GUVERNUL REPUBLICII MOLDOVA

HOTĂRÎRE nr._____/2019

Chișinău

pentru aprobarea Regulamentului privind organizarea şi funcţionarea „Registrului de stat dactiloscopic"

În temeiul Legii nr.1549/2002 cu privire la înregistrarea dactiloscopică de stat (Monitorul Oficial al Republicii Moldova, 2003, nr.14-17, art.51) și Legii nr.71/2007 cu privire la registre (Monitorul Oficial al Republicii Moldova, 2007, nr.70-73 art.314),

Guvernul HOTĂRĂŞTE:

1. Se instituie Registrul de stat dactiloscopic format de Sistemul informaţional automatizat „Registrul de stat dactiloscopic".
2. Se aprobă Regulamentul privind modalitatea de ținere a Registrului de stat dactiloscopic format de Sistemul informațional automatizat „Registrul de stat dactiloscopic" (conform anexei).
3. Se stabilește că cheltuielile pentru organizarea şi funcţionarea Sistemului informaţional automatizat „Registrul de stat dactiloscopic" se vor efectua din contul şi în limitele alocațiilor aprobate anual în bugetul Ministerului Afacerilor Interne, precum și din contul mijloacelor speciale prevăzute de lege, inclusiv a mijloacelor obținute din prestarea serviciilor.
4. Controlul asupra executării prezentei hotărîri se pune în sarcina Ministerului Afacerilor Interne.

Prim-ministru **Maia SANDU**

Contrasemnează:

Viceprim-ministru,
ministru al afacerilor interne Andrei NĂSTASE

Aprobat
prin Hotărîrea Guvernului
nr._____/2019

REGULAMENT
privind modalitatea de ținere a Registrului de stat dactiloscopic format de Sistemul informațional automatizat „Registrul de stat dactiloscopic"

I. Dispoziții generale

1. Regulamentul privind modalitatea de ținere a Registrului de stat dactiloscopic format de Sistemul informațional automatizat „Registrul de stat dactiloscopic" (în continuare Regulament) stabileşte modul de organizare şi mecanismul de funcţionare a sistemului informaţional automatizat „Registrul dactiloscopic".

2. Sistemul informațional automatizat „Registrul de stat dactiloscopic" (în continuare Sistem) reprezintă resursa informațională a Sistemului informațional al organelor de drept.

3. Sistemul reunește masivul dactiloscopic al persoanelor pasibile înregistrării dactiloscopice şi al cadavrelor neidentificate, precum şi masivul dactiloscopic al urmelor papilare şi palmare ridicate în cadrul cercetării la fața locului şi este destinat pentru formarea, acumularea, stocarea, actualizarea şi procesarea informației dactiloscopice în Republica Moldova.

4. Regulamentul determină subiecții relațiilor de drept în domeniul creării şi funcţionării Sistemului, drepturile şi obligaţiile subiecților relațiilor de drept în domeniul creării şi exploatării Sistemului, obiectele informaţionale şi lista datelor introduse, procedura de acumulare şi managementul datelor, interacţiunea cu alte registre, modul de asigurare a funcţionalităţii, precum şi metodele de protecţie a datelor.

5. În sensul prezentului Regulament, se definesc următoarele noțiuni:

administrator – entitatea responsabilă de gestionarea şi operarea resurselor informaționale ale Sistemului;

date de referință – ansamblu de date constituit din date dactiloscopice și un număr de referință, ce nu permite identificarea directă a unei persoane;

căutare și comparare – procedurile prin care se stabilește dacă există o concordanță între datele dactiloscopice și datele de referință stocate în sistemele automatizate de identificare dactiloscopică;

căutare automatizată – procedura de acces direct printr-un serviciu de comunicații electronice pentru căutarea și compararea datelor de referință în sistemele automatizate de identificare dactiloscopică;

informație dactiloscopică – date dactiloscopice, date cu caracter personal, precum și date despre caz;

număr de referință – număr format din combinația următoarelor elemente: un cod care permite identificarea și extragerea datelor cu caracter personal și a altor informații din sistemul automatizat de identificare dactiloscopică și un cod care indică originea națională a datelor dactiloscopice;

prelucrarea informației dactiloscopice – acțiunile necesare privind verificarea corectitudinii, calității, plenitudinii, precum și sistematizarea informației dactiloscopice.

