GUVERNUL REPUBLICII MOLDOVA

ПРАВИТЕЛЬСТВО РЕСПУБЛИКИ МОЛДОВА

H O T Ă R Î R E

cu privire la Sistemul informaţional integrat al Poliţiei 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 Poliţiei de Frontieră", la orice caz gramatical, se substituie cu cuvintele „Inspectoratul General al Poliţiei 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 informaţional integrat al Serviciului Grăniceri", la orice formă gramaticală, se substituie prin cuvintele "Sistemul informaţional integrat al Poliţiei 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

HOTĂRĂŞTE:

1. Se aprobă:

1) Conceptul tehnic al Sistemului informaţional integrat al Poliţiei de Frontieră, conform anexei nr.1;

2) Regulamentul privind modul de ţinere a Registrului care formează Sistemul informaţional integrat al Poliţiei de Frontieră, conform anexei nr.2.

[Pct.1 în redacţia 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 Poliţiei de Frontieră în calitate de deţinător al Sistemului informaţional integrat al Poliţiei de Frontieră.

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

3. Inspectoratul General al Poliţiei de Frontieră va asigura elaborarea şi implementarea, în termen de trei luni, a produselor de program necesare pentru accesul organelor centrale de specialitate ale administraţiei publice la Sistemului informaţional integrat al Poliţiei de Frontieră.

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

4. Organizarea şi funcţionarea Sistemului informaţional integrat al Poliţiei de Frontieră se efectuează din contul şi în limitele mijloacelor aprobate în bugetul de stat şi din alte surse prevăzute de legislaţia în vigoare.

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

PRIM-MINISTRU **Zinaida GRECEANÎI**

Contrasemnează:

Ministrul dezvoltării informaţionale **Pavel Buceaţchi**

Chişinău, 7 iulie 2008.

Nr.834.

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

[Parafa de aprobare în redacţia Hot.Guv. nr.1064 din 12.12.2017, în vigoare 15.12.2017]

CONCEPTUL TEHNIC
al Sistemului informaţional integrat al Poliţiei de Frontieră

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

Prezentul Concept transpune parţial Decizia de punere în aplicare (UE) 2017/759 a Comisiei din 28 aprilie 2017 privind protocoalele comune şi formatele de date care trebuie să fie utilizate de transportatorii aerieni la transferul datelor PNR către unităţile de informaţii 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 paşi concreţi în vederea asigurării securităţii frontierei de stat, inclusiv cu asistenţa Uniunii Europene, prin lansarea activităţii Misiunii de asistenţă la frontiera Republicii Moldova şi Ucrainei. Graţie implicării experţilor europeni în dezvoltarea managementului integrat al frontierei de stat a Republicii Moldova, în comun cu organele competente în domeniul frontalier, s-a reuşit într-o perioadă scurtă optimizarea activităţii acestor organe. Totodată, se impune dezvoltarea de mai departe a managementului integrat al frontierei prin utilizarea tehnologiilor informaţionale moderne.

Crearea Sistemului informaţional integrat al Poliţiei de Frontieră presupune nu numai formarea resurselor informaţionale cu referire la evenimentele ce au loc la frontieră, dar şi acumularea, stocarea şi prezentarea lor conform legislaţiei în vigoare, reieşind din competenţa funcţională.

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

Capitolul I
GENERALITĂŢI

1. Definiţia sistemului

Sistemul informaţional integrat al Poliţiei de Frontieră (în continuare - SIIPF) reprezintă ansamblul datelor, informaţiilor, fluxurilor şi circuitelor informaţionale, al procedurilor şi mijloacelor de acumulare şi utilizare a informaţiei menite să contribuie la realizarea obiectivelor instituţiei. Ca rezultat al funcţionării sistemului, se formează resursa informaţională unică a Poliţiei de Frontieră.

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

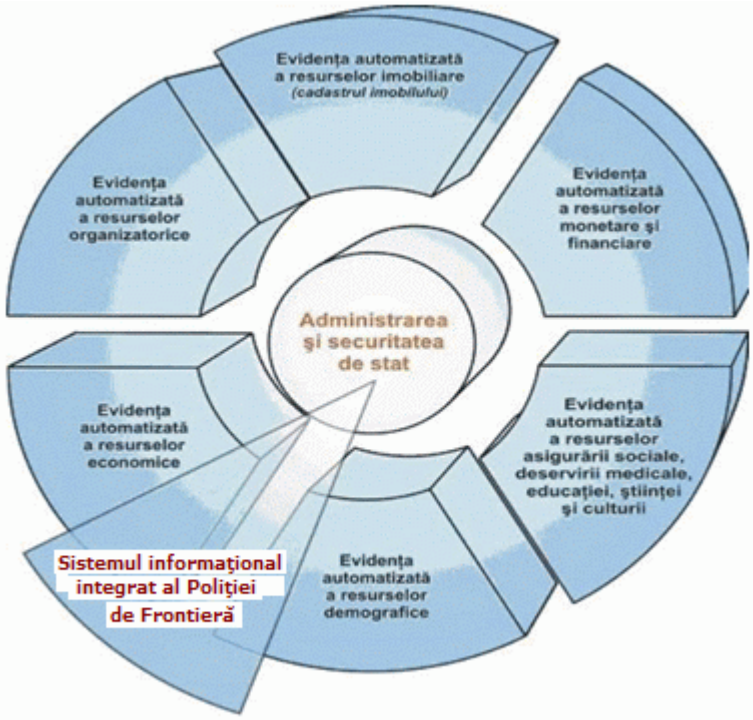

Fig.1. *Locul SIIPF în cadrul Resurselor informaţionale de stat ale Republicii Moldova*

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

1[1]. Noţiuni generale:

identificatori biometrici – datele biometrice conţinute de paşapoartele, 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 şi prelucrate în sistemele informaţionale de stat (amprenta digitală, imaginea facială, înălţimea, culoarea ochilor, grupa sangvină etc.).

[Pct.1[1] introdus prin Hot.Guv. nr.1064 din 12.12.2017, în vigoare 15.12.2017]

2. Destinaţia SIIPF

SIIPF este destinat pentru colectarea, prelucrarea, stocarea, actualizarea şi analiza inclusiv, în prealabil, a datelor despre persoanele fizice şi mijloacele de transport care traversează sau intenţionează să traverseze frontiera de stat a Republicii Moldova, despre evenimentele ce au loc pe segmentul verde al frontierei, cu punerea acestor informaţii la dispoziţia autorităţilor publice competente, altor persoane fizice şi juridice, în conformitate cu Legea nr.283 din 28 decembrie 2011 cu privire la Poliţia de Frontieră şi Legea nr.215 din 4 noiembrie 2011 cu privire la frontiera de stat a Republicii Moldova, precum şi cu alte acte legislative şi 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 şi eficace al frontierei de stat, pentru asigurarea nivelului adecvat de securitate pe toate sectoarele hotarului Republicii Moldova, aliniat la cerinţele comunitare, care să asigure sporirea gradului de securitate a persoanelor, respectînd drepturile şi libertăţile fundamentale ale acestora, fluidizarea traficului legal al persoanelor şi mărfurilor la frontieră. Scopul SIIPF poate fi atins prin realizarea următoarelor obiective:

a) asigurarea autorităţilor administraţiei publice competente cu informaţii veridice şi operative privind intrarea/ieşirea persoanelor şi mijloacelor de transport, necesare pentru luarea deciziilor judicioase la nivel de stat;

b) micşorarea timpului de staţionare în punctele de trecere a frontierei de stat a persoanelor şi a unităţilor de transport ce traversează frontiera de stat;

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

d) formarea unei bănci de date privind traversarea frontierei de către persoanele fizice şi unităţile de transport;

e) asigurarea interacţiunii efective între ministere şi alte autorităţi ale administraţiei publice centrale interesate;

f) depistarea persoanelor, mijloacelor de transport, documentelor anunţate în căutare, a cetăţenilor străini şi apatrizilor cărora intrarea în Republica Moldova le-a fost interzisă;

