



HOTĂRÎRE

cu privire la Sistemul informațional integrat al Poliției de Frontieră

[Denumirea modificată prin [Hot.Guv. nr.925 din 12.12.2012](#), în vigoare 25.12.2012]

nr. 834 din 07.07.2008

Monitorul Oficial nr.125-126/841 din 15.07.2008

* * *

Notă: Pe tot parcursul textului, cuvintele „Departamentul Poliției de Frontieră”, la orice caz gramatical, se substituie cu cuvintele „Inspectoratul General al Poliției de Frontieră”, la cazul gramatical corespunzătoare, conform Hot.Guv. nr.1145 din 21.11.2018, în vigoare 14.01.2019

Notă: Pe tot parcursul textului, cuvintele “Sistemul informațional integrat al Serviciului Grăniceri”, la orice formă gramaticală, se substituie prin cuvintele “Sistemul informațional integrat al Poliției de Frontieră”, la forma gramaticală corespunzătoare, iar abrevierea “SIISG” se substituie prin abrevierea “SIIPF”, conform [Hot.Guv. nr.925 din 12.12.2012](#), în vigoare 25.12.2012

Pentru realizarea art.10 al [Legii nr.162-XVI din 13 iulie 2007](#) cu privire la Serviciul Grăniceri (Monitorul Oficial al Republicii Moldova, 2007, nr.157-160, art.612), Guvernul

HOTĂRĂȘTE:

1. Se aprobă:

- 1) Conceptul tehnic al Sistemului informațional integrat al Poliției de Frontieră, conform anexei nr.1;
- 2) Regulamentul privind modul de ținere a Registrului care formează Sistemul informațional integrat al Poliției de Frontieră, conform anexei nr.2.

[Pct.1 în redacția [Hot.Guv. nr.1064 din 12.12.2017](#), în vigoare 15.12.2017]

[Pct.1 modificat prin [Hot.Guv. nr.925 din 12.12.2012](#), în vigoare 25.12.2012]

2. Se desemnează Inspectoratul General al Poliției de Frontieră în calitate de deținător al Sistemului informațional integrat al Poliției de Frontieră.

[Pct.2 modificat prin [Hot.Guv. nr.925 din 12.12.2012](#), în vigoare 25.12.2012]

3. Inspectoratul General al Poliției de Frontieră va asigura elaborarea și implementarea, în termen de trei luni, a produselor de program necesare pentru accesul organelor centrale de specialitate ale administrației publice la Sistemului informațional integrat al Poliției de Frontieră.

[Pct.3 modificat prin [Hot.Guv. nr.925 din 12.12.2012](#), în vigoare 25.12.2012]

4. Organizarea și funcționarea Sistemului informațional integrat al Poliției de Frontieră se efectuează din contul și în limitele mijloacelor aprobate în bugetul de stat și din alte surse prevăzute de legislația în vigoare.

[Pct.4 introdus prin [Hot.Guv. nr.1064 din 12.12.2017](#), în vigoare 15.12.2017]

PRIM-MINISTRU

Zinaida GRECEANÎ

Contrasemnează:

Ministrul dezvoltării informaționale

Pavel Buceațchi

Chișinău, 7 iulie 2008.

Nr.834.

Anexa nr.1
la Hotărârea Guvernului
nr.834 din 7 iulie 2008

[Parafa de aprobare în redacția [Hot.Guv. nr.1064 din 12.12.2017](#), în vigoare 15.12.2017]

CONCEPTUL TEHNIC

al Sistemului informațional integrat al Poliției de Frontieră

[Titlul modificat prin [Hot.Guv. nr.925 din 12.12.2012](#), în vigoare 25.12.2012]

Prezentul Concept transpune parțial Decizia de punere în aplicare (UE) 2017/759 a Comisiei din 28 aprilie 2017 privind protocoalele comune și formatele de date care trebuie să fie utilizate de transportatorii aerieni la transferul datelor PNR către unitățile de informații despre pasageri (CELEX: 32017D0759), publicată în Jurnalul Oficial al Uniunii Europene L 113 din 29 aprilie 2017.

[Clauza de armonizare introdusă prin [Hot.Guv. nr.1067 din 27.12.2023](#), în vigoare 05.02.2024]

INTRODUCERE

În ultimii ani Republica Moldova a întreprins pași concreți în vederea asigurării securității frontierei de stat, inclusiv cu asistența Uniunii Europene, prin lansarea activității Misiunii de asistență la frontiera Republicii Moldova și Ucrainei. Grație implicării experților europeni în dezvoltarea managementului integrat al frontierei de stat a Republicii Moldova, în comun cu organele competente în domeniul frontier, s-a reușit într-o perioadă scurtă optimizarea activității acestor organe. Totodată, se impune dezvoltarea de mai departe a managementului integrat al frontierei prin utilizarea tehnologiilor informaționale moderne.

Crearea Sistemului informațional integrat al Poliției de Frontieră presupune nu numai formarea resurselor informaționale cu referire la evenimentele ce au loc la frontieră, dar și acumularea, stocarea și prezentarea lor conform legislației în vigoare, reieșind din competența funcțională.

[Introducere modificată prin [Hot.Guv. nr.925 din 12.12.2012](#), în vigoare 25.12.2012]

Capitolul I GENERALITĂȚI

1. Definiția sistemului

Sistemul informațional integrat al Poliției de Frontieră (în continuare - SIIPF) reprezintă ansamblul datelor, informațiilor, fluxurilor și circuitelor informaționale, al procedurilor și mijloacelor de acumulare și utilizare a informației menite să contribuie la realizarea obiectivelor instituției. Ca rezultat al funcționării sistemului, se formează resursa informațională unică a Poliției de Frontieră.

SIIPF este parte componentă a Resurselor informaționale de stat ale Republicii Moldova (fig.1).

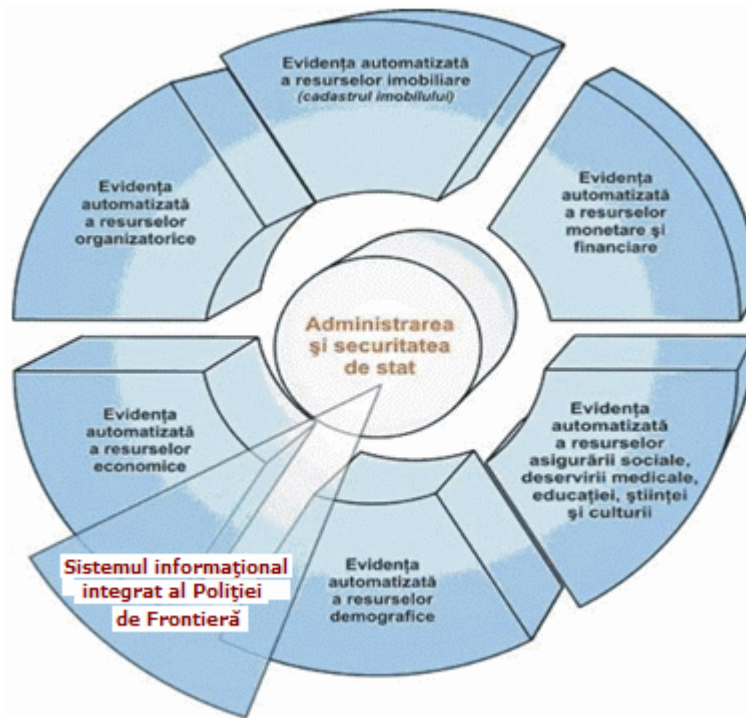


Fig.1. Locul SIIPF în cadrul Resurselor informaționale de stat ale Republicii Moldova

[Pct.1 modificat prin [Hot.Guv. nr.925 din 12.12.2012](#), în vigoare 25.12.2012]

1¹. Noțiuni generale:

identificatori biometrici – datele biometrice conținute de pașapoartele, actele de identitate, documentele de călătorie sau cele colectate nemijlocit la traversarea frontierei de stat;

identificare biometrică – identificarea unei persoane prin compararea datelor biometrice colectate în cadrul controlului la trecerea frontierei cu o serie de modele biometrice stocate și prelucrate în sistemele informaționale de stat (amprenta digitală, imaginea facială, înălțimea, culoarea ochilor, grupa sanguină etc.).

[Pct.1¹ introdus prin [Hot.Guv. nr.1064 din 12.12.2017](#), în vigoare 15.12.2017]

2. Destinația SIIPF

SIIPF este destinat pentru colectarea, prelucrarea, stocarea, actualizarea și analiza inclusiv, în prealabil, a datelor despre persoanele fizice și mijloacele de transport care traversează sau intenționează să traverseze frontiera de stat a Republicii Moldova, despre evenimentele ce au loc pe segmentul verde al frontierei, cu punerea acestor informații la dispoziția autorităților publice competente, altor persoane fizice și juridice, în conformitate cu [Legea nr.283 din 28 decembrie 2011](#) cu privire la Poliția de Frontieră și [Legea nr.215 din 4 noiembrie 2011](#) cu privire la frontiera de stat a Republicii Moldova, precum și cu alte acte legislative și normative în vigoare.

[Pct.2 completat prin [Hot.Guv. nr.1067 din 27.12.2023](#), în vigoare 05.02.2024]

[Pct.2 modificat prin [Hot.Guv. nr.925 din 12.12.2012](#), în vigoare 25.12.2012]

3. Scopul creării SIIPF

Scopul de bază al creării SIIPF constă în realizarea unui management integrat, coerent și eficace al frontierei de stat, pentru asigurarea nivelului adecvat de securitate pe toate sectoarele hotarului Republicii Moldova, aliniat la cerințele comunitare, care să asigure sporirea gradului de securitate a persoanelor, respectând drepturile și libertățile fundamentale ale acestora, fluidizarea traficului legal al persoanelor și mărfurilor la frontieră. Scopul SIIPF poate fi atins prin realizarea următoarelor obiective:

a) asigurarea autorităților administrației publice competente cu informații veridice și operative privind intrarea/ieșirea persoanelor și mijloacelor de transport, necesare pentru luarea deciziilor judicioase la nivel de stat;

b) micșorarea timpului de staționare în punctele de trecere a frontierei de stat a persoanelor și a unităților de transport ce traversează frontiera de stat;

c) sporirea gradului de stabilitate internă a statului, exercitînd un control strict (filtru informațional), prin intermediul înregistrării și verificării persoanelor fizice și a unităților de transport ce traversează frontiera de stat;

d) formarea unei bănci de date privind traversarea frontierei de către persoanele fizice și unitățile de transport;

e) asigurarea interacțiunii efective între ministere și alte autorități ale administrației publice centrale interesate;

f) depistarea persoanelor, mijloacelor de transport, documentelor anunțate în căutare, a cetățenilor străini și apatrizilor cărora intrarea în Republica Moldova le-a fost interzisă;

g) colectarea și stocarea datelor privind starea criminogenă la frontieră, păstrarea acestor date într-un spațiu unic;

h) elaborarea metodologiei și a criteriilor de identificare a riscului, potențialului risc, profilurilor de risc;

i) aprecierea pierderilor posibile în cazurile apariției potențialului risc, precum și pierderile cauzate de riscurile depistate;

j) identificarea măsurilor de prevenire a riscului, minimalizarea lui și stabilirea resurselor necesare pentru aceasta;

k) elaborarea metodologiei de evaluare a eficacității resurselor și de aplicare practică a măsurilor de prevenire și combatere a delictelor frontaliere;

l) controlul practic al măsurilor aplicate pentru contracararea și minimalizarea riscurilor la frontieră;

m) fixarea încălcărilor regimului frontierei de stat;

n) accesul rapid la resursele informaționale ale Poliției de Frontieră;

o) fixarea rezultatelor supravegherii frontierei de stat pe sectorul verde.

