reprofilat în cazul în care, de exemplu, persoana își schimbă locul de muncă la alt FSP sau solicită acces la zonele sensibile conexe ADN într-o organizație diferită.

**64.** Interfața cu bazele de date de eliminare internaționale ale producătorilor – Ministerul Afacerilor Interne trebuie să ia în considerare semnarea acordurilor pentru a obține profilurile ADN ale persoanelor care au fabricat echipamentul și materialele utilizate pentru extragerea ADN. Aceste profiluri ar trebui să fie incluse în baza de date de eliminare pentru grupul „personal din sfera de producție”.

**65.** Perioadele de păstrare a bazei de date de eliminare – se va acorda atenție perioadelor de păstrare care sunt relevante pentru rolul lor după ce membrii de personal și-au încetat activitatea și perioada de timp preconizată în care acel material relevant gestionat de ei va ajunge în cadrul sistemului de justiție penală (CJS) înainte de generarea profilurilor ADN.

**66.** Arhiva – trebuie să fie determinate cerințele ce vizează arhivele și perioada de păstrare pentru fiecare baza de date de eliminare sau rol al membrilor de personal.

**67.** Atunci când obiectul înregistrării este înlăturat, profilul ADN este transferat în arhiva digitală, iar odată cu transferarea în arhivă, datele cu caracter personal sunt eliminate, respectiv accesul la datele din arhivă este acordat în conformitate cu legislația cu privire la arhive și cu Regulamentul de păstrare a arhivei Ministerului Afacerilor Interne.

**68.** În scopul căutării și comparării profilurilor ADN, solicitarea pentru efectuarea comparației poate fi realizată de persoanele autorizate să acceseze datele din RSDG. Răspunsul (raportul despre concordanță) la solicitarea pentru efectuarea comparației profilului ADN trebuie să conțină doar indicații suficiente pentru a identifica înregistrarea din registru și dacă au existat una sau mai multe concordanțe (hit-uri) sau nu a fost identificată nicio concordanță (hit).

**69.** Profilurile ADN pot fi comparate prin diferite metode. În CODIS, acestea sunt numite rigurozități de căutare: „Rigurozitate ridicată” înseamnă că toate alelele din fiecare locus prezent în cadrul unui profil ADN trebuie să fie prezent în profilul ADN concordant în exact aceiași cantitate; „Rigurozitate moderată” înseamnă că, din două profiluri ADN, alelele unui locus cu cel mai mic număr de alele trebuie să fie prezent în locusul corespunzător al altor profiluri ADN. Această rigurozitate este utilizată atunci când se face comparația profilurilor ADN mixte cu profilurile ADN unitare.

**70.** Dat fiind faptul că în CODIS homozigoții sunt desemnați de o singură valoare a alelei, căutarea cu rigurozitate moderată în cadrul profilurilor ADN unitare poate depista, de asemenea, alelele excluse din unul dintre profilurile ADN comparate (de ex., 12/13 va concorda cu homozigoții aparenți 12/ sau 13/); „Rigurozitate scăzută” înseamnă că în fiecare locus comparat între două profilurilor ADN, cel puțin o alelă din acel locus a concordat.

**VI. INTERACŢIUNEA CU ALTE SISTEME INFORMAŢIONALE ŞI CU SISTEMELE INFORMAŢIONALE PARTAJATE**

**71.** SI RSDG este găzduit pe platforma tehnologică guvernamentală comună (MCloud) și interacționează, cu următoarele sisteme informaționale de stat:

1) Sistemul informațional automatizat „Registrul de stat al populației” – pentru schimbul automatizat de date privind persoanele fizice pasibile de înregistrare genetică conform art. 8 din Legea nr. 235/2017 cu privire la înregistrarea genetică;

2) Sistemul informațional „Registrul de stat al actelor juridice” – pentru schimbul automatizat de date privind actele normative aferente procedurii de înregistrare genetică;

3) Sistemul informațional judiciar – pentru schimbul automatizat de date privind actele judecătorești (încheieri, hotărâri, decizii emise de către instanța de judecată);

4) Sistemul informațional „Gestiunea dosarelor de expertiză judiciară” - pentru schimbul automatizat de date privind expertizele genetice judiciare;

5) alte sisteme informaționale stabilite de cadrul normativ aplicabil.

Dacă pentru efectuarea înregistrării genetice de stat legislația prevede deținerea unui document ale cărui date sunt disponibile în resursele informaționale ale altor instituții de stat, ele pot fi consumate sau furnizate prin intermediul Platformei de interoperabilitate (MConnect).