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

h) elaborarea metodologiei şi a criteriilor de identificare a riscului, potenţialului risc, profilurilor de risc;

i) aprecierea pierderilor posibile în cazurile apariţiei potenţialului risc, precum şi pierderile cauzate de riscurile depistate;

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

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

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

m) fixarea încălcărilor regimului frontierei de stat;

n) accesul rapid la resursele informaţionale ale Poliţiei 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 informaţionale automatizate, cele de bază fiind:

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

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

principul integrităţii, plenitudinii şi veridicităţii datelor;

principul confidenţialităţii informaţiei, care prevede răspunderea personală, în conformitate cu legislaţia în vigoare, a colaboratorilor responsabili de prelucrarea informaţiei în SIIPF pentru utilizarea şi difuzarea neregulamentară a informaţiei confidenţiale personificate;

principul securităţii informaţionale, care presupune asigurarea nivelului dorit al integrităţii, exclusivităţii, accesibilităţii şi eficienţei protecţiei datelor împotriva pierderii, denaturării, deteriorării şi utilizării neautorizate. Securitatea sistemului presupune rezistenţa la atacuri şi protecţia caracterului secret, a integrităţii şi pregătirea pentru lucru atît a sistemului, cît şi a datelor lui;

principiul compatibilităţii sistemului informaţional cu sistemele existente autohtone şi străine;

principiul scalabilităţii, care presupune asigurarea unei performanţe constante a soluţiei informatice la creşterea volumului de date şi a solicitării sistemului informaţional;

principiul unităţii spaţiului informaţional, care se referă la utilizarea unui sistem unic de clasificatoare, formate de date, protocoale de interacţiune informaţională, standarde, documente normative şi metodice interdependente;

principiul trasabilităţii, care prevede implementarea procedurilor de înregistrare a tuturor

acţiunilor/evenimentelor asupra obiectelor informaţionale ale SIIPF şi asigurarea capacităţii 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 legislaţia naţională şi tratatele internaţionale la care Republica Moldova este parte. Crearea şi funcţionarea SIIPF sunt reglementate de următoarele acte normative:

1) Legea nr.273/1994 privind actele de identitate din sistemul naţional de paşapoarte;
2) Legea nr.467/2003 cu privire la informatizare şi la resursele informaţionale 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 protecţia 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 Poliţia de Frontieră;
8) Legea nr.59/2012 privind activitatea specială de investigaţii;
9) Legea nr.142/2018 cu privire la schimbul de date şi interoperabilitate;
10) Legea nr.124/2022 privind identificarea electronică şi serviciile de încredere;
11) Legea nr.148/2023 privind accesul la informaţiile de interes public;
11^1) Codul transporturilor rutiere nr.150/2014;
12) Hotărârea Guvernului nr.735/2002 cu privire la sistemele speciale de telecomunicaţii ale Republicii Moldova;
13) Hotărârea Guvernului nr.562/2006 cu privire la crearea sistemelor şi resurselor informaţionale automatizate de stat;
14) Hotărârea Guvernului nr.1090/2013 privind serviciul electronic guvernamental de autentificare şi 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) şi a Regulamentului privind modul de funcţionare şi utilizare a serviciului guvernamental de notificare electronică (MNotify);
22) Hotărârea Guvernului nr.153/2021 pentru aprobarea Conceptului Sistemului informaţional „Registrul resurselor şi sistemelor informaţionale de stat" şi a Regulamentului privind modul de ţinere a Registrului resurselor şi sistemelor informaţionale de stat.

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

[Pct.5 în redacţia 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

SPAŢIUL FUNCŢIONAL AL SIIPF

6. Funcţiile SIIPF

SIIPF urmează să îndeplinească, pe lîngă funcţiile specifice determinate de obiectivele, scopurile şi destinaţia prezentului Concept tehnic, şi funcţiile de bază ale sistemului informaţional tip, stabilite în concepţia sistemului informaţional integrat de stat, cele de bază fiind:

a) formarea băncii de date, care include funcţiile de introducere a datelor în evidenţa iniţială, actualizarea şi radierea lor din evidenţă. Aceste funcţii se realizează în cadrul colectării datelor despre obiectele de evidenţă, precum şi pe parcursul schimbului de informaţii cu autorităţile administraţiei publice centrale şi locale. Informaţiile privind obiectul de evidenţă se introduc în banca de date a SIIPF numai pe baza documentelor ce confirmă autenticitatea lor, cu referinţe stricte la documentul în baza căruia s-a efectuat actualizarea datelor;

b) organizarea asigurării informaţionale din banca de date;

c) asigurarea calităţii informaţiilor din contul creării şi menţinerii componentelor sistemului de calitate;

d) asigurarea multiaspectuală a funcţionării SIIPF;

e) asigurarea protecţiei informaţiei la toate etapele de colectare, stocare şi prezentare;

f) asigurarea cu informaţie statistică a autorităţilor publice competente şi a publicului;

g) asigurarea integrabilităţii cu alte sisteme informaţionale de stat.

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

7. Contururile funcţionale ale SIIPF

SIIPF include următoarele contururi funcţionale:

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

b) conturul evidenţei şi controlului automatizat al persoanelor care trec frontiera de stat (B);

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

d) conturul evidenţei şi controlului automatizat al supravegherii frontierei de stat (D);

e) conturul evidenţei şi controlului automatizat al cazurilor de încălcare a legislaţiei privind frontiera de stat (E).

Fiecare dintre contururile funcţionale exercită mai multe funcţii specifice.

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

B. Conturul evidenţei şi controlului automatizat al persoanelor cuprinde datele privind evidenţa şi verificarea automatizată a persoanelor fizice care se deplasează peste frontiera de stat. El are următoarele funcţii:

a) înregistrarea şi controlul intrării şi ieşirii în/din ţară a persoanelor fizice;

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

c) controlul actelor prezentate de persoanele fizice.

C. Conturul evidenţei şi controlului automatizat al mijloacelor de transport reflectă evidenţa automatizată a mijloacelor de transport ce trec frontiera de stat. El are următoarele funcţii:

a) evidenţa mijloacelor de transport şi a agregatelor numerotate introduse pentru prima dată în Republica Moldova;

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

c) evidenţa mijloacelor de transport ce tranzitează frontiera pe rutele internaţionale;

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

e) controlul actelor privind mijloacele de transport:

certificatul de înregistrare al mijlocului de transport;

permisul de conducere.

D. Conturul evidenţei şi controlului automatizat al supravegherii frontierei de stat reflectă evidenţa automatizată a supravegherii frontierei de stat. El are următoarele funcţii:

a) colectarea, procesarea şi utilizarea datelor de natură generală, precum şi a datelor obţinute de Poliţia de Frontieră pe cazuri individuale;

b) fixarea şi controlul operativ al procesului de supraveghere a frontierei;

c) evidenţa colaboratorilor antrenaţi 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) evidenţa şi controlul valabilităţii permiselor de aflare în zona de frontieră (e-permis).

E. Conturul evidenţei şi controlului automatizat al cazurilor de încălcare a legislaţiei privind frontiera de stat reflectă evidenţa automatizată a persoanelor şi mijloacelor de transport implicate în aceste cazuri, precum şi controlul riscurilor. El are următoarele funcţii:

a) evidenţa şi analiza datelor privind starea criminogenă la frontieră (persoanele, mijloacele de transport implicate, bunurile materiale), stocarea şi păstrarea acestor date într-un spaţiu unic;

b) elaborarea metodologiei de identificare a riscului, identificarea potenţialului risc şi fixarea acestuia;

c) identificarea şi evidenţa cauzelor ce contribuie la încălcarea legislaţiei frontaliere în vigoare;

d) aprecierea şi evidenţa pierderilor posibile în cazurile apariţiei potenţialului risc, precum şi pierderile cauzate de riscurile depistate;

e) identificarea şi evidenţa măsurilor de prevenire a riscului, minimalizarea lui şi resursele necesare pentru aceasta;

f) controlul practic şi evidenţa măsurilor aplicate în contracararea şi minimalizarea riscurilor la frontieră.