[Pct.3 modificat prin [Hot.Guv. nr.925 din 12.12.2012](#), în vigoare 25.12.2012]

4. Principiile de bază ale creării SIIPF

SIIPF este creat în conformitate cu principiile generale de edificare a sistemelor informaționale automatizate, cele de bază fiind:

principiul primei persoane/centrului unic, care semnifică existența unui conducător real de rang superior, cu abilități suficiente pentru luarea deciziilor și coordonarea lucrărilor de creare și exploatare a sistemului;

principiul temeiniciei datelor SIIPF, care presupune introducerea datelor în sistem în baza documentelor autentice;

principiul integrității, plenitudinii și veridicității datelor;

principiul confidențialității informației, care prevede răspunderea personală, în conformitate cu legislația în vigoare, a colaboratorilor responsabili de prelucrarea informației în SIIPF pentru utilizarea și difuzarea neregulamentară a informației confidențiale personificate;

principiul securității informaționale, care presupune asigurarea nivelului dorit al integrității, exclusivității, accesibilității și eficienței protecției datelor împotriva pierderii, denaturării, deteriorării și utilizării neautorizate. Securitatea sistemului presupune rezistența la atacuri și protecția caracterului secret, a integrității și pregătirea pentru lucru atît a sistemului, cît și a datelor lui;

principiul compatibilității sistemului informațional cu sistemele existente autohtone și străine;

principiul scalabilității, care presupune asigurarea unei performanțe constante a soluției informatice la creșterea volumului de date și a solicitării sistemului informațional;

principiul unității spațiului informațional, care se referă la utilizarea unui sistem unic de clasificatoare, formate de date, protocoale de interacțiune informațională, standarde, documente normative și metodice interdependente;

principiul trasabilității, care prevede implementarea procedurilor de înregistrare a tuturor

acțiunilor/evenimentelor asupra obiectelor informaționale ale SIIPF și asigurarea capacității de a identifica prelucrările efectuate cu datele cu caracter personal.

[Pct.4 completat prin Hot.Guv. nr.1067 din 27.12.2023, în vigoare 05.02.2024]

Capitolul II

CADRUL JURIDICO-NORMATIV AL SIIPF

5. Cadrul juridico-normativ al SIIPF se bazează pe legislația națională și tratatele internaționale la care Republica Moldova este parte. Crearea și funcționarea SIIPF sunt reglementate de următoarele acte normative:

- 1) [Legea nr.273/1994](#) privind actele de identitate din sistemul național de pașapoarte;
- 2) [Legea nr.467/2003](#) cu privire la informatizare și la resursele informaționale de stat;
- 3) [Legea nr.71/2007](#) cu privire la registre;
- 4) [Legea nr.245/2008](#) cu privire la secretul de stat;
- 5) [Legea nr.133/2011](#) privind protecția datelor cu caracter personal;
- 6) [Legea nr.215/2011](#) cu privire la frontiera de stat a Republicii Moldova;
- 7) [Legea nr.283/2011](#) cu privire la Poliția de Frontieră;
- 8) [Legea nr.59/2012](#) privind activitatea specială de investigații;
- 9) [Legea nr.142/2018](#) cu privire la schimbul de date și interoperabilitate;
- 10) [Legea nr.124/2022](#) privind identificarea electronică și serviciile de încredere;
- 11) [Legea nr.148/2023](#) privind accesul la informațiile de interes public;
- 11¹) [Codul transporturilor rutiere nr.150/2014](#);
- 12) [Hotărârea Guvernului nr.735/2002](#) cu privire la sistemele speciale de telecomunicații ale Republicii Moldova;
- 13) [Hotărârea Guvernului nr.562/2006](#) cu privire la crearea sistemelor și resurselor informaționale automatizate de stat;
- 14) [Hotărârea Guvernului nr.1090/2013](#) privind serviciul electronic guvernamental de autentificare și control al accesului (MPass);
- 15) [Hotărârea Guvernului nr.128/2014](#) privind platforma tehnologică guvernamentală comună (MCloud);
- 16) [Hotărârea Guvernului nr.405/2014](#) privind serviciul electronic guvernamental integrat de semnătură electronică (MSign);
- 17) [Hotărârea Guvernului nr.708/2014](#) privind serviciul electronic guvernamental de jurnalizare (MLog);
- 18) [Hotărârea Guvernului nr.765/2014](#) cu privire la aprobarea listei documentelor de călătorie acceptate pentru traversarea de către străini a frontierei de stat a Republicii Moldova”;
- 19) [Hotărârea Guvernului nr.297/2017](#) pentru implementarea Legii nr.215 din 4 noiembrie 2011 cu privire la frontiera de stat a Republicii Moldova;
- 20) [Hotărârea Guvernului nr.211/2019](#) privind platforma de interoperabilitate (MConnect);
- 21) [Hotărârea Guvernului nr.376/2020](#) pentru aprobarea Conceptului serviciului guvernamental de notificare electronică (MNotify) și a Regulamentului privind modul de funcționare și utilizare a serviciului guvernamental de notificare electronică (MNotify);
- 22) [Hotărârea Guvernului nr.153/2021](#) pentru aprobarea Conceptului Sistemului informațional „Registrul resurselor și sistemelor informaționale de stat” și a Regulamentului privind modul de ținere a Registrului resurselor și sistemelor informaționale de stat.

[Pct.5 modificat prin Hot.Guv. nr.861 din 18.12.2024, în vigoare 19.01.2025]

[Pct.5 în redacția Hot.Guv. nr.1067 din 27.12.2023, în vigoare 05.02.2024]

[Pct.5 modificat prin Hot.Guv. nr.523 din 22.07.2022, în vigoare 29.07.2022]

[Pct.5 modificat prin [Hot.Guv. nr.925 din 12.12.2012](#), în vigoare 25.12.2012]

[Pct.5 modificat prin [Hot.Guv. nr.709 din 06.08.2010](#), în vigoare 13.08.2010]

Capitolul III

SPAȚIUL FUNCȚIONAL AL SIIPF

6. Funcțiile SIIPF

SIIPF urmează să îndeplinească, pe lângă funcțiile specifice determinate de obiectivele, scopurile și destinația prezentului Concept tehnic, și funcțiile de bază ale sistemului informațional tip, stabilite în concepția sistemului informațional integrat de stat, cele de bază fiind:

a) formarea băncii de date, care include funcțiile de introducere a datelor în evidența inițială, actualizarea și radierea lor din evidență. Aceste funcții se realizează în cadrul colectării datelor despre obiectele de evidență, precum și pe parcursul schimbului de informații cu autoritățile administrației publice centrale și locale. Informațiile privind obiectul de evidență se introduc în banca de date a SIIPF numai pe baza documentelor ce confirmă autenticitatea lor, cu referințe stricte la documentul în baza căruia s-a efectuat actualizarea datelor;

b) organizarea asigurării informaționale din banca de date;

c) asigurarea calității informațiilor din contul creării și menținerii componentelor sistemului de calitate;

d) asigurarea multiaspectuală a funcționării SIIPF;

e) asigurarea protecției informației la toate etapele de colectare, stocare și prezentare;

f) asigurarea cu informație statistică a autorităților publice competente și a publicului;

g) asigurarea integrabilității cu alte sisteme informaționale de stat.

[Pct.6 modificat prin [Hot.Guv. nr.925 din 12.12.2012](#), în vigoare 25.12.2012]

7. Contururile funcționale ale SIIPF

SIIPF include următoarele contururi funcționale:

a) conturul controlului de stat asupra acumulării, păstrării și utilizării resurselor informaționale privind persoanele și mijloacele de transport care trec frontiera de stat (A);

b) conturul evidenței și controlului automatizat al persoanelor care trec frontiera de stat (B);

c) conturul evidenței și controlului automatizat al mijloacelor de transport ce trec frontiera de stat (C);

d) conturul evidenței și controlului automatizat al supravegherii frontierei de stat (D);

e) conturul evidenței și controlului automatizat al cazurilor de încălcare a legislației privind frontiera de stat (E).

Fiecare dintre contururile funcționale exercită mai multe funcții specifice.

A. Conturul controlului de stat asupra acumulării, păstrării și utilizării resurselor informaționale privind persoanele și mijloacele de transport care trec frontiera de stat reprezintă sistemul unic de stat care controlează resursele informaționale privind obiectele evidenței și este inclus în sistemele informaționale automatizate departamentale.

B. Conturul evidenței și controlului automatizat al persoanelor cuprinde datele privind evidența și verificarea automatizată a persoanelor fizice care se deplasează peste frontiera de stat. El are următoarele funcții:

a) înregistrarea și controlul intrării și ieșirii în/din țară a persoanelor fizice;

b) controlul persoanelor fizice cărora le este interzisă intrarea în /ieșirea din Republica Moldova;

c) controlul actelor prezentate de persoanele fizice.

C. Conturul evidenței și controlului automatizat al mijloacelor de transport reflectă evidența automatizată a mijloacelor de transport ce trec frontiera de stat. El are următoarele funcții:

a) evidența mijloacelor de transport și a agregatelor numerotate introduse pentru prima dată în Republica Moldova;

b) evidența mijloacelor de transport scoase definitiv de pe teritoriul Republicii Moldova;

c) evidența mijloacelor de transport ce tranzitează frontiera pe rutele internaționale;

d) controlul mijloacelor de transport cărora le este interzisă intrarea în/ieșirea din teritoriul Republicii Moldova;

e) controlul actelor privind mijloacele de transport:

certificatul de înregistrare al mijlocului de transport;

permisul de conducere.

D. Conturul evidenței și controlului automatizat al supravegherii frontierei de stat reflectă evidența automatizată a supravegherii frontierei de stat. El are următoarele funcții:

- a) colectarea, procesarea și utilizarea datelor de natură generală, precum și a datelor obținute de Poliția de Frontieră pe cazuri individuale;
- b) fixarea și controlul operativ al procesului de supraveghere a frontierei;
- c) evidența colaboratorilor antrenați în supravegherea frontierei de stat;
- d) planificarea serviciului în regim nonstop;
- e) fixarea rezultatelor supravegherii frontierei de stat;
- f) automatizarea proceselor în activitatea subdiviziunilor responsabile de supravegherea frontierei de stat;
- g) evidența și controlul valabilității permiselor de aflare în zona de frontieră (e-permis).

E. Conturul evidenței și controlului automatizat al cazurilor de încălcare a legislației privind frontiera de stat reflectă evidența automatizată a persoanelor și mijloacelor de transport implicate în aceste cazuri, precum și controlul riscurilor. El are următoarele funcții:

- a) evidența și analiza datelor privind starea criminogenă la frontieră (persoanele, mijloacele de transport implicate, bunurile materiale), stocarea și păstrarea acestor date într-un spațiu unic;
- b) elaborarea metodologiei de identificare a riscului, identificarea potențialului risc și fixarea acestuia;
- c) identificarea și evidența cauzelor ce contribuie la încălcarea legislației frontaliere în vigoare;
- d) aprecierea și evidența pierderilor posibile în cazurile apariției potențialului risc, precum și pierderile cauzate de riscurile depistate;
- e) identificarea și evidența măsurilor de prevenire a riscului, minimalizarea lui și resursele necesare pentru aceasta;
- f) controlul practic și evidența măsurilor aplicate în contracararea și minimalizarea riscurilor la frontieră.

F. Conturul evidenței și controlului, inclusiv automatizat, al datelor prelabile despre călători, cu următoarele funcții:

- a) colectarea, de la transportatorii aerieni, în prealabil, a datelor despre călători, prelucrarea și evidența acestora;
- b) crearea criteriilor prestabilite în conformitate cu cadrul normativ;
- c) profilarea călătorilor în baza criteriilor prestabilite în scop de prevenire, depistare, investigare și urmărire penală a infracțiunilor cu caracter terorist, a infracțiunilor transnaționale sau a amenințărilor la adresa securității statului.