6. Sistemul este utilizat pentru păstrarea, prelucrarea și furnizarea informației dactiloscopice.

7. Informația stocată în Sistem se utilizează pentru:

1) căutarea și stabilirea identității cetățenilor Republicii Moldova și a străinilor dispăruți fără urmă;

2) stabilirea identității cadavrelor neidentificate;

3) stabilirea și/sau confirmarea identității cetățenilor Republicii Moldova și a străinilor, dacă aceasta nu este posibilă prin utilizarea altor mijloace;

4) prevenirea și combaterea criminalității.

8. Interoperabilitatea Sistemului cu alte Resurse informaționale de stat, ce fac parte din Sistemul informațional automatizat al organelor de drept (*Hotărîrea Guvernului nr.1202/2006 cu privire la aprobarea Concepției Sistemului informațional integrat al organelor de drept*), urmează a fi realizată în conformitate cu prevederile Hotărîrii Guvernului nr.565/2007 cu privire la aprobarea concepției Sistemului informațional automatizat „Registrul dactiloscopic" și în conformitate cu prevederile Legii nr.142/2018 cu privire la schimbul de date și interoperabilitate.

9. Acțiunea prezentului Regulament nu se extinde asupra relațiilor ce apar la preluarea datelor dactiloscopice în cadrul procesului de perfectare și eliberare a actelor de identitate care conțin date biometrice.

10. Totalitatea informațiilor documentate și ținute în Sistem este organizată în conformitate cu Legea nr.71/2007 cu privire la registre.

11. În condițiile prezentului Regulament, vor fi prelucrate doar date cu caracter personal strict necesare, neexcesive scopului prestabilit, conform competențelor atribuite organelor competente, asigurîndu-se un nivel de securitate și confidențialitate adecvat în ceea ce privește riscurile prezentate de prelucrare și caracterul datelor, conform principiilor stabilite de legislația privind protecția datelor cu caracter personal.

12. În cadrul operațiunilor de prelucrare a datelor cu caracter personal efectuate conform prezentului Regulament se asigură respectarea drepturilor subiecților de date cu caracter personal, conform prevederilor Legii privind protecția datelor cu caracter personal.

13. Sistemul va fi găzduit, după caz, pe platforma tehnologică guvernamentală comună (MCloud), în conformitate cu Hotărârea Guvernului nr.128/2014 privind platforma tehnologică guvernamentală comună (MCloud).

II. Subiecții relațiilor de drept în domeniul creării și exploatării Sistemului

14. Subiecții relațiilor de drept în domeniul creării și exploatării Sistemului sunt:

1) posesorul Sistemului;

2) deținătorul Sistemului;

3) registratorul datelor dactiloscopice;

4) furnizorul datelor dactiloscopice;

5) destinatarul informației dactiloscopice.

15. Posesorul Sistemului este Ministerul Afacerilor Interne, care asigură condițiile juridice, organizatorice şi financiare pentru crearea şi ținerea acestuia.

16. Deținătorul Sistemului este Serviciul tehnologii informaționale al Ministerului Afacerilor Interne, care este responsabil de gestionarea Sistemului.

17. Registratorul datelor dactiloscopice în Sistem sunt subdiviziunile specializate ale Centrului tehnico-criminalistic şi expertize judiciare al Inspectoratului General al Poliției al Ministerului Afacerilor Interne şi subdiviziunile specializate ale Serviciului tehnologii informaționale al Ministerului Afacerilor Interne, ale căror atribuții de serviciu presupun acțiuni de primire, verificare, înregistrare, sistematizare şi eliberare a datelor dactiloscopice din Sistem.

18. Furnizori ai datelor registrului sunt persoanele fizice sau persoanele juridice de drept privat sau public, care prezintă registratorului date despre obiectul registrului în modul stabilit de lege sau acord.