F. Conturul evidenţei şi controlului, inclusiv automatizat, al datelor prealabile despre călători, cu următoarele funcţii:

a) colectarea, de la transportatorii aerieni, în prealabil, a datelor despre călători, prelucrarea şi evidenţa acestora;

b) crearea criteriilor prestabilite în conformitate cu cadrul normativ;

c) profilarea călătorilor în baza criteriilor prestabilite în scop de prevenire, depistare, investigare şi urmărire penală a infracţiunilor cu caracter terorist, a infracţiunilor transnaţionale sau a ameninţărilor la adresa securităţii 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 ORGANIZAŢIONALĂ A SIIPF

8. Deţinătorul SIIPF

Deţinătorul sistemului este Inspectoratul General al Poliţiei de Frontieră. SIIPF se înregistrează, în modul stabilit, în Registrul resurselor şi sistemelor informaţionale de stat, în conformitate cu prevederile Hotărîrii Guvernului nr.1032 din 6 septembrie 2006 “Cu privire la aprobarea Concepţiei sistemului informaţional automatizat “Registrul resurselor şi sistemelor informaţionale de stat”.

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

9. Registratorii SIIPF

Funcţiile legate de formarea şi exploatarea SIIPF revin Inspectoratului General al Poliţiei de Frontieră. Registratori ai sistemului sînt inspectorii calificaţi numiţi în funcţie, 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 informaţiei SIIPF

Există două categorii de utilizatori ai sistemului:

a) interni, care vor fi desemnaţi prin ordinul şefului Inspectoratului General al Poliţiei de Frontieră;

b) externi - entităţile publice competente şi structurile internaţionale de profil, care pot accesa informaţia din sistem numai în baza acordurilor interinstituţionale încheiate cu Inspectoratul General al Poliţiei 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) paşaportul cetăţeanului Republicii Moldova;

b) paşaportul diplomatic;

c) paşaportul de serviciu;

d) documentul de călătorie (Convenţia privind statutul apatrizilor din 28 septembrie 1954);

e) documentul de călătorie (Convenţia privind statutul refugiaţilor din 28 iulie 1951);

f) documentul de călătorie (protecţie umanitară);

g) buletinul de identitate al cetăţeanului Republicii Moldova;

h) buletinul de identitate electronic al cetăţeanului Republicii Moldova;

i) buletinul de identitate provizoriu al cetăţeanului Republicii Moldova;

j) buletinul de identitate pentru refugiaţi;

k) buletinul de identitate pentru apatrizi;

l) buletinul de identitate pentru beneficiarii de protecţie umanitară;

m) permisul de şedere permanentă;

n) permisul de şedere provizorie pentru cetăţenii străini;

o) permisul de şedere provizorie pentru apatrizi;

p) paşaportul marinarului;

q) paşaportul cetăţeanului străin sau documentul de călătorie valabil, emis de statul unde persoana îşi are stabilit domiciliul;

r) actul de identitate de uz intern al cetăţeanului străin, eliberat de autorităţile 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 internaţionale 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) paşaportul tehnic al unităţii 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 şi statistice;
c) procura pentru dreptul de însoţire 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
SPAŢIUL INFORMAŢIONAL AL SIIPF

12. Obiectele informaţionale

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

Obiectele de evidenţă şi control ale SIIPF sînt:
a) traversarea frontierei de stat:
- poliţistul de frontieră care a autorizat traversarea;
- persoana fizică care traversează frontiera de stat;
- mijlocul de transport;
- documentul;
- trecerea frontierei de stat;
b) planificarea activităţii de serviciu la controlul frontierei:
- rezultatul activităţii de control;
c) incidentul legat de încălcarea legislaţiei transfrontaliere:
- încălcarea regimului frontierei de stat;
- încălcarea regimului zonei de frontieră;
- încălcarea regimului punctelor de trecere a frontierei de stat etc.;
d) refuzul intrării/ieşirii în/din Republica Moldova:
- poliţistul de frontieră care nu a autorizat traversarea;
- persoana fizică;
- mijlocul de transport;
- documentul;
e) consemnul la frontieră:
- actul de dispoziţie;
- datele persoanei;
- datele mijlocului de transport;
- documentul.
f) permisul de aflare în zona de frontieră:
- numărul şi valabilitatea permisului de aflare în zona de frontieră;
- scopul aflării în zona de frontieră;
- datele persoanei;
- datele mijlocului de transport;
- informaţiile privind persoana juridică.

g) rezervarea biletului de zbor spre/dinspre Republica Moldova:
- datele biletului de zbor;
- persoana care a rezervat biletul de zbor;
- datele adiţionale privind rezervarea şi achiziţia 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 redacţia Hot.Guv. nr.1064 din 12.12.2017, în vigoare 15.12.2017]

13. Identificarea obiectelor informaţionale

Obiectele de evidenţă şi 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 uzanţelor internaţionale, 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 contravenţiei şi a infracţiunii - 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 informaţional prin intermediul cărora se realizează funcţiile SIIPF. Realizarea funcţiilor SIIPF are loc conform următoarelor scenarii:
a) pentru obiectul informaţional „traversarea frontierei de stat":
Evidenţa datelor se efectuează după autorizarea traversării frontierei de stat a Republicii Moldova în baza deciziei adoptate referitor la participanţii la traversare, ce va conţine informaţiile privind poliţistul de frontieră care a autorizat traversarea (numele, prenumele, gradul special şi numărul ştampilei autorizate întărite).
Modificarea datelor are loc în cazul depistării datelor eronate.
Radierea datelor are loc la expirarea termenului de stocare a informaţiei;
b) pentru obiectul informaţional „planificarea activităţii de serviciu la controlul frontierei":
Evidenţa datelor se efectuează după luarea deciziei cu privire la activităţile întreprinse pentru supravegherea frontierei de stat.
Radierea datelor are loc la expirarea termenului de stocare a informaţiilor, în conformitate cu instrucţiunile interne ale Inspectoratului General al Poliţiei de Frontieră;
c) pentru obiectul informaţional „incidentul legat de încălcarea legislaţiei transfrontaliere":
Evidenţa datelor se efectuează după depistarea incidentului şi întocmirea actelor procesuale.
Radierea datelor are loc la expirarea termenului de stocare a datelor;
d) pentru obiectul informaţional „refuzul intrării/ieşirii în/din Republica Moldova":
Evidenţa datelor se efectuează după refuzul intrării/ieşirii 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 informaţional „consemnul la frontieră":
Evidenţa datelor se efectuează în baza actelor de procedură prevăzute de legislaţia în vigoare, care va conţine numărul documentului ce întemeiază aplicarea consemnului, emitentul acestuia, temeiul legal, descrierea succintă a dispozitivului, data aplicării consemnului, data expirării interdicţiei, numele, prenumele şi gradul poliţistului care a aplicat în SIIPF consemnul la frontieră.
Modificarea datelor are loc:
- în cazul depistării datelor eronate;

- în cazul apariţiei unor circumstanţe legale în baza actelor prevăzute de legislaţia 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 legislaţia în vigoare.

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

Evidenţa datelor se efectuează în baza cererii depuse de persoana fizică/juridică. Datele conţin informaţiile privind datele din actul de identitate, existenţa antecedentelor penale, precum şi a încălcărilor anterioare ale regulilor regimului frontierei de stat şi ale regimului zonei de frontieră, scopul declarat, numărul şi seria permisului de aflare în zona de frontieră, data emiterii, data expirării, numele, prenumele şi gradul poliţistului 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 şi ale regimului zonei de frontieră;

- în cazul apariţiei unor circumstanţe legale, în baza actelor prevăzute de legislaţie.