[Pct.7 completat prin Hot.Guv. nr.1067 din 27.12.2023, în vigoare 05.02.2024]

[Pct.7 modificat prin Hot.Guv. nr.523 din 22.07.2022, în vigoare 29.07.2022]

[Pct.7 modificat prin [Hot.Guv. nr.925 din 12.12.2012](#), în vigoare 25.12.2012]

Capitolul IV

STRUCTURA ORGANIZAȚIONALĂ A SIIPF

8. Deținătorul SIIPF

Deținătorul sistemului este Inspectoratul General al Poliției de Frontieră. SIIPF se înregistrează, în modul stabilit, în Registrul resurselor și sistemelor informaționale de stat, în conformitate cu prevederile [Hotărârii Guvernului nr.1032 din 6 septembrie 2006](#) "Cu privire la aprobarea Concepției sistemului informațional automatizat "Registrul resurselor și sistemelor informaționale de stat".

[Pct.8 modificat prin [Hot.Guv. nr.925 din 12.12.2012](#), în vigoare 25.12.2012]

9. Registratorii SIIPF

Funcțiile legate de formarea și exploatarea SIIPF revin Inspectoratului General al Poliției de Frontieră. Registratorii ai sistemului sînt inspectorii calificați numiți în funcție, cu drept de acces în sistem.

[Pct.9 modificat prin [Hot.Guv. nr.925 din 12.12.2012](#), în vigoare 25.12.2012]

10. Utilizatorii informației SIIPF

Există două categorii de utilizatori ai sistemului:

- a) interni, care vor fi desemnați prin ordinul șefului Inspectoratului General al Poliției de Frontieră;
- b) externi - entitățile publice competente și structurile internaționale de profil, care pot accesa informația din sistem numai în baza acordurilor interinstituționale încheiate cu Inspectoratul General al Poliției de Frontieră.

[Pct.10 modificat prin Hot.Guv. nr.1067 din 27.12.2023, în vigoare 05.02.2024]

[Pct.10 modificat prin [Hot.Guv. nr.925 din 12.12.2012](#), în vigoare 25.12.2012]

Capitolul V DOCUMENTELE SIIPF

11. Documentele sistemului

Documentele sistemului se divizează în următoarele categorii:

- a) documentele de identificare a persoanei (A);
- b) documentele conducătorului de autovehicul (B);
- c) documentele mijlocului de transport (C);
- d) documentele tehnologice (D);
- e) documentele despre zbor (E).

A. Documentele de identificare a persoanei

Din categoria documentelor de identificare a persoanei fac parte următoarele acte:

- a) pașaportul cetățeanului Republicii Moldova;
- b) pașaportul diplomatic;
- c) pașaportul de serviciu;
- d) documentul de călătorie (Convenția privind statutul apatrizilor din 28 septembrie 1954);
- e) documentul de călătorie (Convenția privind statutul refugiaților din 28 iulie 1951);
- f) documentul de călătorie (protecție umanitară);
- g) buletinul de identitate al cetățeanului Republicii Moldova;
- h) buletinul de identitate electronic al cetățeanului Republicii Moldova;
- i) buletinul de identitate provizoriu al cetățeanului Republicii Moldova;
- j) buletinul de identitate pentru refugiați;
- k) buletinul de identitate pentru apatrizi;
- l) buletinul de identitate pentru beneficiarii de protecție umanitară;
- m) permisul de ședere permanentă;
- n) permisul de ședere provizorie pentru cetățenii străini;
- o) permisul de ședere provizorie pentru apatrizi;
- p) pașaportul marinarului;
- q) pașaportul cetățeanului străin sau documentul de călătorie valabil, emis de statul unde persoana își are stabilit domiciliul;
- r) actul de identitate de uz intern al cetățeanului străin, eliberat de autoritățile străine;
- s) certificatul eliberat de ambasada statului străin în Republica Moldova în schimbul documentului pierdut;
- t) titlul de călătorie;
- u) alte documente ce identifică persoana, în conformitate cu tratatele internaționale la care Republica Moldova este parte.

B. Documentele conducătorului de autovehicul

La trecerea frontierei de stat conducătorul mijlocului de transport este obligat să prezinte permisul de conducere.

C. Documentele mijlocului de transport

În cazul trecerii frontierei de stat cu un mijloc de transport, pentru acesta se prezintă următoarele documente:

- a) pașaportul tehnic al unității de transport;
- b) mandatul, în caz de necesitate;
- c) certificatul de înmatriculare a vehiculului, eliberat pe numele conducătorului.

D. Documentele tehnologice

- a) certificate;
- b) rapoarte analitice și statistice;
- c) procura pentru dreptul de însoțire a persoanei fizice;
- d) permisul de aflare în zona de frontieră.

E. Documentele despre zbor

- a) biletul de zbor;
- b) cardul bancar.

[Pct.11 completat prin Hot.Guv. nr.1067 din 27.12.2023, în vigoare 05.02.2024]

[Pct.11 completat prin Hot.Guv. nr.523 din 22.07.2022, în vigoare 29.07.2022]

[Pct.11 modificat prin [Hot.Guv. nr.1064 din 12.12.2017](#), în vigoare 15.12.2017]

Capitolul VI

SPAȚIUL INFORMAȚIONAL AL SIIPF

12. Obiectele informaționale

SIIPF este format dintr-un nucleu constituit din ansamblul indivizibil al obiectelor supuse evidenței și controlului în cadrul sistemului și din scenariile după care acestea interacționează. Cîmpurile de date se formează prin manifestarea atributelor obiectelor ca urmare a interacțiunii lor conform scenariilor ordinare, care au un caracter ciclic.

Obiectele de evidență și control ale SIIPF sînt:

a) traversarea frontierei de stat:

- polițistul de frontieră care a autorizat traversarea;
- persoana fizică care traversează frontiera de stat;
- mijlocul de transport;
- documentul;

- trecerea frontierei de stat;

b) planificarea activității de serviciu la controlul frontierei:

- rezultatul activității de control;

c) incidentul legat de încălcarea legislației transfrontaliere:

- încălcarea regimului frontierei de stat;
- încălcarea regimului zonei de frontieră;
- încălcarea regimului punctelor de trecere a frontierei de stat etc.;

d) refuzul intrării/ieșirii în/din Republica Moldova:

- polițistul de frontieră care nu a autorizat traversarea;
- persoana fizică;
- mijlocul de transport;
- documentul;

e) consemnul la frontieră:

- actul de dispoziție;
- datele persoanei;
- datele mijlocului de transport;
- documentul.

f) permisul de aflare în zona de frontieră:

- numărul și valabilitatea permisului de aflare în zona de frontieră;
- scopul aflării în zona de frontieră;
- datele persoanei;
- datele mijlocului de transport;
- informațiile privind persoana juridică.

g) rezervarea biletului de zbor spre/dinspre Republica Moldova:

- datele biletului de zbor;
- persoana care a rezervat biletul de zbor;
- datele adiționale privind rezervarea și achiziția biletului de zbor;
- criteriile prestabilite de profilare a călătorilor.

[Pct.12 completat prin Hot.Guv. nr.1067 din 27.12.2023, în vigoare 05.02.2024]

[Pct.12 completat prin Hot.Guv. nr.523 din 22.07.2022, în vigoare 29.07.2022]

[Pct.12 în redacția [Hot.Guv. nr.1064 din 12.12.2017](#), în vigoare 15.12.2017]

13. Identificarea obiectelor informaționale

Obiectele de evidență și control ale SIIPF se identifică prin intermediul următorilor indici de bază:

- a) identificatorul traversării frontierei de stat - după un identificator intern;
- b) numărul de stat de identificare a persoanei fizice (IDNP),
- c) numărul de identificare a mijlocului de transport (codul VIN, conform uzanțelor internaționale, ca abreviere a sintagmei din limba engleză "Vehicle Identification Number");
- d) identificarea documentelor - se efectuează după o cheie combinată ce include următoarele elemente: tipul documentului + seria documentului + numărul documentului;
- e) identificarea contravenției și a infracțiunii - se identifică după un identificator intern;
- f) identificatorul rezervării biletului de zbor spre/dinspre Republica Moldova – codul de rezervare a biletului de zbor.

[Pct.13 completat prin Hot.Guv. nr.1067 din 27.12.2023, în vigoare 05.02.2024]

14. Scenariile de bază

Scenariile reprezintă o listă de evenimente ce se produc cu obiectul informațional prin intermediul cărora se realizează funcțiile SIIPF. Realizarea funcțiilor SIIPF are loc conform următoarelor scenarii:

- a) pentru obiectul informațional „traversarea frontierei de stat”:

Evidența datelor se efectuează după autorizarea traversării frontierei de stat a Republicii Moldova în baza deciziei adoptate referitor la participanții la traversare, ce va conține informațiile privind polițistul de frontieră care a autorizat traversarea (numele, prenumele, gradul special și numărul ștampilei autorizate întărite).

Modificarea datelor are loc în cazul depistării datelor eronate.

Radierea datelor are loc la expirarea termenului de stocare a informației;

- b) pentru obiectul informațional „planificarea activității de serviciu la controlul frontierei”:

Evidența datelor se efectuează după luarea deciziei cu privire la activitățile întreprinse pentru supravegherea frontierei de stat.

Radierea datelor are loc la expirarea termenului de stocare a informațiilor, în conformitate cu instrucțiunile interne ale Inspectoratului General al Poliției de Frontieră;

- c) pentru obiectul informațional „incidentul legat de încălcarea legislației transfrontaliere”:

Evidența datelor se efectuează după depistarea incidentului și întocmirea actelor procesuale.

Radierea datelor are loc la expirarea termenului de stocare a datelor;

- d) pentru obiectul informațional „refuzul intrării/ieșirii în/din Republica Moldova”:

Evidența datelor se efectuează după refuzul intrării/ieșirii în/din Republica Moldova.

Modificarea datelor are loc în cazul depistării datelor eronate.

Radierea datelor are loc la expirarea termenului de stocare a datelor;

- e) pentru obiectul informațional „consemnul la frontieră”:

Evidența datelor se efectuează în baza actelor de procedură prevăzute de legislația în vigoare, care va conține numărul documentului ce întemeiază aplicarea consemnului, emitentul acestuia, temeiul legal, descrierea succintă a dispozitivului, data aplicării consemnului, data expirării interdicției, numele, prenumele și gradul polițistului care a aplicat în SIIPF consemnul la frontieră.

Modificarea datelor are loc:

- în cazul depistării datelor eronate;

- în cazul apariției unor circumstanțe legale în baza actelor prevăzute de legislația în vigoare.

Radierea datelor are loc:

- la expirarea termenului prevăzut în actele în baza cărora au fost introduse datele privind consemnul;

- la revocarea consemnului în baza actelor de procedură prevăzute de legislația în vigoare.

f) pentru obiectul informațional „permisul de aflare în zona de frontieră”:

Evidența datelor se efectuează în baza cererii depuse de persoana fizică/juridică. Datele conțin informațiile privind datele din actul de identitate, existența antecedentelor penale, precum și a încălcărilor anterioare ale regulilor regimului frontierei de stat și ale regimului zonei de frontieră, scopul declarat, numărul și seria permisului de aflare în zona de frontieră, data emiterii, data expirării, numele, prenumele și gradul polițistului de frontieră care a validat emiterea permisului de aflare în zona de frontieră.

Modificarea datelor are loc:

- în cazul depistării datelor eronate;

- în cazul încălcării de către solicitant a regulilor regimului frontierei de stat și ale regimului zonei de frontieră;

- în cazul apariției unor circumstanțe legale, în baza actelor prevăzute de legislație.