19. Destinatarii informației dactiloscopice sunt:

1) procurorii, ofițerii de urmărire penală, ofițerii de investigații care desfăşoară activități speciale de investigații în scopurile prevăzute la pct.6 al prezentului Regulament;

2) statele cu care Republica Moldova a încheiat tratate în domeniu în scopurile prevăzute la pct.6 al prezentului Regulament.

III. Ținerea şi asigurarea funcționării Sistemului

20. Resursele informaționale ale Sistemului includ masivul dactiloscopic, creat în procesul înregistrării dactiloscopice de stat, format şi gestionat de Serviciul tehnologii informaționale al Ministerului Afacerilor Interne, precum şi masivul de urme digitale şi palmare ridicate în cadrul cercetării la fața locului, format şi gestionat de Centrul tehnico-criminalistic şi expertize judiciare al Inspectoratului General al Poliției al Ministerului Afacerilor Interne.

21. Resursele informaționale ale Sistemului se țin în formă electronică.

22. Modul automatizat de ținere a resurselor informaționale presupune şi utilizarea de sisteme automatizate de identificare dactiloscopică.

23. La formarea resurselor informaționale este permisă utilizarea scanerelor.

24. Informația dactiloscopică conținută în Sistem se ține în limba de stat şi în limba rusă.

25. Înregistrarea informației dactiloscopice în Sistem se efectuează:

1) prin scanare de către Registrator a fişelor dactiloscopice şi a urmelor digitale şi palmare recepționate de la furnizorii de informații dactiloscopice;

2) prin stocarea datelor dactiloscopice transmise printr-un document electronic;

3) în regim online de către Registrator direct în Sistem, utilizînd aplicația software specializată în combinație cu live-scanere.

În toate cazurile, datele trebuie să fie complete, calitative și veridice. În caz contrar, registratorul este în drept de a le restitui furnizorului pentru rectificare sau, după caz, preluare repetată a acestora.

26. Ordinea evidenței datelor în Sistem va fi asigurată de atribuirea fiecărui obiect, în mod obligatoriu, a unui identificator unic, care rămîne invariabil pe parcursul întregii perioade de existență a obiectului în registru. După radierea obiectului din registru, atribuirea identificatorului acestuia unui alt obiect este interzisă.

27. Actualizarea, completarea sau modificarea în datele obiectului din Sistem se efectuează în baza deciziei registratorului. Împreună cu datele modificate, în Sistem se introduce informația privitor la faptul înregistrării modificărilor operate în documentele în baza cărora a fost adoptată decizia de modificare.

Actualizarea, completarea sau modificarea informației dactiloscopice din Sistem va fi efectuată în cazul în care:

1) la prelucrarea acesteia au fost depistate date relevante despre identitatea persoanei, date despre caz sau modificări ale datelor dactiloscopice (cicatrice, lipsa degetului, ș.a.);

2) de către subiecții relațiilor de drept prevăzuți la punctul 14 subpunctele 3,4,5 a fost depusă o notificare motivată de actualizare, completare sau modificare a informației dactiloscopice din Sistem.

28. Radierea obiectului din Sistem se efectuează în baza deciziei registratorului în condițiile prevăzute de articolul 15 al Legii nr.1549/2002 „cu privire la înregistrarea dactiloscopică de stat" și aliniatul 5 al articolului 20 al Legii nr.71/2007 „cu privire la registre". Informația dată va fi utilizată în exclusivitate doar în scop de statistică.

29. Accesul la Sistem și schimbul informațional se realizează inclusiv prin Serviciul guvernamental de autentificare și control al accesului (MPass), iar schimbul informațional se realizează prin intermediul Platformei de schimb de date și interoperabilitate (MConnect).

30. Accesul la informația dactiloscopică se realizează prin nivele diferite de acces autorizat pentru fiecare destinatar.

31. Procesul de creare și înregistrare a destinatarului de informație se efectuează conform regulilor stabilite de Deținător, în conformitate cu prevederile Hotărîrii 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.

32. Accesul la informația din Sistem este asigurată de administrator și poate fi obținută de către Subiecții relațiilor de drept în domeniul creării și exploatării Sistemului în baza unei cereri scrise și motivate adresate Deținătorului Sistemului. Cererea trebuie să conțină numărul necesar de destinatari, IDNP, numele, prenumele, data, luna, anul nașterii și funcția acestora.