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 informaţional rezervarea biletului de zbor spre/dinspre Republica Moldova:

Evidenţa datelor se efectuează din momentul furnizării datelor despre călători de la transportatorii aerieni, prin metoda „push”, prin cel puţin unul dintre următoarele formate şi 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 autorităţi); 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 autorităţi); 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 acelaşi zbor, aceştia 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 redacţia 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 şi ora traversării;

- direcţia de deplasare;

- punctul de trecere;

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

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

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

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

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

- informaţiile despre forţe şi mijloace implicate în activitatea de control;

- graficul şi orarul turelor;

- informaţiile despre tipurile de activitate de control;

- informaţiile despre ora şi data activităţii de control;

- informaţii despre itinerarele de deplasare şi locul de desfăşurare a activităţii de control;

- informaţiile despre rezultatele activităţii de control;

c) datele despre incidentul legat de încălcarea legislaţiei transfrontaliere:

- data şi ora producerii incidentului;

- locul producerii incidentului;

- tipul incidentului;

- date despre persoana implicată în incident;

- informaţiile despre mijlocul de transport implicat în incident;

- informaţiile despre bunuri, documente parte a incidentului;

- informaţii despre măsurile întreprinse în partea ce ţine de incident;

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

- data şi ora refuzului intrării/ieşirii;

- direcţia;

- punctul de trecere;

- temeiul refuzului autorizării;

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

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

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

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

e) datele despre consemnul la frontieră:

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

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

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

- documentul (tip, număr, data eliberării, ţara 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, iniţialele şi data naşterii ale pasagerului asociate rezervării, titlul/grad ştiinţific, alte informaţii cu privire la nume;

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

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

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

- itinerarul complet de călătorie (îmbarcare iniţială, escală, debarcare finală);

- informaţiile din profilul „client fidel” (frequent flyer);

- datele agenţiei sau agentului de turism (denumirea/numele şi 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, situaţia înregistrării pentru zbor, informaţii privind neprezentarea pasagerului la îmbarcare sau privind prezentarea acestuia în ultimul moment la îmbarcare, fără rezervare prealabilă;

- informaţiile scindate sau divizate din registrul cu numele pasagerilor;

- menţiunile cu caracter general, inclusiv toate informaţiile disponibile despre minorii neînsoţiţi cu vârsta sub 18 ani, precum numele, prenumele şi sexul minorului, vârsta, limba/limbile vorbită/vorbite, numele, prenumele şi datele de contact ale persoanei care îl însoţeşte la plecare şi relaţia sa cu minorul, numele, prenumele şi datele de contact ale persoanei care îl aşteaptă la sosire şi relaţia sa cu minorul, agentul prezent la plecare şi la sosire;

- informaţiile despre bilet, inclusiv numărul biletului, data emiterii biletului şi biletul dus simplu, câmpurile aferente furnizării automate a preţului unui bilet de călătorie;

- numărul locului şi alte informaţii privind locul (locul solicitat şi locul efectiv după închiderea zborului);

- informaţiile cu privire la partajarea de coduri;

- toate informaţiile cu privire la bagaje, numărul (cantitatea) de bagaje, numărul etichetei de identificare a bagajului, greutatea bagajelor, toată informaţia 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 destinaţie/descărcare a bagajului;

- numărul pasagerilor înregistraţi în PNR şi alte nume ale acestora;

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

- un istoric al tuturor modificărilor datelor PNR;

- numele şi prenumele persoanei care a făcut rezervarea;

- aşteptarea locului (standby);

- toate informaţiile despre înregistrarea pasagerului la ghişeu (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 autorizaţie:

- tipul autorizaţiei (autorizaţie de transport rutier de persoane prin servicii regulate, autorizaţie de tip pendular, autorizaţie de transport rutier de persoane prin servicii ocazionale, Carnet INTERBUS);

- seria şi/sau numărul autorizaţiei/lipsa acesteia;

- denumirea operatorului de transport;

- numărul de înmatriculare al autocarului;

- regimul de utilizare a autorizaţiei (bilateral, tranzit, ţară terţă).

[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 redacţia 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 veridicităţii informaţiilor şi reducerea volumului de date păstrate în SIIPF, se utilizează un sistem de clasificatoare care pot fi grupate în trei categorii:

a) internaţionale;

b) naţionale:

CS – clasificatorul statelor;

CA – clasificatorul modelelor unităţilor de transport;

CUTAM – clasificatorul unităţilor administrativ-teritoriale;

c) interne.

Clasificatoarele interne se elaborează şi se utilizează în cadrul SIIPF numai în lipsa clasificatoarelor internaţionale şi naţionale aprobate.

17. Sursele de informaţii ale SIIPF

Principala sursă de informaţii este Poliţia de Frontieră, care oferă date despre trecerea frontierei de stat de către persoane fizice şi mijloace de transport; date generale cu privire la supravegherea frontierei de stat; date statistice, informaţii individuale, factori de presiune, informaţii despre infracţionalitate şi informaţii referitoare la pericole.

Surse suplimentare de informaţii sînt:

a) Instituţia publică „Agenţia Servicii Publice", care oferă date privind persoanele fizice şi actele eliberate acestora, date privind mijloacele de transport;

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

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

d) Ministerul Justiţiei, care furnizează date privind deciziile instanţelor judecătoreşti prin care se interzice anumitor persoane fizice trecerea frontierei Republicii Moldova;

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

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

SIIPF este unica sursă de informaţii privind trecerea frontierei de stat de către persoane fizice şi mijloace de transport pentru sistemele informaţionale 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. Interacţiunea cu alte sisteme informaţionale

În scopul formării corecte a resursei informaţionale a SIIPF şi al asigurării furnizării datelor din această resursă autorităţilor/instituţiilor publice, în limitele competenţelor stabilite de actele normative, SIIPF va interacţiona, prin intermediul platformei de interoperabilitate (MConnect), cu următoarele sisteme informaţionale de stat:

a) Registrul de stat al populaţiei, care conţine date privind persoanele fizice şi actele eliberate acestora;

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

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

d) Sistemul informaţional integrat al organelor de drept;

e) Sistemul informaţional integrat automatizat de evidenţă a infracţiunilor, a cauzelor penale şi a persoanelor care au săvîrşit infracţiuni;

f) Sistemul informaţional automatizat "Registrul informaţiei criminalistice şi criminologice";

g) Sistemul informaţional automatizat "Registrul armelor";

h) Sistemul informaţional integrat vamal;

i) Sistemul informaţional 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 informaţional automatizat „Registrul de stat al populaţiei", ce conţine date privind vizele valabile pentru Republica Moldova;

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

l) Sistemul informaţional automatizat „Registru dactiloscopic”;

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

n) Sistemul informaţional „e-Autorizaţie transport”.

Interacţiunea cu registrele informaţionale ale altor state sau ale organizaţiilor internaţionale se va organiza în conformitate cu tratatele internaţionale 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
SPAŢIUL TEHNOLOGIC AL SIIPF

19. Nivelurile infrastructurii informaţionale

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

Arhitectura SIIPF este concepută după schema-tip a infrastructurii informaţionale a sistemului informaţional automatizat, în conformitate cu cerinţele expuse în Concepţia creării infrastructurii informaţionale de stat.

Infrastructura informaţională a SIIPF este amplasată în două niveluri:

a) central (A);

b) local (B).

A. Nivelul central este amplasat în municipiul Chişinău. Funcţia de bază a nivelului central al infrastructurii informaţionale de telecomunicaţii este asigurarea păstrării informaţiei şi acordarea ei utilizatorilor prin portalul informaţional de stat. La nivelul central se află banca centrală de date a sistemului.