Radierea datelor are loc:

- la expirarea termenului de valabilitate al permisului de aflare în zona de frontieră;

- la anularea permisului de aflare în zona de frontieră.

g) pentru obiectul informațional rezervarea biletului de zbor spre/dinspre Republica Moldova:

Evidența datelor se efectuează din momentul furnizării datelor despre călători de la transportatorii aerieni, prin metoda „push”, prin cel puțin unul dintre următoarele formate și protocoale compatibile:

a) formate de date pentru transferul de date PNR:

- EDIFACT PNRGOV, astfel cum este descris în EDIFACT implementation guide (Ghidul de punere în aplicare EDIFACT); PNR data pushed to states or other authorities (date PNR transmise prin metoda „push” către state sau alte autorități); formatul de mesaj PNRGOV (PNRGOV message), versiunea 11.1 sau ulterioară;

- XML PNRGOV, astfel cum este descris în XML implementation guide (ghidul de punere în aplicare XML); PNR data pushed to States or other authorities (date PNR transmise prin metoda „push” către state sau alte autorități); formatul de mesaj PNRGOV (PNRGOV message), versiunea 13.1 sau ulterioară;

b) protocoalele de transmitere:

- IBM MQ;

- IATA Type B;

- profilul AS4 al ebMS 3.0;

- alte protocoale securizate stabilite de comun acord.

În cazul în care transportatorii aerieni transferă date API separat de datele PNR transferate pentru același zbor, aceștia utilizează formatul de date EDIFACT PAXLST.

Modificarea datelor are loc în cazul depistării datelor eronate.

Radierea datelor are loc la expirarea termenului de stocare a datelor.

[Pct. 14 completat prin Hot.Guv. nr.1067 din 27.12.2023, în vigoare 05.02.2024]

[Pct.14 modificat prin Hot.Guv. nr.523 din 22.07.2022, în vigoare 29.07.2022]

[Pct.14 în redacția Hot.Guv. nr.1064 din 12.12.2017, în vigoare 15.12.2017]

[Pct.14 modificat prin Hot.Guv. nr.925 din 12.12.2012, în vigoare 25.12.2012]

15. Datele

Datele stocate în SIIPF sînt:

a) datele despre traversarea frontierei de stat:

- data și ora traversării;

- direcția de deplasare;

- punctul de trecere;

- datele ce vizează polițistul de frontieră care a autorizat traversarea (nume, prenume, grad special, numărul ștampilei autorizate întărite);

- datele despre persoana fizică (nume, prenume, patronimic, sex, data nașterii, IDNP, cetățenie, copia filei documentului de călătorie care conține poza persoanei, amprentele digitale pentru cazurile stabilite, statutul la traversarea frontierei – șofer, pasager, pieton, ciclist);

- datele despre mijlocul de transport (număr de înmatriculare, marcă, model, anul fabricării, culoare, numărul certificatului de înmatriculare, numărul caroseriei/șasiului);

- documentul (seria și numărul documentului, data expirării);

b) datele despre planificarea activității de serviciu la controlul frontierei:

- informațiile despre forțe și mijloace implicate în activitatea de control;

- graficul și orarul turelor;

- informațiile despre tipurile de activitate de control;

- informațiile despre ora și data activității de control;

- informații despre itinerarele de deplasare și locul de desfășurare a activității de control;

- informațiile despre rezultatele activității de control;

c) datele despre incidentul legat de încălcarea legislației transfrontaliere:

- data și ora producerii incidentului;

- locul producerii incidentului;

- tipul incidentului;

- date despre persoana implicată în incident;

- informațiile despre mijlocul de transport implicat în incident;

- informațiile despre bunuri, documente parte a incidentului;

- informații despre măsurile întreprinse în partea ce ține de incident;

d) datele despre refuzul intrării/ieșirii în/din Republica Moldova:

- data și ora refuzului intrării/ieșirii;

- direcția;

- punctul de trecere;

- temeiul refuzului autorizării;

- datele privind polițistul de frontieră care nu a autorizat traversarea (nume, prenume, grad special, numărul ștampilei autorizate întărite);

- datele despre persoană (nume, prenume, prenumele tatălui, sex, data nașterii, IDNP, cetățenie, statutul persoanei la traversarea frontierei – șofer, pasager, pieton, ciclist);

- datele despre mijlocul de transport (număr de înmatriculare, marcă, model, anul fabricării, culoare, numărul certificatului de înmatriculare, numărul caroseriei/șasiului);

- documentul (seria și numărul documentului, data expirării);

e) datele despre consemnul la frontieră:

- actul de dispoziție (temeiul emiterii, data emiterii, măsura aplicată, autoritatea care ține controlul consemnului, termenul încetării consemnului la frontieră);

- datele persoanei (nume, prenume, prenumele tatălui, data nașterii, IDNP);

- datele mijlocului de transport (marcă, model, culoare, număr de înmatriculare, anul fabricării, numărul caroseriei/șasiului);

- documentul (tip, număr, data eliberării, țara emitentă, termen de valabilitate).

f) datele despre rezervarea biletului de zbor spre/dinspre Republica Moldova:

- codul de reper al dosarului pasagerului/codul de rezervare;

- data rezervării/emiterii biletului de călătorie;

- data/datele programată/programate a/ale călătoriei;

- numele, prenumele, inițialele și data nașterii ale pasagerului asociate rezervării, titlul/grad științific, alte informații cu privire la nume;

- adresa și informațiile de contact indicate în rezervare (numărul de telefon, adresă de e-mail);

- toate informațiile privind forma de plată, inclusiv adresa de facturare (numerar, card de credit, numărul și data expirării cardului de credit, notificarea de plată în avans (PTA), valuta, datele despre

persoană/agenție care efectuează plata, codurile reducerilor de serviciu pentru personal);

- itinerarul complet de călătorie (îmbarcare inițială, escală, debarcare finală);
- informațiile din profilul „client fidel” (frequent flyer);
- datele agenției sau agentului de turism (denumirea/numele și prenumele, adresa, datele de contact, codul IATA) prin care a fost făcută rezervarea sau a fost cumpărat biletul;
- statutul călătorului (pasager, membrul echipajului, în tranzit), inclusiv confirmările, situația înregistrării pentru zbor, informații privind neprezentarea pasagerului la îmbarcare sau privind prezentarea acestuia în ultimul moment la îmbarcare, fără rezervare prealabilă;
- informațiile scindate sau divizate din registrul cu numele pasagerilor;
- mențiunile cu caracter general, inclusiv toate informațiile disponibile despre minorii neînsoțiți cu vârsta sub 18 ani, precum numele, prenumele și sexul minorului, vârsta, limba/limbile vorbită/vorbite, numele, prenumele și datele de contact ale persoanei care îl însoțește la plecare și relația sa cu minorul, numele, prenumele și datele de contact ale persoanei care îl așteaptă la sosire și relația sa cu minorul, agentul prezent la plecare și la sosire;
- informațiile despre bilet, inclusiv numărul biletului, data emiterii biletului și biletul dus simplu, câmpurile aferente furnizării automate a prețului unui bilet de călătorie;
- numărul locului și alte informații privind locul (locul solicitat și locul efectiv după închiderea zborului);
- informațiile cu privire la partajarea de coduri;
- toate informațiile cu privire la bagaje, numărul (cantitatea) de bagaje, numărul etichetei de identificare a bagajului, greutatea bagajelor, toată informația cu privire la bagajele combinate, persoana după care este înregistrat bagajul combinat, numărul de locuri pentru bagajul/bagajele combinate, codul transportatorului bagajului, statutul bagajului, punctul de destinație/descărcare a bagajului;
- numărul pasagerilor înregistrați în PNR și alte nume ale acestora;
- compania aeriană, numărul zborului, data plecării și sosirii (data planificată de plecare și sosire a aeronavei în baza timpului local al plecării), aeroportul de plecare, aeroportul de tranzit, aeroportul de sosire, ora plecării și ora sosirii (în baza orelor locale de plecare și sosire);
- un istoric al tuturor modificărilor datelor PNR;
- numele și prenumele persoanei care a făcut rezervarea;
- așteptarea locului (standby);
- toate informațiile despre înregistrarea pasagerului la ghișeu (check-in) – numărul de control la check-in, numele de identificare al agentului de check-in, timpul check-inului, statutul check-inului, statutul de confirmare, numărul de îmbarcare, indicatorul de îmbarcare, ordinea check-inului;
- numărul total de persoane transportate în aeronavă.

g) datele despre autorizație:

- tipul autorizației (autorizație de transport rutier de persoane prin servicii regulate, autorizație de tip pendular, autorizație de transport rutier de persoane prin servicii ocazionale, Carnet INTERBUS);
- seria și/sau numărul autorizației/lipsa acesteia;
- denumirea operatorului de transport;
- numărul de înmatriculare al autocarului;
- regimul de utilizare a autorizației (bilateral, tranzit, țară terță).

[Pct.15 completat prin Hot.Guv. nr.861 din 18.12.2024, în vigoare 19.01.2025]

[Pct.15 modificat prin Hot.Guv. nr.1067 din 27.12.2023, în vigoare 05.02.2024]

[Pct.15 în redacția [Hot.Guv. nr.1064 din 12.12.2017](#), în vigoare 15.12.2017]

[Pct.15 modificat prin [Hot.Guv. nr.925 din 12.12.2012](#), în vigoare 25.12.2012]

16. Clasificatoare

Pentru asigurarea veridicității informațiilor și reducerea volumului de date păstrate în SIIPF, se utilizează un sistem de clasificatoare care pot fi grupate în trei categorii:

- a) internaționale;
- b) naționale:

CS – clasificatorul statelor;
CA – clasificatorul modelelor unităților de transport;
CUTAM – clasificatorul unităților administrativ-teritoriale;
c) interne.

Clasificatoarele interne se elaborează și se utilizează în cadrul SIIPF numai în lipsa clasificatoarelor internaționale și naționale aprobate.

17. Sursele de informații ale SIIPF

Principala sursă de informații este Poliția de Frontieră, care oferă date despre trecerea frontierei de stat de către persoane fizice și mijloace de transport; date generale cu privire la supravegherea frontierei de stat; date statistice, informații individuale, factori de presiune, informații despre infracționalitate și informații referitoare la pericole.

Surse suplimentare de informații sînt:

a) Instituția publică „Agenția Servicii Publice”, care oferă date privind persoanele fizice și actele eliberate acestora, date privind mijloacele de transport;

b) Ministerul Afacerilor Externe și Integrării Europene, care oferă date privind acordarea vizelor de intrare cetățenilor străini și apatrizilor de către consulatele de peste hotare;

c) organele de drept, care oferă date privind persoanele fizice și mijloacele de transport date în urmărire;

d) Ministerul Justiției, care furnizează date privind deciziile instanțelor judecătorești prin care se interzice anumitor persoane fizice trecerea frontierei Republicii Moldova;

e) autoritățile statelor vecine competente în managementul frontierei de stat, care oferă date despre traversarea frontierei de stat de către persoane fizice și mijloace de transport;

f) transportatorii aerieni, care oferă date prealabile despre zbor și călători.

SIIPF este unica sursă de informații privind trecerea frontierei de stat de către persoane fizice și mijloace de transport pentru sistemele informaționale automatizate de stat.