33. Funcționarea Sistemului se suspendă în caz de:

1) efectuare a lucrărilor de mentenanță;

2) situații excepționale;

3) constatare a unor amenințări la adresa securității informaționale a Registrului;

4) încălcare a cerințelor de funcționare a complexului de echipament tehnic-hardware și asigurare software.

34. Lucrările de mentenanță ale complexului de mijloace software și hardware se execută după anunțarea Subiecților relațiilor de drept în domeniul creării și exploatării Sistemului, în scris, la telefon sau prin e-mail, cel puțin cu o zi înainte de începerea lucrărilor, cu indicarea, după posibilitate, a termenelor de finalizare.

35. Se revocă dreptul de a accesa Sistemul dacă:

1) în adresa Deținătorului a parvenit solicitarea scrisă prin care informează excluderea destinatarului;

2) a fost încetat raportul de muncă dintre destinatar și angajatorul său;

3) a avut loc modificarea raporturilor de muncă dintre destinatar și angajatorul acestuia, cînd noile atribuții de serviciu nu presupun accesul la informația Sistemului;

4) au fost încălcate regulile de utilizare a Sistemului;

5) au fost constatate unele amenințări la adresa securității informaționale a Sistemului, la baza cărora au stat activitățile destinatarului.

Drepturile și obligațiile Posesorului și Deținătorului Sistemului

36. Posesorul Sistemului este obligat să asigure condițiile de drept, organizaționale și financiare pentru crearea și funcționarea Sistemului.

37. Deținătorul Sistemului este obligat:

1) să asigure funcționarea Sistemului;

2) să asigure posibilitatea de conectare a destinatarilor autorizați la Sistem;

3) să asigure crearea înregistrărilor de evidență (conturilor) pentru destinatarii Sistemului, cu atribuirea rolurilor și drepturilor de acces la interfață și date;

4) să asigure siguranța și integritatea datelor din Sistem;

5) să efectueze monitorizarea și controlul fluxului datelor din Sistem;

6) să asigure susținerea metodologică prin elaborarea procedurilor, regulilor și instrucțiunilor privind introducerea, acumularea, păstrarea, completarea, corectarea, sistematizarea și utilizarea datelor, precum și funcționarea Sistemului;

7) să asigure și să execute controlul Sistemului la compartimentul securității informaționale, să fixeze cazurile și tentativele de încălcare a ei, să ia măsurile corespunzătoare pentru prevenirea și eliminarea consecințelor;

8) să asigure accesul securizat la informația din Sistem și respectarea condițiilor generale de securitate și regulilor de exploatare a Sistemului;

9) să asigure, organizeze și să amenajeze locurile de muncă corespunzătoare pentru persoanele împuternicite, responsabile pentru deservirea Sistemului;

10) să asigure condiţiile necesare pentru păstrarea securizată a purtătorului de informaţie şi copiilor de rezervă care se efectuează automat în Sistem, precum şi pentru excluderea accesului persoanelor, care nu au permisiune la purtătorii corespunzători de informaţie;

11) să ofere asistenţa necesară persoanelor autorizate, care au acces la datele din Sistem, pentru utilizarea complexului de mijloace software a Sistemului;

12) să informeze Subiecţii relaţiilor de drept în domeniul creării şi exploatării Sistemului despre schimbările condiţiilor tehnice de funcţionare a Sistemului;

13) să asigure protecţia Sistemului împotriva viruşilor şi spam-ului;

14) să asigure deservirea tehnică a componentelor, înlăturarea defecţiunilor tehnice a locurilor de muncă automatizate conectate la Sistem;

15) să asigure implementarea măsurilor organizaţionale şi tehnice, necesare pentru asigurarea regimului de confidenţialitate şi securitate a datelor personale în corespundere cu Legea nr.133/2011 privind protecţia datelor cu caracter personal, precum şi respectarea cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, aprobate prin Hotărîrea Guvernului nr.1123/2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal;

16) să utilizeze informaţia din Sistem numai în scopurile stabilite la pct.6 al prezentului Regulament.