B. Nivelul local este amplasat în unităţile teritoriale ale Poliţiei de Frontieră. În fiecare dintre unităţile teritoriale ale Poliţiei de Frontieră de toate nivelurile sistemului se instalează module-tip. Accesul la informaţie pentru utilizatorii autorizaţi se efectuează prin portalul informaţional.

[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 şi a mijloacelor tehnice utilizate la crearea infrastructurii informaţionale se determină de către elaboratorul sistemului în comun cu deţinătorul la etapele ulterioare de elaborare a sistemului.

Pentru comunicarea între nivelurile sistemului se utilizează sistemul de telecomunicaţii al autorităţilor administraţiei publice.

20^1. Integrarea cu sisteme informaţionale partajate

Pentru asigurarea funcţionării şi dezvoltării, SIIPF este integrat cu şi reutilizează funcţionalităţile generice ale sistemelor informaţionale partajate, în special, dar nu exclusiv:

1) serviciul electronic guvernamental de autentificare şi control al accesului (MPass) – pentru autentificarea şi 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 şi a interoperabilităţii cu alte sisteme informaţionale de stat;

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

operaţiunilor (evenimentelor) produse în cadrul sistemului;

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

[Pct.20[1] introdus prin Hot.Guv. nr.523 din 22.07.2022, în vigoare 29.07.2022]

Capitolul VIII
ASIGURAREA SECURITĂŢII INFORMAŢIONALE A SIIPF

21. Securitatea informaţională

Securitatea informaţională trebuie să fie asigurată printr-un sistem complex de măsuri juridice, tehnico-organizatorice şi economice, cu utilizarea mijloacelor tehnologice, dispozitivelor software/hardware şi a mecanismelor criptografice de protecţie a informaţiei, orientate spre asigurarea nivelului necesar de integritate, confidenţialitate şi accesibilitate al resurselor informaţionale.

La elaborarea, susţinerea funcţionării şi administrarea SIIPF, Inspectoratul General al Poliţiei de Frontieră se va conduce de legislaţia în vigoare şi standardele naţionale în domeniul asigurării securităţii informaţionale şi protecţiei informaţiei.

Metodele de asigurare a securităţii informaţionale trebuie reexaminate şi ajustate periodic sub aspect juridic, tehnico-organizatoric şi economic.

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

21[1]. Termenul de stocare a informaţiei

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.21[1] completat prin Hot.Guv. nr.1067 din 27.12.2023, în vigoare 05.02.2024]

[Pct.21[1] în redacţia Hot.Guv. nr.523 din 22.07.2022, în vigoare 29.07.2022]

[Pct.21[1] introdus prin Hot.Guv. nr.249 din 03.04.2014, în vigoare 05.04.2014]

22. Sarcinile securităţii informaţionale

a) Crearea sistemului complex al securităţii informaţionale include o serie de etape consecutive:
determinarea profilurilor protecţiei;
clasificarea resurselor protejate;
analiza riscurilor;
elaborarea politicii securităţii;
elaborarea arhitecturii securităţii;
crearea şi implementarea sistemului securităţii informaţionale;
certificarea sistemului.

b) Componentele de bază ale sistemului securităţii informaţionale sînt:
protecţia informaţiei şi infrastructurii de suport la conectarea la reţelele externe;
protecţia informaţiei în procesul interacţiunii între reţele;
protecţia fluxurilor de date;
protecţia serviciilor sistemului;
protecţia antivirus;
asigurarea securităţii mediului software;
autentificarea;
protocolare şi audit.

c) Mecanismele tehnologice de bază de asigurare a protecţiei securităţii informaţiei sînt:
autentificarea şi autorizarea;
dirijarea accesului;
înregistrarea acţiunilor şi auditul;

criptarea informaţiei;

delimitarea accesului utilizatorilor la date, în conformitate cu rolurile acestora în SIIPF;

aplicarea mijloacelor bioidentificării utilizatorilor;

aplicarea semnăturii digitale;

accesul la date doar prin interfaţa unică de obiect;

dirijarea centralizată şi controlul accesului la date.

d) Sistemul complex al securităţii informaţionale asigură:

confidenţialitatea informaţiei;

integritatea logică a informaţiei;

integritatea fizică a informaţiei;

protecţia infrastructurii informaţionale în cazul tentativelor de deteriorare sau de modificare a funcţionării SIIPF.

Una dintre cele mai vulnerabile verigi în sistemul securităţii informaţionale este factorul uman. În legătură cu aceasta, un element important al securităţii informaţionale este instruirea personalului, familiarizîndu-l cu metodele şi procedeele de contracarare a pericolelor.

23. Pericolele securităţii informaţionale

Prin pericol se subînţelege un eveniment sau o acţiune potenţială, orientată spre cauzarea de prejudicii resurselor informaţionale sau infrastructurii informaţionale.

a) Pericolele de bază ale securităţii informaţionale sînt:

colectarea şi utilizarea ilegală a informaţiei;

nimicirea, deteriorarea, suprimarea radioelectronică sau distrugerea mijloacelor şi sistemelor de prelucrare a informaţiei, de telecomunicaţii şi comunicaţii;

compromiterea cheilor şi mijloacelor de protecţie criptografică a informaţiei.

b) Obiecte ale pericolelor sînt resursele informaţionale sau infrastructura informaţională de telecomunicaţii.

c) Surse ale pericolelor sînt infractorii, funcţionarii publici corupţi, precum şi utilizatorii de rea-credinţă.

24. Protecţia informaţiilor împotriva accesului neautorizat

a) Sistemul de protecţie a informaţiilor împotriva accesului neautorizat include măsuri organizaţionale, echipamente şi produse de program care asigură blocarea:

scurgerii informaţiilor prin canalele tehnice;

accesului neautorizat la resursele reţelei.

Măsurile organizatorice de protecţie sînt asigurate de către serviciile respective ale participanţilor la sistem şi exclud accesul necontrolat al persoanelor străine la mijloacele tehnice ale sistemului informaţional de telecomunicaţii, la purtătorii magnetici, mijloacele de eliberare a copiilor pe suporţi materiali şi la sistemele de cablu.

b) Echipamentele şi produsele de program de protecţie contra accesului neautorizat asigură:

identificarea resurselor aflate sub protecţie;

autentificarea resurselor şi utilizatorilor aflaţi sub protecţie;

confidenţialitatea informaţiei care circulă în sistem;

schimbul de date autentificat;

integritatea datelor la apariţia, transmiterea, utilizarea şi păstrarea informaţiei;

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

delimitarea accesului utilizatorilor la sistem;

delimitarea accesului utilizatorilor la resursele aflate sub protecţie;

administrarea (indicarea dreptului de acces la resursele aflate sub protecţie, prelucrarea informaţiei din registre, instalarea şi dezinstalarea sistemului de protecţie);

înregistrarea acţiunilor de intrare a utilizatorilor în sistem, ieşire din sistem, încălcare a dreptului de acces la resursele aflate sub protecţie; controlul integrităţii şi capacităţii de funcţionare a sistemului de protecţie;

securitatea în situaţii de forţă majoră.

Capitolul IX
DISPOZIŢII FINALE ŞI TRANZITORII

25. Implementarea efectivă a SIIPF revine Inspectoratului General al Poliţiei 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 şi alte instituţii ale statului, precum şi organizaţii neguvernamentale, care cooperează potrivit competenţelor şi în condiţiile legii.