[Pct.17 completat prin Hot.Guv. nr.1067 din 27.12.2023, în vigoare 05.02.2024]

[Pct.17 modificat prin [Hot.Guv. nr.1064 din 12.12.2017](#), în vigoare 15.12.2017]

[Pct.17 modificat prin [Hot.Guv. nr.925 din 12.12.2012](#), în vigoare 25.12.2012]

18. Interacțiunea cu alte sisteme informaționale

În scopul formării corecte a resursei informaționale a SIIPF și al asigurării furnizării datelor din această resursă autorităților/instituțiilor publice, în limitele competențelor stabilite de actele normative, SIIPF va interacționa, prin intermediul platformei de interoperabilitate (MConnect), cu următoarele sisteme informaționale de stat:

a) Registrul de stat al populației, care conține date privind persoanele fizice și actele eliberate acestora;

b) Registrul de stat al transporturilor, ce cuprinde date privind mijloacele de transport (inclusiv agregatele numerotate) și documentele de înmatriculare;

c) Registrul de stat al conducătorilor de vehicule, ce conține date privind dreptul persoanei fizice de conducere a mijlocului respectiv de transport;

d) Sistemul informațional integrat al organelor de drept;

e) Sistemul informațional integrat automatizat de evidență a infracțiunilor, a cauzelor penale și a persoanelor care au săvîrșit infracțiuni;

f) Sistemul informațional automatizat “Registrul informației criminalistice și criminologice”;

g) Sistemul informațional automatizat “Registrul armelor”;

h) Sistemul informațional integrat vamal;

i) Sistemul informațional automatizat de stat în domeniul asigurărilor obligatorii de răspundere civilă pentru pagube produse de autovehicule;

j) subsistemul „Viza” din cadrul conturului automatizat „Consul” al Sistemului informațional automatizat „Registrul de stat al populației”, ce conține date privind vizele valabile pentru Republica Moldova;

k) subsistemul „Titlu de călătorie” din cadrul Sistemului informațional „Consul”, ce conține date privind titlurile de călătorie eliberate;

l) Sistemul informațional automatizat „Registru dactiloscopic”;

m) sistemele informaționale ale transportatorilor aerieni care desfășoară activitățile pe teritoriul Republicii Moldova, în măsura în care acestea permit schimbul de date cu PNR prin intermediul platformei de interoperabilitate (MConnect);

n) Sistemul informațional „e-Autorizație transport”.

Interacțiunea cu registrele informaționale ale altor state sau ale organizațiilor internaționale se va organiza în conformitate cu tratatele internaționale la care Republica Moldova este parte.

[Pct.18 completat prin Hot.Guv. nr.861 din 18.12.2024, în vigoare 19.01.2025]

[Pct.18 completat prin Hot.Guv. nr.1067 din 27.12.2023, în vigoare 05.02.2024]

[Pct.18 modificat prin Hot.Guv. nr.523 din 22.07.2022, în vigoare 29.07.2022]

[Pct.18 modificat prin [Hot.Guv. nr.1064 din 12.12.2017](#), în vigoare 15.12.2017]

Capitolul VII

SPAȚIUL TEHNOLOGIC AL SIIPF

19. Nivelurile infrastructurii informaționale

SIIPF este proiectat ca sistem modular, care asigură posibilitatea dezvoltării sale fără a afecta continuitatea funcționării.

Arhitectura SIIPF este concepută după schema-tip a infrastructurii informaționale a sistemului informațional automatizat, în conformitate cu cerințele expuse în Concepția creării infrastructurii informaționale de stat.

Infrastructura informațională a SIIPF este amplasată în două niveluri:

a) central (A);

b) local (B).

A. Nivelul central este amplasat în municipiul Chișinău. Funcția de bază a nivelului central al infrastructurii informaționale de telecomunicații este asigurarea păstrării informației și acordarea ei utilizatorilor prin portalul informațional de stat. La nivelul central se află banca centrală de date a sistemului.

B. Nivelul local este amplasat în unitățile teritoriale ale Poliției de Frontieră. În fiecare dintre unitățile teritoriale ale Poliției de Frontieră de toate nivelurile sistemului se instalează module-tip. Accesul la informație pentru utilizatorii autorizați se efectuează prin portalul informațional.

[Pct.19 modificat prin [Hot.Guv. nr.925 din 12.12.2012](#), în vigoare 25.12.2012]

20. Complexul software-hardware

Arhitectura complexului software-hardware, lista produselor software și a mijloacelor tehnice utilizate la crearea infrastructurii informaționale se determină de către elaboratorul sistemului în comun cu deținătorul la etapele ulterioare de elaborare a sistemului.

Pentru comunicarea între nivelurile sistemului se utilizează sistemul de telecomunicații al autorităților administrației publice.

20¹. Integrarea cu sisteme informaționale partajate

Pentru asigurarea funcționării și dezvoltării, SIIPF este integrat cu și reutilizează funcționalitățile generice ale sistemelor informaționale partajate, în special, dar nu exclusiv:

1) serviciul electronic guvernamental de autentificare și control al accesului (MPass) – pentru autentificarea și controlul accesului în cadrul sistemului, utilizând mecanismul de autentificare prin semnătură electronică;

2) serviciul electronic guvernamental integrat de semnătură electronică (MSign) – pentru semnarea documentelor electronice;

3) platforma de interoperabilitate (MConnect) – pentru organizarea schimbului de date și a interoperabilității cu alte sisteme informaționale de stat;

4) serviciul electronic guvernamental de jurnalizare (MLog) – pentru asigurarea evidenței

operațiunilor (evenimentelor) produse în cadrul sistemului;

5) serviciul electronic guvernamental de notificare (MNotify) – pentru notificarea registratorilor și utilizatorilor.

[Pct.20¹ introdus prin Hot.Guv. nr.523 din 22.07.2022, în vigoare 29.07.2022]

Capitolul VIII

ASIGURAREA SECURITĂȚII INFORMAȚIONALE A SIIPF

21. Securitatea informațională

Securitatea informațională trebuie să fie asigurată printr-un sistem complex de măsuri juridice, tehnico-organizatorice și economice, cu utilizarea mijloacelor tehnologice, dispozitivelor software/hardware și a mecanismelor criptografice de protecție a informației, orientate spre asigurarea nivelului necesar de integritate, confidențialitate și accesibilitate al resurselor informaționale.

La elaborarea, susținerea funcționării și administrarea SIIPF, Inspectoratul General al Poliției de Frontieră se va conduce de legislația în vigoare și standardele naționale în domeniul asigurării securității informaționale și protecției informației.

Metodele de asigurare a securității informaționale trebuie reexamineate și ajustate periodic sub aspect juridic, tehnico-organizatoric și economic.

[Pct.21 modificat prin Hot.Guv. nr.925 din 12.12.2012, în vigoare 25.12.2012]

21¹. Termenul de stocare a informației

Datele cu caracter personal prelucrate în cadrul SIIPF sunt stocate pentru o perioadă de 5 ani, ulterior se distrug în mod automatizat, în ordinea în care au fost înregistrate.

La expirarea termenului de 6 luni de la data furnizării, datele indicate la pct.15 lit.f) sunt depersonalizate în conformitate cu prevederile [Legii nr.379/2023](#) privind utilizarea datelor din registrul cu numele pasagerilor.

[Pct.21¹ completat prin Hot.Guv. nr.1067 din 27.12.2023, în vigoare 05.02.2024]

[Pct.21¹ în redacția Hot.Guv. nr.523 din 22.07.2022, în vigoare 29.07.2022]

[Pct.21¹ introdus prin Hot.Guv. nr.249 din 03.04.2014, în vigoare 05.04.2014]

22. Sarcinile securității informaționale

a) Crearea sistemului complex al securității informaționale include o serie de etape consecutive: determinarea profilurilor protecției; clasificarea resurselor protejate; analiza riscurilor; elaborarea politicii securității; elaborarea arhitecturii securității; crearea și implementarea sistemului securității informaționale; certificarea sistemului.

b) Componentele de bază ale sistemului securității informaționale sînt: protecția informației și infrastructurii de suport la conectarea la rețelele externe; protecția informației în procesul interacțiunii între rețele; protecția fluxurilor de date; protecția serviciilor sistemului; protecția antivirus; asigurarea securității mediului software; autentificarea; protocolare și audit.

c) Mecanismele tehnologice de bază de asigurare a protecției securității informației sînt: autentificarea și autorizarea; dirijarea accesului; înregistrarea acțiunilor și auditul;

criptarea informației;
delimitarea accesului utilizatorilor la date, în conformitate cu rolurile acestora în SIIPF;
aplicarea mijloacelor bioidentificării utilizatorilor;
aplicarea semnăturii digitale;
accesul la date doar prin interfața unică de obiect;
dirijarea centralizată și controlul accesului la date.

d) Sistemul complex al securității informaționale asigură:

confidențialitatea informației;
integritatea logică a informației;
integritatea fizică a informației;

protecția infrastructurii informaționale în cazul tentativelor de deteriorare sau de modificare a funcționării SIIPF.

Una dintre cele mai vulnerabile verigi în sistemul securității informaționale este factorul uman. În legătură cu aceasta, un element important al securității informaționale este instruirea personalului, familiarizându-l cu metodele și procedeele de contracarare a pericolelor.

23. Pericolele securității informaționale

Prin pericol se subînțelege un eveniment sau o acțiune potențială, orientată spre cauzarea de prejudicii resurselor informaționale sau infrastructurii informaționale.

a) Pericolele de bază ale securității informaționale sînt:

colectarea și utilizarea ilegală a informației;

nimicirea, deteriorarea, suprimarea radioelectronică sau distrugerea mijloacelor și sistemelor de prelucrare a informației, de telecomunicații și comunicații;

compromiterea cheilor și mijloacelor de protecție criptografică a informației.

b) Obiecte ale pericolelor sînt resursele informaționale sau infrastructura informațională de telecomunicații.

c) Surse ale pericolelor sînt infractorii, funcționarii publici corupți, precum și utilizatorii de rea-credință.

24. Protecția informațiilor împotriva accesului neautorizat

a) Sistemul de protecție a informațiilor împotriva accesului neautorizat include măsuri organizaționale, echipamente și produse de program care asigură blocarea:

scurgerii informațiilor prin canalele tehnice;

accesului neautorizat la resursele rețelei.

Măsurile organizatorice de protecție sînt asigurate de către serviciile respective ale participanților la sistem și exclud accesul necontrolat al persoanelor străine la mijloacele tehnice ale sistemului informațional de telecomunicații, la purtătorii magnetici, mijloacele de eliberare a copiilor pe suport material și la sistemele de cablu.

b) Echipamentele și produsele de program de protecție contra accesului neautorizat asigură:

identificarea resurselor aflate sub protecție;

autentificarea resurselor și utilizatorilor aflați sub protecție;

confidențialitatea informației care circulă în sistem;

schimbul de date autentificat;

integritatea datelor la apariția, transmiterea, utilizarea și păstrarea informației;

accesul autorizat al tuturor resurselor sistemului în condiții de exploatare normală;

delimitarea accesului utilizatorilor la sistem;

delimitarea accesului utilizatorilor la resursele aflate sub protecție;

administrarea (indicarea dreptului de acces la resursele aflate sub protecție, prelucrarea informației din registre, instalarea și deinstalarea sistemului de protecție);

înregistrarea acțiunilor de intrare a utilizatorilor în sistem, ieșire din sistem, încălcare a dreptului de acces la resursele aflate sub protecție; controlul integrității și capacității de funcționare a sistemului de protecție;

securitatea în situații de forță majoră.

Capitolul IX

DISPOZIȚII FINALE ȘI TRANZITORII

25. Implementarea efectivă a SIIPF revine Inspectoratului General al Poliției de Frontieră, în comun cu alte organe competente.

[Pct.25 modificat prin [Hot.Guv. nr.925 din 12.12.2012](#), în vigoare 25.12.2012]

26. La îndeplinirea obiectivelor SIIPF pot participa și alte instituții ale statului, precum și organizații neguvernamentale, care cooperează potrivit competențelor și în condițiile legii.

[Pct.26 modificat prin [Hot.Guv. nr.925 din 12.12.2012](#), în vigoare 25.12.2012]

Anexa nr.2
la Hotărârea Guvernului
nr.834 din 7 iulie 2008

[Anexa nr.2 introdusă prin [Hot.Guv. nr.1064 din 12.12.2017](#), în vigoare 15.12.2017]

REGULAMENT

privind modul de ținere a Registrului care formează Sistemul informațional integrat al Poliției de Frontieră

I. DISPOZIȚII GENERALE

1. Regulamentul privind modul de ținere a Registrului care formează Sistemul informațional integrat al Poliției de Frontieră (în continuare – *Regulament*) stabilește modul de organizare și funcționare a Sistemului informațional integrat al Poliției de Frontieră (în continuare – *SIIPF*), ce reprezintă ansamblul datelor, informațiilor, fluxurilor și circuitelor informaționale, al procedurilor și mijloacelor de acumulare și utilizare a informației necesare pentru realizarea obiectivelor Poliției de Frontieră.