38. Deţinătorul Sistemului are dreptul:

1) să iniţieze elaborarea proiectelor de acte normative în domeniul funcţionării Sistemului;

2) să propună şi să implementeze soluţii pentru îmbunătăţirea şi creşterea eficacităţii procesului de funcţionare a Sistemului;

3) să monitorizeze situaţia la compartimentul securităţii informaţionale, să înregistreze cazurile şi încercările de apariţie a unor ameninţări;

4) să iniţieze procedura de revocare a drepturilor de acces la Sistem în cazurile prevăzute la punctul 35;

5) să solicite de la furnizori datele necesare pentru completarea informaţiei în Sistem;

6) să refuze eliberarea informaţiei din Sistem în cazul în care nu sunt respectate prevederile punctelor 7 şi 19 al prezentului Regulament.

Drepturile şi obligaţiile altor subiecţi ai Sistemului

39. Registratorul Sistemului este obligat:

1) să verifice plenitudinea informaţiei dactiloscopice înregistrate de către furnizor, transmise pentru introducere în Sistem;

2) să informeze în scris furnizorul despre motivele refuzului înregistrării informaţiei dactiloscopice în Sistem;

3) să asigure în procesul de vizualizare, colectare și prelucrare a informației dactiloscopice, respectarea drepturilor subiecților de date cu caracter personal conform prevederilor Legii nr.133/2011 cu privire la protecția dactelor cu caracter personal și Legii nr.1549/2002 cu privire la înregistrarea dactiloscopică de stat;

4) să asigure înregistrarea informației dactiloscopice în Sistem;

5) să respecte normele etice şi secretul profesional.

40. Furnizorii datelor dactiloscopice ai Sistemului sunt obligați:

1) să asigure plenitudinea informației dactiloscopice în procesul de colectare a acestei în strictă conformitate cu prevederile Legii nr.1549/2002 cu privire la înregistrarea dactiloscopică de stat;

2) să asigure în cadrul procesului de colectare, prelucrare și transmitere a informației dactiloscopice, respectarea prevederilor Legii nr.133/2011 cu privire la protecția dactelor cu caracter personal;

3) să asigure protecția informației dactiloscopică stocate sau transmise împotriva distrugerii accidentale ori ilicite, împotriva pierderii sau deteriorării accidentale şi împotriva stocării, prelucrării, accesării ori divulgării ilicite.

41. Destinatarul Sistemului este obligat:

1) să utilizeze informația obținută din Sistem numai în scop de serviciu;

2) să anunțe Deținătorul Sistemului despre cazurile de încălcare a securităţii informaţionale a Sistemului;

3) să anunțe Deţinătorul Sistemului despre apariţia situaţiilor de forţă majoră, care pot influenţa negativ asupra informațiilor din Sistem.

42. Subiecții relațiilor de drept în domeniul creării şi exploatării Sistemului au dreptul:

1) să participe la implementarea şi dezvoltarea Sistemului;

2) să înainteze Posesorului şi/sau Deţinătorului propuneri privind modificarea cadrului normativ care reglementează funcţionarea Sistemului;

3) să solicite şi să primească de la Deţinător asistenţă metodologică şi practică la compartimentul utilizării Sistemului;

4) să înainteze Deținătorului propuneri privind modalitățile de creştere a eficacităţii funcţionării Sistemului.

VI. Obiectul informațional al Sistemului

43. Conţinutul datelor şi dependenţa obiectelor informaţionale sunt descrise în documentația tehnică a Sistemului.

În Sistem se conțin:

1) date dactiloscopice;

2) date cu caracter personal, importate automatizat din Registrul de stat al populației, sau introduse manual de registratorul Sistemului;

3) date despre caz importate automatizat din Registrul informației criminalistice și criminologice sau introduse manual de registratorul Sistemului.

Datele sunt disponibile în Sistem numai pentru vizualizare și nu pot fi modificate.

44. Obiectele informaționale, care reprezintă resursa informațională a

Sistemului, sunt alcătuite din următoarele componente:

1) fișa dactiloscopică cu semnificațiile corespunzătoare;

2) urme papilare și palmare ridicate de la locul faptei.