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

Anexa nr.2
la Hotărîrea 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 ţinere a Registrului care formează Sistemul informaţional integrat al Poliţiei de Frontieră

I. DISPOZIŢII GENERALE

1. Regulamentul privind modul de ţinere a Registrului care formează Sistemul informaţional integrat al Poliţiei de Frontieră (în continuare – *Regulament*) stabileşte modul de organizare şi funcţionare a Sistemului informaţional integrat al Poliţiei de Frontieră (în continuare – *SIIPF*), ce reprezintă ansamblul datelor, informaţiilor, fluxurilor şi circuitelor informaţionale, al procedurilor şi mijloacelor de acumulare şi utilizare a informaţiei necesare pentru realizarea obiectivelor Poliţiei de Frontieră.

2. Noţiunile utilizate în prezentul Regulament au semnificaţia prevăzută în Legea nr.467-XV din 21 noiembrie 2003 cu privire la informatizare şi la resursele informaţionale 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 informaţional integrat al Poliţiei de Frontieră din anexa nr.1.

În sensul prezentului Regulament se definesc următoarele noţiuni:

integritate – certitudinea, necontradictorialitatea şi actualitatea informaţiei, protecţia ei împotriva distrugerii şi modificării neautorizate;

recunoaştere facială – prelucrarea automatizată a imaginilor, care constă în identificarea unor caracteristici faciale specifice persoanei fizice, precum ochii, nasul şi gura, extragerea unor caracteristici esenţiale 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 şi duce la identificarea persoanei;

utilizator – persoana cu drept de acces la SIIPF. Există două categorii de utilizatori ai SIIPF – interni, care sînt desemnaţi prin ordinul şefului Inspectoratului General al Poliţiei de Frontieră, şi externi – autorităţile administraţiei publice centrale competente şi structurile internaţionale de profil, care pot accesa informaţia din SIIPF numai în baza acordurilor interinstituţionale încheiate cu Inspectoratul General al Poliţiei de Frontieră.

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

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

5. SIIPF creează spaţiul informaţional unic în care se stochează şi se prelucrează informaţii privind

traversarea frontierei de stat de către persoane fizice şi mijloace de transport, informaţii cu privire la supravegherea frontierei de stat, datele PNR date statistice, precum şi informaţii despre infracţionalitate şi pericole.

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

II. SUBIECŢII RAPORTURILOR JURIDICE ÎN DOMENIUL CREĂRII ŞI FUNCŢIONĂRII SIIPF

6. SIIPF este o resursă informaţională departamentală şi face parte din registrele de stat.

7. Subiecţi ai raporturilor juridice apărute ca rezultat al creării şi funcţionării SIIPF sînt:

1) statul, în calitate de proprietar;

2) Inspectoratul General al Poliţiei de Frontieră, în calitate de posesor, deţinător, administrator tehnic şi registrator al SIIPF;

3) persoana fizică care traversează frontiera de stat, în calitate de furnizor de date ale SIIPF;

3^1) transportatorii aerieni, în calitate de furnizor de date ale SIIPF;

4) persoana fizică sau juridică mandatată cu dreptul de a primi informaţii ce o vizează din SIIPF, conform legislaţiei, acordurilor internaţionale la care Republica Moldova este parte, precum şi acordurilor interinstituţionale încheiate cu Inspectoratul General al Poliţiei 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 Poliţiei de Frontieră realizează atribuţiile privind asigurarea funcţionării SIIPF prin crearea, implementarea, dezvoltarea şi ţinerea acestuia.

9. Posesorul, deţinătorul şi registratorul SIIPF sînt obligaţi:

1) să asigure funcţionarea SIIPF în conformitate cu actele normative în vigoare;

2) să asigure înregistrarea, colectarea, acumularea, prelucrarea şi stocarea informaţiilor în SIIPF în baza documentelor prezentate de către persoana fizică care traversează frontiera de stat sau în temeiul solicitărilor şi actelor legale ale subiecţilor de drept, în cazurile expres prevăzute de legislaţie;

3) să asigure corectitudinea, autenticitatea şi actualitatea datelor introduse în SIIPF;

4) să acorde utilizatorilor acces la SIIPF, în conformitate cu legislaţia în vigoare;

5) să asigure implementarea 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 din 14 decembrie 2010;

6) să efectueze monitorizarea şi supravegherea prelucrării informaţiei din SIIPF;

7) să efectueze auditul securităţii SIIPF;

7^1) să stocheze rezultatele auditului securităţii SIIPF pentru o perioadă de 3 ani;

8) să asigure regimul de securitate şi confidenţialitate a datelor stocate şi prelucrate în SIIPF;

9) să asigure integritatea informaţiilor stocate şi prelucrate în SIIPF.

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

10. Posesorul, deţinătorul şi registratorul SIIPF au următoarele drepturi:

1) să asigure implementarea şi respectarea cerinţelor de securitate informaţională a sistemului de către utilizatori, să fixeze şi să întreprindă măsuri de prevenire şi sancţionare a tentativelor de încălcare a regulilor de utilizare, în conformitate cu legislaţia în vigoare;

2) să iniţieze procedura de suspendare a drepturilor de acces la datele prelucrate şi stocate în SIIPF în cazurile de nerespectare a regulilor, standardelor şi normelor general acceptate în domeniul securităţii informaţionale şi protecţiei datelor cu caracter personal, în conformitate cu legislaţia în vigoare;

3) să perfecţioneze şi să eficientizeze funcţionalitatea SIIPF;

4) să refuze furnizarea informaţiilor din SIIPF în cazurile prevăzute de legislaţia în vigoare.

11. Utilizatorii SIIPF sînt obligaţi:

1) să utilizeze informaţia obţinută din SIIPF doar în scopurile stabilite de legislaţie;

2) să înştiinţeze imediat, prin orice mijloc de comunicare, Inspectoratul General al Poliţiei de Frontieră despre cazurile de încălcare a securităţii informaţionale a SIIPF;

3) să aducă imediat la cunoştinţa deţinătorului SIIPF orice situaţie de forţă majoră apărută care ar putea influenţa în mod negativ exercitarea funcţiilor utilizatorului.

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

1) să participe la crearea, implementarea şi dezvoltarea SIIPF, în conformitate cu legislaţia naţională;

2) să prezinte propuneri cu privire la iniţierea modificărilor actelor normative care reglementează funcţionarea SIIPF;

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

4) să prezinte propuneri deţinătorului SIIPF privind perfecţionarea şi eficientizarea funcţionării acestui sistem informaţional.

13. Drepturile şi obligaţiile destinatarului datelor din SIIPF se stabilesc în legislaţia privind accesul la informaţie, protecţia datelor cu caracter personal, activitatea specială de investigaţii, legislaţia procesual-penală şi procesual-civilă, legislaţia privind secretul de stat şi acordurile interinstituţionale încheiate cu Inspectoratul General al Poliţiei de Frontieră.

14. Ţinerea SIIPF este supusă controlului intern şi 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 cerinţelor privind crearea, ţinerea, exploatarea şi reorganizarea SIIPF este efectuat de organele statale abilitate prin lege.

III. ŢINEREA ŞI ASIGURAREA FUNCŢIONĂRII SIIPF

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

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

17. Obiectele informaţionale de bază ale SIIPF sînt:

1) traversarea frontierei de stat:

a) poliţistul 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 activităţii de serviciu la controlul frontierei:

a) rezultatul activităţii de control;

3) incidentul legat de încălcarea legislaţiei 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/ieşirii în/din Republica Moldova:

a) poliţistul de frontieră care nu a autorizat traversarea;

b) persoana fizică;

c) mijlocul de transport;

d) documentul;

5) consemnul la frontieră:

a) actul de dispoziţie;

b) datele persoanei;

c) datele mijlocului de transport;

d) documentul.

6) permisul de aflare în zona de frontieră:

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

b) scopul aflării în zona de frontieră;

c) datele persoanei;

d) datele mijlocului de transport;

e) informaţiile 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 adiţionale privind rezervarea şi achiziţia biletului de zbor;

d) criteriile prestabilite de profilare a călătorilor.

Evidenţa obiectelor informaţionale se ţine conform prezentului Regulament, precum şi conform instrucţiunilor aprobate de către posesorul SIIPF.