2. Noțiunile utilizate în prezentul Regulament au semnificația prevăzută în [Legea nr.467-XV din 21 noiembrie 2003](#) cu privire la informatizare și la resursele informaționale de stat, [Legea nr.71-XVI din 22 martie 2007](#) cu privire la registre, [Legea nr.215 din 4 noiembrie 2011](#) cu privire la frontiera de stat a Republicii Moldova, Conceptul tehnic al Sistemului informațional integrat al Poliției de Frontieră din anexa nr.1.

În sensul prezentului Regulament se definesc următoarele noțiuni:

integritate – certitudinea, necontradictorialitatea și actualitatea informației, protecția ei împotriva distrugerii și modificării neautorizate;

recunoaștere facială – prelucrarea automatizată a imaginilor, care constă în identificarea unor caracteristici faciale specifice persoanei fizice, precum ochii, nasul și gura, extragerea unor caracteristici esențiale din datele biometrice, cum ar fi măsurările faciale pornind de la o imagine captată, inclusiv prin reprezentarea matematică a întregii imagini care rezultă din analiza componentelor principale ale acesteia și duce la identificarea persoanei;

utilizator – persoana cu drept de acces la SIIPF. Există două categorii de utilizatori ai SIIPF – interni, care sînt desemnați prin ordinul șefului Inspectoratului General al Poliției de Frontieră, și externi – autoritățile administrației publice centrale competente și structurile internaționale de profil, care pot accesa informația din SIIPF numai în baza acordurilor interinstituționale încheiate cu Inspectoratul General al Poliției de Frontieră.

3. SIIPF este o parte componentă a resurselor informaționale de stat ale Republicii Moldova.

4. Scopul SIIPF constă în realizarea unui management integrat, coerent și eficace al frontierei de stat, racordat la cerințele comunitare, pentru asigurarea, pe toate sectoarele frontierei de stat, a securității Republicii Moldova și pentru sporirea gradului de securitate a persoanelor, respectînd drepturile și libertățile fundamentale ale acestora și fluidizarea traficului legal al persoanelor la frontieră.

5. SIIPF creează spațiul informațional unic în care se stochează și se prelucrează informații privind

traversarea frontierei de stat de către persoane fizice și mijloace de transport, informații cu privire la supravegherea frontierei de stat, datele PNR date statistice, precum și informații despre infracționalitate și pericole.

[Pct.5 completat prin Hot.Guv. nr.1067 din 27.12.2023, în vigoare 05.02.2024]

II. SUBIECȚII RAPORTURILOR JURIDICE ÎN DOMENIUL CREĂRII ȘI FUNCȚIONĂRII SIIPF

6. SIIPF este o resursă informațională departamentală și face parte din registrele de stat.

7. Subiecți ai raporturilor juridice apărute ca rezultat al creării și funcționării SIIPF sînt:

- 1) statul, în calitate de proprietar;
- 2) Inspectoratul General al Poliției de Frontieră, în calitate de posesor, deținător, administrator tehnic și registrator al SIIPF;
- 3) persoana fizică care traversează frontiera de stat, în calitate de furnizor de date ale SIIPF;
- 3¹) transportatorii aerieni, în calitate de furnizor de date ale SIIPF;
- 4) persoana fizică sau juridică mandată cu dreptul de a primi informații ce o vizează din SIIPF, conform legislației, acordurilor internaționale la care Republica Moldova este parte, precum și acordurilor interinstituționale încheiate cu Inspectoratul General al Poliției de Frontieră, în calitate de destinatar.

[Pct.7 completat prin Hot.Guv. nr.1067 din 27.12.2023, în vigoare 05.02.2024]

8. Inspectoratul General al Poliției de Frontieră realizează atribuțiile privind asigurarea funcționării SIIPF prin crearea, implementarea, dezvoltarea și ținerea acestuia.

9. Posesorul, deținătorul și registratorul SIIPF sînt obligați:

- 1) să asigure funcționarea SIIPF în conformitate cu actele normative în vigoare;
- 2) să asigure înregistrarea, colectarea, acumularea, prelucrarea și stocarea informațiilor în SIIPF în baza documentelor prezentate de către persoana fizică care traversează frontiera de stat sau în temeiul solicitărilor și actelor legale ale subiecților de drept, în cazurile expres prevăzute de legislație;
- 3) să asigure corectitudinea, autenticitatea și actualitatea datelor introduse în SIIPF;
- 4) să acorde utilizatorilor acces la SIIPF, în conformitate cu legislația în vigoare;
- 5) să asigure implementarea și respectarea Cerințelor 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 din 14 decembrie 2010](#);
- 6) să efectueze monitorizarea și supravegherea prelucrării informației din SIIPF;
- 7) să efectueze auditul securității SIIPF;
- 7¹) să stocheze rezultatele auditului securității SIIPF pentru o perioadă de 3 ani;
- 8) să asigure regimul de securitate și confidențialitate a datelor stocate și prelucrate în SIIPF;
- 9) să asigure integritatea informațiilor stocate și prelucrate în SIIPF.

[Pct.9 completat prin Hot.Guv. nr.523 din 22.07.2022, în vigoare 29.07.2022]

10. Posesorul, deținătorul și registratorul SIIPF au următoarele drepturi:

- 1) să asigure implementarea și respectarea cerințelor de securitate informațională a sistemului de către utilizatori, să fixeze și să întreprindă măsuri de prevenire și sancționare a tentativelor de încălcare a regulilor de utilizare, în conformitate cu legislația în vigoare;
- 2) să inițieze procedura de suspendare a drepturilor de acces la datele prelucrate și stocate în SIIPF în cazurile de nerespectare a regulilor, standardelor și normelor general acceptate în domeniul securității informaționale și protecției datelor cu caracter personal, în conformitate cu legislația în vigoare;
- 3) să perfecționeze și să eficientizeze funcționalitatea SIIPF;
- 4) să refuze furnizarea informațiilor din SIIPF în cazurile prevăzute de legislația în vigoare.

11. Utilizatorii SIIPF sînt obligați:

- 1) să utilizeze informația obținută din SIIPF doar în scopurile stabilite de legislație;
- 2) să înștiințeze imediat, prin orice mijloc de comunicare, Inspectoratul General al Poliției de Frontieră despre cazurile de încălcare a securității informaționale a SIIPF;

3) să aducă imediat la cunoștința deținătorului SIIPF orice situație de forță majoră apărută care ar putea influența în mod negativ exercitarea funcțiilor utilizatorului.

12. Utilizatorii SIIPF, în limitele competenței, au următoarele drepturi:

1) să participe la crearea, implementarea și dezvoltarea SIIPF, în conformitate cu legislația națională;

2) să prezinte propuneri cu privire la inițierea modificărilor actelor normative care reglementează funcționarea SIIPF;

3) să prelucreze informația din SIIPF și rapoartele statistice generalizate extrase din sistem exclusiv prin metoda vizualizării, accesării și extragerii;

4) să prezinte propuneri deținătorului SIIPF privind perfecționarea și eficientizarea funcționării acestui sistem informațional.

13. Drepturile și obligațiile destinatarului datelor din SIIPF se stabilesc în legislația privind accesul la informație, protecția datelor cu caracter personal, activitatea specială de investigații, legislația procesual-penală și procesual-civilă, legislația privind secretul de stat și acordurile interinstituționale încheiate cu Inspectoratul General al Poliției de Frontieră.

14. Ținerea SIIPF este supusă controlului intern și extern în conformitate cu prevederile art.31 din [Legea nr.71-XVI din 22 martie 2007](#) cu privire la registre. Controlul intern este efectuat de posesorul SIIPF. Controlul extern asupra respectării cerințelor privind crearea, ținerea, exploatarea și reorganizarea SIIPF este efectuat de organele statale abilitate prin lege.

III. ȚINEREA ȘI ASIGURAREA FUNCȚIONĂRII SIIPF

15. SIIPF se ține în formă electronică, în limba de stat.

16. Ținerea electronică a SIIPF se realizează prin intermediul constituirii resursei informaționale, care reprezintă un ansamblu de obiecte informaționale.

17. Obiectele informaționale de bază ale SIIPF sînt:

1) traversarea frontierei de stat:

a) polițistul de frontieră care a autorizat traversarea;

b) persoana fizică ce traversează frontiera de stat;

c) mijlocul de transport ce traversează frontiera de stat;

d) actul în baza căruia a avut loc autorizarea traversării frontierei de stat;

2) planificarea activității de serviciu la controlul frontierei:

a) rezultatul activității de control;

3) incidentul legat de încălcarea legislației transfrontaliere:

a) încălcarea regimului frontierei de stat;

b) încălcarea regimului zonei de frontieră;

c) încălcarea regimului punctelor de trecere a frontierei de stat etc.;

4) refuzul intrării/ieșirii în/din Republica Moldova:

a) polițistul de frontieră care nu a autorizat traversarea;

b) persoana fizică;

c) mijlocul de transport;

d) documentul;

5) consemnul la frontieră:

a) actul de dispoziție;

b) datele persoanei;

c) datele mijlocului de transport;

d) documentul.

6) permisul de aflare în zona de frontieră:

a) numărul și valabilitatea permisului de aflare în zona de frontieră;

b) scopul aflării în zona de frontieră;

c) datele persoanei;

d) datele mijlocului de transport;

- e) informațiile privind persoana juridică.
- 7) rezervarea biletului de zbor spre/dinspre Republica Moldova:
 - a) datele biletului de zbor;
 - b) persoana care a rezervat biletul de zbor;
 - c) datele adiționale privind rezervarea și achiziția biletului de zbor;
 - d) criteriile prestabilite de profilare a călătorilor.

Evidența obiectelor informaționale se ține conform prezentului Regulament, precum și conform instrucțiunilor aprobate de către posesorul SIIPF.

- 8) autorizația de transport:
 - a) tipul autorizației;
 - b) denumirea operatorului de transport;
 - c) numărul de înmatriculare al autocarului;
 - d) regimul de utilizare a autorizației;
 - e) seria și/sau numărul autorizației/lipsa acesteia

[Pct.17 completat prin Hot.Guv. nr.861 din 18.12.2024, în vigoare 19.01.2025]

[Pct.17 completat prin Hot.Guv. nr.1067 din 27.12.2023, în vigoare 05.02.2024]

[Pct.17 completat prin Hot.Guv. nr.523 din 22.07.2022, în vigoare 29.07.2022]

18. Totalitatea atributelor obiectelor informaționale constituie datele SIIPF. Datele prelucrate prin intermediul SIIPF sînt:

- 1) datele despre traversarea frontierei de stat:
 - a) data și ora traversării;
 - b) direcția de deplasare;
 - c) punctul de trecere;
 - d) datele ce vizează polițistul de frontieră care a autorizat traversarea (nume, prenume, grad special, numărul ștampilei autorizate întărite);
 - e) datele despre persoana fizică (nume, prenume, prenumele tatălui, sex, data nașterii, IDNP, cetățenie, copiile digitale ale paginii de date a documentului de călătorie și amprentelor digitale, statutul la traversarea frontierei – șofer, pasager, pieton, ciclist);
 - f) datele despre mijlocul de transport (număr de înmatriculare, marcă, model, anul fabricării, culoare, numărul certificatului de înmatriculare, numărul caroseriei/șasiului);
 - g) documentul (seria și numărul documentului, data expirării);
- 2) datele despre planificarea activității de serviciu la controlul frontierei:
 - a) informațiile despre forțe și mijloace implicate în activitatea de control;
 - b) graficul și orarul turelor;
 - c) informații despre tipurile de activitate de control;
 - d) datele despre ora și data activității de control;
 - e) informațiile despre itinerarele de deplasare și locul de desfășurare a activității de control;
 - f) informațiile despre rezultatele activității de control;
- 3) datele despre incidentul legat de încălcarea legislației transfrontaliere:
 - a) data și ora producerii incidentului;
 - b) locul producerii incidentului;
 - c) tipul incidentului;
 - d) date despre persoana implicată în incident;
 - e) informațiile despre mijlocul de transport implicat în incident;
 - f) informațiile despre bunuri, documente parte a incidentului;
 - g) informații despre măsurile întreprinse în partea ce ține de incident;
- 4) datele despre refuzul intrării/ieșirii în/din Republica Moldova:
 - a) data și ora refuzului intrării/ieșirii;
 - b) direcția;
 - c) punctul de trecere;