**72.** SI RSDG va interacționa cu următoarele sisteme informaționale partajate:

1) Platforma tehnologică guvernamentală comună (MCloud) – pentru găzduirea sistemului;

2) Platforma de interoperabilitate (MConnect) – pentru schimbul de date cu alte sisteme informaționale şi registre;

3) Serviciul electronic guvernamental integrat de semnătură electronică (MSign) – pentru semnarea documentelor electronice;

4) Serviciul electronic guvernamental de autentificare şi control al accesului (MPass) – pentru autentificarea şi controlul accesului în cadrul sistemului;

5) Serviciul electronic guvernamental de jurnalizare (MLog) – pentru asigurarea evidenței operațiunilor (evenimentelor) produse în cadrul SI RSDG;

6) Serviciul electronic guvernamental de notificare (MNotify) – pentru notificarea furnizorilor de date, registratorilor și utilizatorilor;

7) Sistemul informațional automatizat „Registrul împuternicirilor de reprezentare în baza semnăturii electronice” (MPower) – pentru validarea împuternicirilor de reprezentare;

8) Serviciul guvernamental de livrare (MDelivery) – pentru oferirea unui mecanism unic de livrare fizică a rezultatelor din cadrul procesului de înregistrare genetică judiciară.

**VII. ASIGURAREA PROTECŢIEI ŞI SECURITĂŢII**

**INFORMAŢIEI SI RSDG**

**73.** Datele din SI RSDG fac parte din categoria datelor care necesită a fi protejate. Asigurarea securității, confidențialității şi a integrității datelor prelucrate în cadrul SI RSDG se efectuează de către subiecții cu drepturi de acces la sistem şi cu respectarea cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora.

**74.** Măsurile de protecție şi securitate a datelor din SI RSDG reprezintă totalitatea acțiunilor juridice, organizatorice, economice şi tehnologice orientate spre prevenirea pericolelor asociate resurselor şi infrastructurii informaționale.

**75.** Din motive criminalistice și în temeiul legislației privind protecția datelor cu caracter personal, profilurile ADN și informațiile asociate ar trebui introduse și stocate în mod corect, prin evitarea introducerii manuală a profilurilor ADN.

**76.** Accesul la baza de date ADN trebuie să fie limitat prin măsuri fizice și organizaționale numai la persoanele care solicită accesul. Periodic, trebuie să fie făcute copii de rezerva care să fie stocate într-un loc sigur și recuperate periodic pentru a simula restabilirea în urma unui dezastru.

**77.** Atunci când profilurile ADN și informațiile asociate acestora sunt prezente în sisteme diferite, aceste sisteme trebuie să fie comparate periodic pentru a verifica că sunt sincronizate în mod adecvat.

**78.** Obiecte ale asigurării protecției şi securității datelor din SI RSDG se consideră tot complexul de mijloace software şi hardware care asigură realizarea proceselor informaționale, şi anume:

1) baza de date, sistemele informaționale, sistemele operaționale, sistemele de gestiune a bazelor de date, sistemele de evidență şi alte aplicații care asigură funcționarea SI RSDG;

2) sistemele de comunicații electronice, rețelele, serverele, calculatoarele şi alte mijloace tehnice de prelucrare a datelor.

**79.** Securitatea informațională a SI RSDG se efectuează prin aplicarea metodelor şi efectuarea acțiunilor descrise în Planul de continuitate al acestuia şi, după caz, a procedurilor operaționale.

**80.** Protecția datelor din SI RSDG se realizează prin următoarele metode:

1) prevenirea acțiunilor intenționate şi/sau neintenționate care pot duce la distrugerea sau denaturarea datelor;

2) utilizarea obligatorie a produselor de program licențiate şi aprobate. Orice solicitare de instalare a unui produs de program trebuie coordonată cu administratorul tehnic;

3) monitorizarea procesului de exploatare al SI RSDG prin intermediul mecanismului de jurnalizare efectuat de către deținătorul tehnic al acestuia.

**81.** la utilizarea şi exploatarea SI RSDG, subiecții asigură implementarea normelor de securitate, acestea urmând să conțină următoarele acte confirmative:

1) identitatea persoanei responsabile de implementarea normelor de securitate şi împuternicirile acesteia;

2) implementarea principalelor măsuri tehnico-organizatorice necesare asigurării funcționării SI RSDG;

3) implementarea procedurilor interne ce exclud cazurile de modificare nesancționată a mijloacelor software şi/sau a informației din SI RSDG;

4) informarea registratorilor, furnizorilor de date și utilizatorilor şi instruirea acestora cu privire la modalitățile şi mecanismele de asigurare a securității informaționale;

5) procedurile de control intern al subiectului SI RSDG privind respectarea condițiilor de securitate informațională.