8) autorizaţia de transport:

a) tipul autorizaţiei;

b) denumirea operatorului de transport;

c) numărul de înmatriculare al autocarului;

d) regimul de utilizare a autorizaţiei;

e) seria şi/sau numărul autorizaţiei/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 informaţionale constituie datele SIIPF. Datele prelucrate prin intermediul SIIPF sînt:

1) datele despre traversarea frontierei de stat:

a) data şi ora traversării;

b) direcţia de deplasare;

c) punctul de trecere;

d) datele ce vizează poliţistul de frontieră care a autorizat traversarea (nume, prenume, grad special, numărul ştampilei autorizate întărite);

e) datele despre persoana fizică (nume, prenume, prenumele tatălui, sex, data naşterii, IDNP, cetăţenie, copiile digitale ale paginii de date a documentului de călătorie şi amprentelor digitale, statutul la traversarea frontierei – şofer, pasager, pieton, ciclist);

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

g) documentul (seria şi numărul documentului, data expirării);

2) datele despre planificarea activităţii de serviciu la controlul frontierei:

a) informaţiile despre forţe şi mijloace implicate în activitatea de control;

b) graficul şi orarul turelor;

c) informaţii despre tipurile de activitate de control;

d) datele despre ora şi data activităţii de control;

e) informaţiile despre itinerarele de deplasare şi locul de desfăşurare a activităţii de control;

f) informaţiile despre rezultatele activităţii de control;

3) datele despre incidentul legat de încălcarea legislaţiei transfrontaliere:

a) data şi ora producerii incidentului;

b) locul producerii incidentului;

c) tipul incidentului;

d) date despre persoana implicată în incident;

e) informaţiile despre mijlocul de transport implicat în incident;

f) informaţiile despre bunuri, documente parte a incidentului;

g) informaţii despre măsurile întreprinse în partea ce ţine de incident;

4) datele despre refuzul intrării/ieşirii în/din Republica Moldova:

a) data şi ora refuzului intrării/ieşirii;

b) direcţia;

c) punctul de trecere;

d) temeiul refuzului autorizării;

e) datele privind poliţistul de frontieră care nu a autorizat traversarea (nume, prenume, grad special, numărul ştampilei autorizate întărite);

f) datele despre persoană (nume, prenume, prenumele tatălui, sex, data naşterii, IDNP, cetăţenie, statutul persoanei la traversarea frontierei – şofer, pasager, pieton, ciclist);

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

h) documentul (seria şi numărul documentului, data expirării);

5) datele despre consemnul la frontieră:

a) actul de dispoziţie (temeiul emiterii, data emiterii, măsura aplicată, autoritatea care ţine controlul consemnului, termenul încetării consemnului la frontieră);

b) datele persoanei (nume, prenume, prenumele tatălui, data naşterii, IDNP);

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

d) documentul (tip, număr, data eliberării, ţara emitentă, termen de valabilitate).

6) datele despre permisul de aflare în zona de frontieră:

a) datele despre persoana fizică (nume, prenume, data naşterii, IDNP, cetăţenie, fotografie, declaraţie pe proprie răspundere privind lipsa de antecedente penale şi încălcări anterioare ale legislaţiei cu privire la frontiera de stat, precum şi privind respectarea legislaţiei în timpul aflării în zona de frontieră, locul, perioada şi scopul aflării, numărul permisului, data emiterii permisului, perioada pentru care s-a acordat permisul, informarea în prealabil a subdiviziunii Poliţiei de Frontieră, observaţii);

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, observaţii);

c) datele despre persoana juridică (denumire, număr de identificare de stat (IDNO), adresa juridică, activitatea pentru care este solicitat permisul, actul care permite desfăşurarea activităţii; autorizarea organului vamal privind desfăşurarea activităţii 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; declaraţia pe proprie răspundere a angajatului agentului economic sau organizaţiei privind lipsa de antecedente penale şi încălcări anterioare ale legislaţiei cu privire la frontiera de stat, precum şi privind respectarea legislaţiei referitoare la frontiera de stat; numărul permisului, data emiterii permisului, perioada pentru care s-a acordat acesta, informarea în prealabil a subdiviziunii Poliţiei de Frontieră, observaţii);

d) datele personale ale poliţistului de frontieră care a validat emiterea permisului de aflare în zona de frontieră (nume, prenume, grad special, numărul şi seria legitimaţiei 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, iniţialele şi data naşterii ale pasagerului asociate rezervării, titlul/grad ştiinţific, alte informaţii cu privire la numele pasagerului;

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

f) toate informaţiile privind forma de plată, inclusiv adresa de facturare (numerar, card de credit, numărul şi data expirării cardului de credit, notificarea de plată în avans (PTA), valuta, datele despre persoana/agenţia care efectuează plata, codurile reducerilor de serviciu pentru personal);

g) itinerarul complet de călătorie (îmbarcare iniţială, escală, debarcare finală);

h) informaţiile din profilul „client fidel” (frequent flyer);

i) datele agenţiei sau agentul de turism (denumirea/numele şi 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, situaţia

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

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

l) menţiunile cu caracter general, inclusiv toate informaţiile disponibile despre minorii neînsoţiţi cu vârsta sub 18 ani, precum numele, prenumele şi sexul minorului, vârsta, limba/limbile vorbită/vorbite, numele, prenumele şi datele de contact ale persoanei care îl însoţeşte la plecare şi relaţia sa cu minorul, numele, prenumele şi datele de contact ale persoanei care îl aşteaptă la sosire şi relaţia sa cu minorul, agentul prezent la plecare şi la sosire;

m) informaţiile despre biletul de călătorie, inclusiv numărul biletului, data emiterii biletului şi bilete dus simplu, câmpurile aferente furnizării automate a preţului unui bilet de călătorie;

n) numărul locului şi alte informaţii privind locul (locul solicitat şi locul efectiv după închiderea zborului);

o) informaţiile cu privire la partajarea de coduri;

p) toate informaţiile cu privire la bagaje, numărul (cantitatea) de bagaje, numărul etichetei de identificare a bagajului, greutatea bagajelor, toată informaţia 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 destinaţie/descărcare a bagajului;

q) numărul pasagerilor înregistraţi în PNR şi alte nume ale acestora;

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

s) un istoric al tuturor modificărilor datelor PNR;

t) numele şi prenumele persoanei care a făcut rezervarea;

u) aşteptarea locului (standby);

v) toate informaţiile despre înregistrarea pasagerului la ghişeu (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 autorizaţie:

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

b) seria şi/sau numărul autorizaţiei/lipsa acesteia;

c) denumirea operatorului de transport;

d) numărul de înmatriculare al autocarului;

e) regimul de utilizare a autorizaţiei (bilateral, tranzit, ţară terţă).

[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 şi 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 internaţionale la care Republica Moldova este parte.

21. Datele despre unităţile 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 informaţiilor ce sînt prelucrate şi stocate în SIIPF sînt reglementate în capitolul VI din anexa nr.1.

23. Modalitatea de introducere şi folosire a datelor SIIPF prevăzute în pct.18 subpct.2), 4), 5) şi 6) din prezentul Regulament se stabileşte de către şeful Inspectoratului General al Poliţiei de Frontieră, în

conformitate cu legislaţia 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 şi stocată fotografia digitală a feţei şi amprentele digitale doar ale persoanei supuse verificării prin metoda de recunoaştere facială şi sistemul de verificare a amprentei 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 existenţei consimţămîntului persoanei de a fi supusă procedurilor de verificare prin metoda recunoaşterii faciale şi 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 redacţia 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) ordonanţa organului de urmărire penală;

2) încheierea instanţei judecătoreşti referitoare la judecarea cauzei;

3) demersul motivat al subiecţilor care efectuează activitatea specială de investigaţii, în condiţiile legii.