- d) temeiul refuzului autorizării;
 - e) datele privind polițistul de frontieră care nu a autorizat traversarea (nume, prenume, grad special, numărul ștampilei autorizate întărite);
 - f) datele despre persoană (nume, prenume, prenumele tatălui, sex, data nașterii, IDNP, cetățenie, statutul persoanei la traversarea frontierei – șofer, pasager, pieton, ciclist);
 - g) datele despre mijlocul de transport (număr de înmatriculare, marcă, model, anul fabricării, culoare, numărul certificatului de înmatriculare, numărul caroseriei/șasiului);
 - h) documentul (seria și numărul documentului, data expirării);
- 5) datele despre consemnul la frontieră:
- a) actul de dispoziție (temeiul emiterii, data emiterii, măsura aplicată, autoritatea care ține controlul consemnului, termenul încetării consemnului la frontieră);
 - b) datele persoanei (nume, prenume, prenumele tatălui, data nașterii, IDNP);
 - c) datele mijlocului de transport (marcă, model, culoare, număr de înmatriculare, anul fabricării, numărul caroseriei/șasiului);
 - d) documentul (tip, număr, data eliberării, țara emitentă, termen de valabilitate).
- 6) datele despre permisul de aflare în zona de frontieră:
- a) datele despre persoana fizică (nume, prenume, data nașterii, IDNP, cetățenie, fotografie, declarație pe proprie răspundere privind lipsa de antecedente penale și încălcări anterioare ale legislației cu privire la frontiera de stat, precum și privind respectarea legislației în timpul aflării în zona de frontieră, locul, perioada și scopul aflării, numărul permisului, data emiterii permisului, perioada pentru care s-a acordat permisul, informarea în prealabil a subdiviziunii Poliției de Frontieră, observații);
 - b) datele despre mijlocul de transport (număr de înmatriculare, marcă, model, număr al certificatului de înmatriculare, număr al permisului, data emiterii permisului, perioada pentru care s-a acordat permisul, observații);
 - c) datele despre persoana juridică (denumire, număr de identificare de stat (IDNO), adresa juridică, activitatea pentru care este solicitat permisul, actul care permite desfășurarea activității; autorizarea organului vamal privind desfășurarea activității de orice natură în punctul de trecere al frontierei de stat, eliberată în conformitate cu prevederile [Codului vamal al Republicii Moldova nr.1149/2000](#); tabelul nominal cu personalul ce urmează să lucreze în perimetrul punctului de trecere a frontierei de stat; declarația pe proprie răspundere a angajatului agentului economic sau organizației privind lipsa de antecedente penale și încălcări anterioare ale legislației cu privire la frontiera de stat, precum și privind respectarea legislației referitoare la frontiera de stat; numărul permisului, data emiterii permisului, perioada pentru care s-a acordat acesta, informarea în prealabil a subdiviziunii Poliției de Frontieră, observații);
 - d) datele personale ale polițistului de frontieră care a validat emiterea permisului de aflare în zona de frontieră (nume, prenume, grad special, numărul și seria legitimației de serviciu).
- 7) datele despre rezervarea biletului de zbor spre/dinspre Republica Moldova:
- a) codul de reper al dosarului pasagerului/codul de rezervare;
 - b) data rezervării/emiterii biletului de călătorie;
 - c) data/datele programată/programate a/ale călătoriei;
 - d) numele, prenumele, inițialele și data nașterii ale pasagerului asociate rezervării, titlul/grad științific, alte informații cu privire la numele pasagerului;
 - e) adresa și informațiile de contact indicate în rezervare (numărul de telefon, adresă de e-mail);
 - f) toate informațiile privind forma de plată, inclusiv adresa de facturare (numerar, card de credit, numărul și data expirării cardului de credit, notificarea de plată în avans (PTA), valuta, datele despre persoana/agenția care efectuează plata, codurile reducerilor de serviciu pentru personal);
 - g) itinerarul complet de călătorie (îmbarcare inițială, escală, debarcare finală);
 - h) informațiile din profilul „client fidel” (frequent flyer);
 - i) datele agenției sau agentul de turism (denumirea/numele și prenumele, adresa, datele de contact, codul IATA) prin care a fost făcută rezervarea sau a fost cumpărat biletul;
 - j) statutul călătorului (pasager, membrul echipajului, în tranzit), inclusiv confirmările, situația

înregistrării pentru zbor, informații privind neprezentarea pasagerului la îmbarcare sau privind prezentarea acestuia în ultimul moment la îmbarcare, fără rezervare prealabilă;

k) informațiile scindate sau divizate din registrul cu numele pasagerilor;

l) mențiunile cu caracter general, inclusiv toate informațiile disponibile despre minorii neînsoțiți cu vârsta sub 18 ani, precum numele, prenumele și sexul minorului, vârsta, limba/limbile vorbită/vorbite, numele, prenumele și datele de contact ale persoanei care îl însoțește la plecare și relația sa cu minorul, numele, prenumele și datele de contact ale persoanei care îl așteaptă la sosire și relația sa cu minorul, agentul prezent la plecare și la sosire;

m) informațiile despre biletul de călătorie, inclusiv numărul biletului, data emiterii biletului și bilete dus simplu, câmpurile aferente furnizării automate a prețului unui bilet de călătorie;

n) numărul locului și alte informații privind locul (locul solicitat și locul efectiv după închiderea zborului);

o) informațiile cu privire la partajarea de coduri;

p) toate informațiile cu privire la bagaje, numărul (cantitatea) de bagaje, numărul etichetei de identificare a bagajului, greutatea bagajelor, toată informația cu privire la bagajele combinate, persoana după care este înregistrat bagajul combinat, numărul de locuri pentru bagajul(le) combinat(e), codul transportatorului bagajului, statutul bagajului, punctul de destinație/descărcare a bagajului;

q) numărul pasagerilor înregistrați în PNR și alte nume ale acestora;

r) compania aeriană, numărul zborului, data plecării și sosirii (data planificată de plecare și sosire a aeronavei în baza timpului local al plecării), aeroportul de plecare, aeroportul de tranzit, aeroportul de sosire, ora plecării și ora sosirii (în baza orelor locale de plecare și sosire);

s) un istoric al tuturor modificărilor datelor PNR;

t) numele și prenumele persoanei care a făcut rezervarea;

u) așteptarea locului (standby);

v) toate informațiile despre înregistrarea pasagerului la ghișeu (check-in) – numărul de control la check-in, numele de identificare al agentului de check-in, timpul check-inului, statutul check-inului, statutul de confirmare, numărul de îmbarcare, indicatorul de îmbarcare, ordinea check-inului;

w) numărul total de persoane transportate în aeronavă.

8) datele despre autorizație:

a) tipul autorizației (autorizație de transport rutier de persoane prin servicii regulate, autorizație de tip „pendular”, autorizație de transport rutier de persoane prin servicii ocazionale, Carnet INTERBUS);

b) seria și/sau numărul autorizației/lipsa acesteia;

c) denumirea operatorului de transport;

d) numărul de înmatriculare al autocarului;

e) regimul de utilizare a autorizației (bilateral, tranzit, țară terță).

[Pct.18 completat prin Hot.Guv. nr.861 din 18.12.2024, în vigoare 19.01.2025]

[Pct.18 modificat prin Hot.Guv. nr.1067 din 27.12.2023, în vigoare 05.02.2024]

[Pct.18 completat prin Hot.Guv. nr.523 din 22.07.2022, în vigoare 29.07.2022]

19. Datele despre traversarea frontierei de stat sînt introduse în SIIPF de către registrator în momentul efectuării controlului la traversarea frontierei de stat.

20. Datele despre persoana care traversează frontiera de stat și despre actul conform căruia a avut loc traversarea frontierei de stat se introduc în SIIPF de către registrator în baza documentelor prevăzute de actele normative în vigoare, tratatele sau acordurile internaționale la care Republica Moldova este parte.

21. Datele despre unitățile de transport care traversează frontiera de stat se introduc în SIIPF de către registratori în baza documentelor prevăzute în actele normative în vigoare.

22. Enumerarea categoriilor informațiilor ce sînt prelucrate și stocate în SIIPF sînt reglementate în capitolul VI din anexa nr.1.

23. Modalitatea de introducere și folosire a datelor SIIPF prevăzute în pct.18 subpct.2), 4), 5) și 6) din prezentul Regulament se stabilește de către șeful Inspectoratului General al Poliției de Frontieră, în

conformitate cu legislația în vigoare.

[Pct.23 modificat prin Hot.Guv. nr.523 din 22.07.2022, în vigoare 29.07.2022]

24. În SIIPF va fi introdusă și stocată fotografia digitală a feței și amprentele digitale doar ale persoanei supuse verificării prin metoda de recunoaștere facială și sistemul de verificare a amprenteii digitale. Aceste proceduri se aplică:

1) în cazul controlului în linia a doua, în conformitate cu prevederile art.21 din [Legea nr.215 din 4 noiembrie 2011](#) cu privire la frontiera de stat a Republicii Moldova;

2) în cazul existenței consimțământului persoanei de a fi supusă procedurilor de verificare prin metoda recunoașterii faciale și a amprentelor digitale în scopul traversării rapide a frontierei de stat a Republicii Moldova.

25. Datele introduse în SIIPF sunt stocate pentru o perioadă de 5 ani, ulterior acestea se distrug în mod automatizat, în ordinea în care au fost înregistrate. La expirarea termenului de 6 luni de la data furnizării, datele indicate la pct.18 sunt depersonalizate în conformitate cu prevederile [Legii nr.379/2023](#) privind utilizarea datelor din registrul cu numele pasagerilor.

[Pct.25 completat prin Hot.Guv. nr.1067 din 27.12.2023, în vigoare 05.02.2024]

[Pct.25 în redacția Hot.Guv. nr.523 din 22.07.2022, în vigoare 29.07.2022]

26. Termenul de stocare a datelor în SIIPF poate fi prelungit în legătură cu:

- 1) ordonanța organului de urmărire penală;
- 2) încheierea instanței judecătorești referitoare la judecarea cauzei;
- 3) demersul motivat al subiecților care efectuează activitatea specială de investigații, în condițiile legii.

27. Prolungirea termenului de stocare a datelor din SIIPF urmează a fi efectuată cu asigurarea drepturilor și libertăților subiectului datelor cu caracter personal, în baza deciziei motivate emise de o comisie specială, formată din reprezentanții deținătorului SIIPF, care include, în mod obligatoriu, persoana responsabilă de politica de securitate a datelor cu caracter personal din cadrul Inspectoratului General al Poliției de Frontieră. Comisia specială este formată în componență nominală potrivit ordinului șefului Inspectoratului General al Poliției de Frontieră.

28. În cazurile prevăzute la pct.26, subiecții de drept indică, în mod obligatoriu, termenul ce urmează a fi prelungit în vederea asigurării statutului activ al informațiilor prelucrate și stocate în SIIPF, norma legală care întemeiază acest fapt și actul juridic care întemeiază această necesitate, cum ar fi ordonanța, încheierea etc., precum și informează asupra necesității restricționării drepturilor subiecților de date cu caracter personal sau lipsei acestei necesități.

29. Termenul de stocare a datelor în SIIPF nu poate fi prelungit decât pentru perioada necesară atingerii scopului urmărit, cu indicarea în decizia prevăzută la pct.26 a perioadei exacte de timp.