**82.** Schimbul informațional se efectuează cu utilizarea mijloacelor software şi hardware, doar prin canale securizate, asigurând integritatea şi securitatea datelor.

**83.** Deținătorul desemnează o persoană subordonată nemijlocit conducătorului instituției, responsabilă de implementarea şi monitorizarea respectării normelor de securitate informațională.

**84.** Normele de securitate informațională se aduc la cunoștință registratorilor, furnizorilor de date și utilizatorilor și sunt obligatorii pentru respectare.

**VIII. ASIGURAREA CONTROLULUI INTERN ȘI EXTERN ŞI RESPONSABILITATEA SI RSDG**

**85.** SI RSDG este supus controlului intern şi extern. Controlul intern privind organizarea şi funcționarea SI RSDG se efectuează de către posesor. Controlul extern asupra respectării cerințelor privind crearea, ținerea, exploatarea şi reorganizarea SI RSDG se efectuează de către instituții abilitate şi certificate în domeniul auditului.

**86.** SI RSDG se înregistrează în Registrul resurselor şi sistemelor informaționale de stat şi în Registrul de evidență a operatorilor de date cu caracter personal.

**87.** Responsabilitatea pentru organizarea funcționării SI RSDG aparține posesorului/deținătorului acestuia.

**88.** Subiecții sistemului, în atribuțiile cărora intră ținerea SI RSDG, introducerea datelor, furnizarea informațiilor şi asigurarea funcționării acestuia, poartă răspundere personală, în conformitate cu legislația, pentru completitudinea, autenticitatea, veridicitatea, integritatea informației, precum şi pentru păstrarea şi utilizarea ei. Încălcarea prezentului Regulament se pedepsește pe cale civilă, contravențională sau penală.

**89.** Toți subiecții SI RSDG poartă răspundere, conform legislației, pentru prelucrarea, divulgarea, transmiterea informației din sistem persoanelor terțe, contrar legislaţiei.

**90.** Anual, până la data de 31 ianuarie, posesorul prezintă Centrului Național pentru Protecția Datelor cu Caracter Personal un raport generalizat despre incidentele de securitate din cadrul SI RSDG, în conformitate cu pct. 90 din 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. 1123/2010.

**91.** Controlul legalității operațiunilor de prelucrare a datelor cu caracter personal desfășurate în SI RSDG se efectuează de către Centrul Național pentru Protecția Datelor cu Caracter Personal.

**92.** Pentru asigurarea funcționalității eficiente şi neîntrerupte a SI RSDG, schimbul informațional de date este asigurat în regim nonstop.

**93.** Lucrările profilactice planificate în complexul de mijloace software şi hardware se efectuează după notificarea, în scris sau prin e-mail, a registratorilor de către deținător, în baza planului coordonat cu administratorul tehnic, cu cel puțin două zile lucrătoare înainte de începerea lucrărilor, cu indicarea termenului de finalizare a acestora, după caz, dacă aceasta este posibil. Lucrările profilactice neplanificate se efectuează la solicitarea registratorului şi coordonarea prealabilă cu deținătorul în situația nefuncționării sau funcționării necorespunzătoare a complexului de mijloace software şi hardware.

**94.** Funcționarea SI RSDG se suspendă de către administratorul tehnic, la inițiativa proprie sau la demersul posesorului, care asigură funcționalitatea sistemului informațional şi a resurselor informaționale, după coordonarea prealabilă cu deținătorul, în caz de apariție a uneia dintre următoarele situații:

1) în timpul efectuării lucrărilor profilactice ale complexului de mijloace software şi hardware al SI RSDG;

2) la apariția circumstanțelor de forță majoră;

3) la încălcarea cerințelor sistemului securității informației, dacă aceasta prezintă pericol pentru funcționarea SI RSDG;

4) în cazul apariției dificultăților tehnice în funcționarea complexului de mijloace software şi hardware al SI RSDG;

5) la cererea scrisă a posesorului.

**95.** În cazul apariției circumstanțelor de forță majoră şi a dificultăților tehnice în funcționarea complexului de mijloace software şi hardware ale SI RSDG din vina terțelor persoane, poate fi sistată funcționarea sistemului, cu informarea subiecților SI RSDG prin mijloacele tehnice disponibile.