45. Datele obiectelor informaționale sunt:

1) datele obiectului informațional „persoana fizică" pasibilă de înregistrare dactiloscopică în conformitate cu prevederile Legii nr.1549/2002 cu privire la înregistrarea dactiloscopică de stat sunt:

a) datele de identificare ale persoanei:

- numărul de identificare al solicitantului (în cazul persoanelor care dispun de IDNP), extrase din Registrul de stat al populației;
- numele;
- prenumele;
- patronimicul;
- data, luna, anul nașterii;
- locul nașterii;
- cetățenia;
- sexul;
- identificatorul unic de înregistrare în Sistem (generat în mod automatizat);
- fotografia;
- imagini de amprente digitale și palmare.

b) date suplimentare:

- tipul înregistrării dactiloscopice;
- categoria persoanei supuse înregistrării dactiloscopice;
- numărul de înregistrare a materialului/cauzei penale și alte informații relevante la acest subiect;
- articolul, alineatul, punctul din Codul penal sau Codul contravențional;
- data, luna, anul înregistrării datelor în Sistem;
- alte date relevante despre persoană.

2) datele obiectului informațional „cadavrul neidentificat" sunt:

a) identificatorul unic de înregistrare în Sistem;

b) imagini de amprente digitale și palmare;

c) date suplimentare (după caz);

d) numărul de înregistrare a materialului/cauzei penale și alte informații relevante la acest subiect;

e) data, luna, anul înregistrării datelor în Sistem;

f) alte date relevante despre cadavrul neidentificat.

3) datele obiectului informațional „furnizorul datelor dactiloscopice" sunt:

a) organul sau subdiviziunea instituției care a preluat și remis registratorului datele dactiloscopice (în cazul dactiloscopierii manuale) sau care a introdus în regim online datele în Sistem (în cazul dactiloscopierii automatizate);

b) țara, regiunea, raionul, orașul, organul (în cazul furnizorilor de date din alte state cu care sunt încheiate acorduri).

4) datele obiectului informațional „date dactiloscopice" sunt:

a) imagini de amprente digitale;

b) imagini de amprente digitale latente;

c) imagini de amprente palmare;

d) imagini de amprente palmare latente.

5) Atributele obiectului informațional „registrator și destinatar" sunt:

a) username;

b) nume, prenume;

c) numărul de identificare (IDNP);

d) stare (activă sau pasivă);

e) rolul;

f) subdiviziunea;

g) data creării în sistem.

6) datele obiectului informațional „fișa de evidență a urmei" sunt:

a) identificatorul unic de înregistrare al cartelei de urme în Sistem (generat în mod automatizat);

b) numărul de ordine al urmei;

c) numărul de înregistrare a materialului/cauzei penale;

d) tipul infracțiunii;

e) locul și data comiterii faptei;

f) datele de identificare ale candidatului sau infractorului;

g) date despre expertiză (țara, regiunea, raionul, orașul, data efectuării expertizei, numărul de înregistrare a expertizei, subdiviziunea care a efectuat raportul de expertiză, ș.a.);

h) date despre expert (nume, prenume, patronimic, funcția,);

j) informație suplimentară (persoanele verificate, locul pătrunderii, locul faptei de unde au fost ridicate datele dactiloscopice, metoda utilizată la ridicarea datelor dactiloscopice, angajatul care a depistat și ridicat datele dactiloscopice și alte note).

VII. Asigurarea protecției și securității informației Sistemului

46. Asigurarea securității, confidențialității și integrității datelor prelucrate în cadrul Sistemului se efectuează de către subiecții Sistemului cu respectarea cerințelor față de asigurare a securității datelor cu caracter personal conform prevederilor Hotărîrii Guvernului nr.1123/2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal.

47. Protecția informației dactiloscopice din Sistem la nivel de administrator se efectuează prin următoarele metode:

1) prevenirea conexiunilor neautorizate la rețelele de comunicații guvernamentale și interceptării datelor din Sistem transmise prin aceste rețele;

2) asigurarea măsurilor de protecție criptografice și tehnică a informațiilor;

3) excluderea accesului neautorizat la datele din Sistem;

4) efectuarea copiilor de siguranță a datelor și fișierelor mijloacelor de program;

5) asigurarea restabilirii și continuității funcționării Sistemului în cazul situațiilor excepționale.