[Pct.29 modificat prin Hot.Guv. nr.523 din 22.07.2022, în vigoare 29.07.2022]

30. Ținerea SIIPF este asigurată pînă la adoptarea deciziei de lichidare a acestuia. În cazul lichidării SIIPF, datele și documentele conținute în acesta se transmit în arhivă, conform legislației.

31. Datele din SIIPF fac parte din categoria informațiilor oficiale cu accesibilitate limitată. Asigurarea securității, confidențialității și integrității datelor prelucrate în cadrul SIIPF se efectuează cu respectarea strictă a Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal.

IV. INTEROPERABILITATEA CU ALTE SISTEME INFORMAȚIONALE

32. Pentru asigurarea formării corecte a resursei informaționale și asigurarea SIIPF cu date veridice, se realizează interacțiunea și sincronizarea cu sistemele informaționale de stat care conțin date despre persoane, documente, mijloace de transport și alte date relevante pentru activitatea Poliției de Frontieră.

33. Actualizarea informației din SIIPF are loc la introducerea datelor de către utilizatorul din cadrul

Inspectoratului General al Poliției de Frontieră, recepționarea informației suplimentare din partea furnizorilor de informații, inclusiv automatizat în cazul schimbării datelor din sistemele informaționale de stat cu care interacționează SIIPF.

34. Datele accesate din registrele de stat nu pot fi modificate prin intermediul SIIPF. Acestea se vor constitui în calitate de sursă primară și veridică a datelor destinate SIIPF.

35. Interoperabilitatea cu alte sisteme se realizează prin intermediul platformei de interoperabilitate (MConnect), în conformitate cu prevederile legislației în vigoare.

36. Interacțiunea cu registrele informaționale internaționale se organizează în conformitate cu tratatele internaționale la care Republica Moldova este parte.

V. REGIMUL JURIDIC DE UTILIZARE A DATELOR DIN SIIPF

37. Punerea la dispoziție a datelor din SIIPF și furnizarea lor de către deținătorul SIIPF autorităților și instituțiilor publice se realizează prin intermediul platformei de interoperabilitate (MConnect) în conformitate cu prevederile cadrului normativ în domeniul schimbului de date și interoperabilității, în condițiile în care acestea invocă un scop și un temei legal pentru prelucrarea setului de date solicitat și respectă cerințele de securitate și confidențialitate ce decurg din regimul juridic al datelor vizate.

[Pct.37 în redacția Hot.Guv. nr.523 din 22.07.2022, în vigoare 29.07.2022]

38. Extrasele din SIIPF, adeverințele și documentele se eliberează de către deținătorul SIIPF sau de către persoana desemnată de acesta și sînt semnate de către conducătorul acestuia. Documentele electronice generate în SIIPF sînt semnate cu semnătura electronică avansată calificată a persoanei împuternicite de către deținătorul SIIPF.

[Pct.38 modificat prin Hot.Guv. nr.861 din 18.12.2024, în vigoare 19.01.2025]

39. Informația generată în SIIPF se marchează, indicîndu-se prescripția pentru prelucrarea ulterioară a acesteia și numărul de identificare unic din Registrul de evidență a operatorilor de date cu caracter personal.

40. Utilizarea datelor din SIIPF în scopuri contrare legii atrage după sine răspunderea disciplinară, civilă, contravențională și penală.

41. Destinatarul datelor din SIIPF nu este în drept să modifice datele obținute din SIIPF, iar la utilizarea acestora este obligat să indice sursa lor.

VI. MODALITATEA DE CONECTARE/DECONECTARE LA/DE LA SIIPF

42. Utilizatorii dispun de dreptul de acces la informația stocată și prelucrată în SIIPF în funcție de rolurile și drepturile atribuite.

43. Utilizatorii vor fi conectați la SIIPF de către deținătorul acestuia doar în baza existenței temeiului legal și a demersului oficial, în care vor fi indicate numărul necesar de locuri automatizate de muncă și datele cu caracter personal ale utilizatorilor SIIPF, primind următoarele credențiale de acces, inclusiv prin serviciul electronic guvernamental de autentificare și control al accesului (MPass):

- 1) numele utilizatorului;
- 2) codul (parola) de acces.

44. Parola de acces este generată în mod manual de către deținătorul SIIPF și este transmisă utilizatorului prin una dintre următoarele modalități:

- 1) personal, contra semnătură;
- 2) prin intermediul poștei recomandate, cu inscripția „personal”.

45. La prima intrare în sistem utilizatorul este obligat să schimbe parola, care conține cel puțin 8 simboluri pe diferite registre de tastatură.

46. La prelucrarea informației din SIIPF, utilizatorii au obligația asigurării protecției datelor cu caracter personal, conform [Legii nr.133 din 8 iulie 2011](#) privind protecția datelor cu caracter personal.

47. Accesul la SIIPF este suspendat de către deținătorul acestuia în următoarele cazuri:

- 1) în timpul efectuării lucrărilor profilactice ale complexului de mijloace software și hardware ale

SIIPF;

2) la apariția circumstanțelor de forță majoră;

3) la încălcarea securității informaționale în cadrul SIIPF, dacă aceasta prezintă pericol pentru funcționarea lui;

4) la încălcarea legislației cu privire la protecția datelor cu caracter personal.

48. Lucrările profilactice în complexul de mijloace software și hardware ale SIIPF se efectuează după notificarea în scris a utilizatorilor cu cel puțin două zile lucrătoare înainte de începerea lucrărilor, cu indicarea termenului de finalizare a acestora.

49. Revocarea dreptului de acces la SIIPF se efectuează în una dintre următoarele situații:

1) în temeiul cererii oficiale de deconectare a utilizatorului, semnată de către conducătorul acestuia;

2) la încetarea raporturilor de muncă/de serviciu ale utilizatorilor SIIPF sau la modificarea acestora în cazul în care noile atribuții nu impun accesul la datele din SIIPF;

3) la constatarea încălcării de către utilizator a securității informaționale a SIIPF și legislației privind protecția datelor cu caracter personal.

VII. ASIGURAREA PROTECȚIEI ȘI SECURITĂȚII INFORMAȚIEI ȘI RESURSELOR INFORMAȚIONALE ALE SIIPF

50. Măsurile de protecție și securitate a informației din SIIPF reprezintă o parte componentă a lucrărilor de creare, dezvoltare și exploatare a SIIPF și se efectuează neîntrerupt de către deținătorul SIIPF.

51. Obiecte ale asigurării protecției și securității informației din SIIPF se consideră:

1) masivele informaționale, indiferent de formele păstrării, bazele de date, suporturile materiale care conțin informații privind date cu caracter personal;

2) sistemele informaționale, sistemele operaționale, sistemele de gestionare a bazelor de date și alte aplicații care asigură activitatea SIIPF;

3) sistemele de telecomunicații, rețelele, inclusiv mijloacele de confecționare și multiplicare a documentelor și alte mijloace tehnice de prelucrare a informației.

52. Protecția informației cu caracter personal din SIIPF se efectuează prin următoarele metode:

1) prevenirea conexiunilor neautorizate la rețelele telecomunicaționale și a interceptării cu ajutorul mijloacelor tehnice a datelor din SIIPF transmise prin aceste rețele, asigurată prin folosirea metodelor de cifrare și criptare a acestei informații, inclusiv cu utilizarea măsurilor organizatorice, tehnice și de regim;

2) excluderea accesului neautorizat la datele din SIIPF, asigurată prin folosirea mijloacelor speciale tehnice și de program, cifrarea acestor informații, inclusiv prin măsurile organizatorice și de regim;

3) prevenirea acțiunilor intenționate și/sau neintenționate ale participanților la SIIPF care pot conduce la distrugerea sau modificarea datelor din SIIPF, prin metoda folosirii mijloacelor de protecție speciale tehnice și de program, inclusiv a programelor licențiate, programelor antivirus, organizarea sistemului de control al securității softului și efectuarea periodică a copiilor de siguranță.

53. Deținătorul SIIPF elaborează, aprobă și organizează implementarea documentului care stabilește politica de securitate informațională pentru asigurarea respectării regulilor, standardelor și normelor general acceptate în domeniul securității informaționale, cu indicarea:

1) identității persoanei responsabile de politica de securitate;

2) principalelor măsuri tehnico-organizatorice necesare de asigurare a funcționării SIIPF;

3) procedurilor interne ce exclud cazurile de modificare neautorizată a mijloacelor software și/sau a informației din SIIPF;

4) nivelului necesar de securitate pentru fiecare categorie de utilizatori ai SIIPF;

5) listei nominale a utilizatorilor autorizați să acceseze datele din SIIPF;

6) responsabilităților utilizatorilor SIIPF privind asigurarea securității informaționale;

7) procedurilor de control intern al utilizatorilor SIIPF privind respectarea condițiilor de securitate informațională.

54. Deținătorul SIIPF desemnează o persoană subordonată nemijlocit conducătorului instituției,

responsabilă de elaborarea, implementarea și monitorizarea respectării prevederilor politicii de securitate informațională.

55. Persoana responsabilă de politica securității informaționale asigură definirea clară a tuturor responsabilităților cu privire la securitatea informației din SIIPF (prevenire, supraveghere, detectare și prelucrare), precum și operarea cu ele.

56. În cazul operării cu informația din SIIPF ce a devenit cunoscută utilizatorului SIIPF în urma activității sale, este asigurat regimul de confidențialitate, care presupune următoarele acțiuni:

- 1) limitarea numărului persoanelor cu drept de acces la datele din SIIPF;
- 2) monitorizarea procedurii de admitere și delimitarea funcțională a responsabilităților persoanelor care au acces la informația din SIIPF;
- 3) identificarea și autentificarea participanților la SIIPF cu folosirea mijloacelor moderne de autentificare;
- 4) executarea măsurilor de protecție a informației în cadrul păstrării, prelucrării și transmiterii acestora prin intermediul canalelor de comunicații.

VIII. PROTECȚIA DATELOR CU CARACTER PERSONAL, CONTROLUL ȘI RESPONSABILITATEA

57. Prelucrarea datelor cu caracter personal se efectuează în conformitate cu prevederile actelor normative în domeniul protecției datelor cu caracter personal.

58. Persoanele împuternicite cu drept de acces la SIIPF sînt obligate de a nu divulga informația cu accesibilitate limitată la care au primit acces în legătură cu exercitarea atribuțiilor funcționale, inclusiv după încetarea activității. Pentru încălcarea clauzei de confidențialitate, persoanele vinovate răspund în conformitate cu legislația în vigoare.

59. Responsabilitatea pentru organizarea și funcționarea SIIPF se atribuie deținătorului, care elaborează tipul și modelul documentelor aferente, instrucțiunile privind modul de completare și alte materiale necesare pentru funcționarea SIIPF.

La prelucrarea datelor cu caracter personal, posesorul asigură măsuri organizatorice și tehnice necesare pentru protecția datelor cu caracter personal împotriva distrugerii, a modificării, a blocării, a copierii, a răspândirii, precum și împotriva altor acțiuni ilicite, măsuri menite să asigure un nivel de securitate adecvat în ceea ce privește riscurile prezentate de prelucrare și caracterul datelor prelucrate.

[Pct.59 completat prin Hot.Guv. nr.1067 din 27.12.2023, în vigoare 05.02.2024]

60. În cazul incidentelor de securitate cibernetică, al incidentelor de securitate a resurselor informaționale de date cu caracter personal, deținătorul întreprinde, de comun acord cu autoritățile competente, conform actelor normative, măsurile necesare pentru depistarea sursei de producere a incidentului, efectuează analiza acestuia și înlătură cauzele incidentului de securitate, cu informarea autorităților competente.

[Pct.60 introdus prin Hot.Guv. nr.1067 din 27.12.2023, în vigoare 05.02.2024]

[Anexa nr.2 introdusă prin [Hot.Guv. nr.1064 din 12.12.2017](#), în vigoare 15.12.2017]