48. Protecția informației dactiloscopice din Sistem la nivel de destinatar se efectuează prin prevenirea acțiunilor care pot duce la distrugerea sau denaturarea datelor din Sistem.

49. Accesul în Sistem este asigurat și autorizat inclusiv prin intermediul utilizării semnăturii electronice emise de către Centrul de certificare a cheilor publice a autorităților administrației publice. La începutul sesiunii de lucru fiecare destinatar trece procedura de autentificare în sistem, prin care se verifică corectitudinea identificatorului atribuit destinatarului dat. În caz de neconfirmare a autenticității destinatarului, accesul Sistem nu se permite.

50. Sesiunea de lucru în Sistem se blochează (la solicitarea destinatarului sau automat, după I5 minute de perioadă inactivă a destinatarului), fapt care face imposibil accesul de mai departe pînă în momentul cînd destinatarul nu deblochează sesiunea de lucru prin metoda trecerii repetate a procedurilor de identificare și autentificare.

51. În cadrul Sistemului se va asigura generarea și păstrarea înregistrărilor de audit a securității pentru operațiunile de prelucrare a datelor cu caracter personal, în condițiile Capitolului VIII din Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărîrea Guvernului nr.1123/2010.

52. Înregistrările de audit ale operațiunilor și rezultatele acestora vor putea fi accesate de Centrul Național pentru Protecția Datelor cu Caracter Personal și puse la dispoziția acestei autorități în scopul investigării potențialelor încălcări ale regimului de prelucrare/protecție a datelor cu carecter personal, doar în coordonare cu posesorul Sistemului.

53. În cazul producerii incidentelor de securitate în cadrul Sistemului, persoanele responsabile vor informa neîntîrziat conducerea, vor întreprinde măsurile necesare pentru înlăturarea consecințelor, cu informarea, în termen de 72 de ore din momentul producerii incidentului, a Centrului Național pentru Protecția Datelor cu Caracter Personal.

54. Administratorul Sistemului realizează politica de securitate informațională pentru asigurarea respectării regulilor, standardelor și normelor în domeniul securității informaționale.

55. Transmiterea transfrontalieră a informației din Sistem ce conțin date cu caracter personal pot avea loc doar în condițiile prevăzute de Legea nr.133/2011 privind protecția datelor cu caracter personal.

VIII. Controlul responsabilității

56. Controlul privind organizarea și funcționarea Sistemului se efectuează de către subdiviziunea specializată a Deținătorului Sistemului sau de către alte instituții abilitate și certificate în domeniul auditului informatic. Din cadrul acestor instituții vor fi desemnate persoane responsabile de administrarea și accesarea datelor dactiloscopice din Sistem.

57. Sistemul se înregistrează în Registrul de evidență al operatorilor de date cu caracter personal.

58. La efectuarea controlului, organul de control întocmeşte actul în două exemplare, din care unul este direcţionat către Deţinător, iar altul rămîne la organul de control. Deţinătorul este obligat să întreprindă la necesitate măsuri pentru lichidarea încălcărilor identificate şi să informeze despre aceasta organul de control.

59. Deţinătorul este responsabil pentru organizarea controlului de funcţionare a Sistemului, care este obligat să asigure dreptul de acces la Registru şi mijloacele de ţinere a lui.

60. Angajaţii Deţinătorului Sistemului, în atribuţiile cărora intră vizualizarea şi furnizarea datelor acestuia poartă răspundere disciplinară, civilă, contravenţională sau penală pentru integritatea informaţiei stocate.

61. Toţi subiecţii cu drept de acces la Sistem, precum şi destinatarul informaţiei, cu conţinut de date personale, sunt responsabili în faţa legii pentru dezvăluirea, transmiterea informaţiei din Sistem persoanelor terţe, contrar prevederilor legislaţiei în vigoare.

62. Păstrarea Sistemului este asigurată de Deţinător, pînă la decizia privind lichidarea sau transferul acestuia către alt Deţinător. În cazul lichidării Sistemului, toate datele conţinute în el sunt transmise spre stocare în arhivă.