27. Prelungirea termenului de stocare a datelor din SIIPF urmează a fi efectuată cu asigurarea drepturilor şi libertăţilor subiectului datelor cu caracter personal, în baza deciziei motivate emise de o comisie specială, formată din reprezentanţii deţinătorului SIIPF, care include, în mod obligatoriu, persoana responsabilă de politica de securitate a datelor cu caracter personal din cadrul Inspectoratului General al Poliţiei de Frontieră. Comisia specială este formată în componenţă nominală potrivit ordinului şefului Inspectoratului General al Poliţiei de Frontieră.

28. În cazurile prevăzute la pct.26, subiecţii de drept indică, în mod obligatoriu, termenul ce urmează a fi prelungit în vederea asigurării statutului activ al informaţiilor prelucrate şi stocate în SIIPF, norma legală care întemeiază acest fapt şi actul juridic care întemeiază această necesitate, cum ar fi ordonanţa, încheierea etc., precum şi informează asupra necesităţii restricţionării drepturilor subiecţilor de date cu caracter personal sau lipsei acestei necesităţi.

29. Termenul de stocare a datelor în SIIPF nu poate fi prelungit decît 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. Ţinerea SIIPF este asigurată pînă la adoptarea deciziei de lichidare a acestuia. În cazul lichidării SIIPF, datele şi documentele conţinute în acesta se transmit în arhivă, conform legislaţiei.

31. Datele din SIIPF fac parte din categoria informaţiilor oficiale cu accesibilitate limitată. Asigurarea securităţii, confidenţialităţii şi integrităţii datelor prelucrate în cadrul SIIPF se efectuează cu respectarea strictă a Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal.

IV. INTEROPERABILITATEA CU ALTE SISTEME INFORMAŢIONALE

32. Pentru asigurarea formării corecte a resursei informaţionale şi asigurarea SIIPF cu date veridice, se realizează interacţiunea şi sincronizarea cu sistemele informaţionale de stat care conţin date despre persoane, documente, mijloace de transport şi alte date relevante pentru activitatea Poliţiei de Frontieră.

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

Inspectoratului General al Poliţiei de Frontieră, recepţionarea informaţiei suplimentare din partea furnizorilor de informaţii, inclusiv automatizat în cazul schimbării datelor din sistemele informaţionale de stat cu care interacţionează SIIPF.

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

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

36. Interacţiunea cu registrele informaţionale internaţionale se organizează în conformitate cu tratatele internaţionale la care Republica Moldova este parte.

V. REGIMUL JURIDIC DE UTILIZARE A DATELOR DIN SIIPF

37. Punerea la dispoziţie a datelor din SIIPF şi furnizarea lor de către deţinătorul SIIPF autorităţilor şi instituţiilor publice se realizează prin intermediul platformei de interoperabilitate (MConnect) în conformitate cu prevederile cadrului normativ în domeniul schimbului de date şi interoperabilităţii, în condiţiile în care acestea invocă un scop şi un temei legal pentru prelucrarea setului de date solicitat şi respectă cerinţele de securitate şi confidenţialitate ce decurg din regimul juridic al datelor vizate.

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

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

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

39. Informaţia generată în SIIPF se marchează, indicîndu-se prescripţia pentru prelucrarea ulterioară a acesteia şi numărul de identificare unic din Registrul de evidenţă a operatorilor de date cu caracter personal.

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

41. Destinatarul datelor din SIIPF nu este în drept să modifice datele obţinute 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 informaţia stocată şi prelucrată în SIIPF în funcţie de rolurile şi drepturile atribuite.

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

1) numele utilizatorului;

2) codul (parola) de acces.

44. Parola de acces este generată în mod manual de către deţinătorul SIIPF şi este transmisă utilizatorului prin una dintre următoarele modalităţi:

1) personal, contra semnătură;

2) prin intermediul poştei recomandate, cu inscripţia „personal”.

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

46. La prelucrarea informaţiei din SIIPF, utilizatorii au obligaţia asigurării protecţiei datelor cu caracter personal, conform Legii nr.133 din 8 iulie 2011 privind protecţia datelor cu caracter personal.

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

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

SIIPF;

2) la apariţia circumstanţelor de forţă majoră;

3) la încălcarea securităţii informaţionale în cadrul SIIPF, dacă aceasta prezintă pericol pentru funcţionarea lui;

4) la încălcarea legislaţiei cu privire la protecţia datelor cu caracter personal.

48. Lucrările profilactice în complexul de mijloace software şi hardware ale SIIPF se efectuează după notificarea în scris a utilizatorilor cu cel puţin 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 situaţii:

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 atribuţii nu impun accesul la datele din SIIPF;

3) la constatarea încălcării de către utilizator a securităţii informaţionale a SIIPF şi legislaţiei privind protecţia datelor cu caracter personal.

VII. ASIGURAREA PROTECŢIEI ŞI SECURITĂŢII INFORMAŢIEI ŞI RESURSELOR INFORMAŢIONALE ALE SIIPF

50. Măsurile de protecţie şi securitate a informaţiei din SIIPF reprezintă o parte componentă a lucrărilor de creare, dezvoltare şi exploatare a SIIPF şi se efectuează neîntrerupt de către deţinătorul SIIPF.

51. Obiecte ale asigurării protecţiei şi securităţii informaţiei din SIIPF se consideră:

1) masivele informaţionale, indiferent de formele păstrării, bazele de date, suporturile materiale care conţin informaţii privind date cu caracter personal;

2) sistemele informaţionale, sistemele operaţionale, sistemele de gestionare a bazelor de date şi alte aplicaţii care asigură activitatea SIIPF;

3) sistemele de telecomunicaţii, reţelele, inclusiv mijloacele de confecţionare şi multiplicare a documentelor şi alte mijloace tehnice de prelucrare a informaţiei.

52. Protecţia informaţiei cu caracter personal din SIIPF se efectuează prin următoarele metode:

1) prevenirea conexiunilor neautorizate la reţelele telecomunicaţionale şi a interceptării cu ajutorul mijloacelor tehnice a datelor din SIIPF transmise prin aceste reţele, asigurată prin folosirea metodelor de cifrare şi criptare a acestei informaţii, inclusiv cu utilizarea măsurilor organizatorice, tehnice şi de regim;

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

3) prevenirea acţiunilor intenţionate şi/sau neintenţionate ale participanţilor la SIIPF care pot conduce la distrugerea sau modificarea datelor din SIIPF, prin metoda folosirii mijloacelor de protecţie speciale tehnice şi de program, inclusiv a programelor licenţiate, programelor antivirus, organizarea sistemului de control al securităţii softului şi efectuarea periodică a copiilor de siguranţă.

53. Deţinătorul SIIPF elaborează, aprobă şi organizează implementarea documentului care stabileşte politica de securitate informaţională pentru asigurarea respectării regulilor, standardelor şi normelor general acceptate în domeniul securităţii informaţionale, cu indicarea:

1) identităţii persoanei responsabile de politica de securitate;

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

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

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

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

6) responsabilităţilor utilizatorilor SIIPF privind asigurarea securităţii informaţionale;

7) procedurilor de control intern al utilizatorilor SIIPF privind respectarea condiţiilor de securitate informaţională.

54. Deţinătorul SIIPF desemnează o persoană subordonată nemijlocit conducătorului instituţiei,

responsabilă de elaborarea, implementarea şi monitorizarea respectării prevederilor politicii de securitate informaţională.

55. Persoana responsabilă de politica securităţii informaţionale asigură definirea clară a tuturor responsabilităţilor cu privire la securitatea informaţiei din SIIPF (prevenire, supraveghere, detectare şi prelucrare), precum şi operarea cu ele.

56. În cazul operării cu informaţia din SIIPF ce a devenit cunoscută utilizatorului SIIPF în urma activităţii sale, este asigurat regimul de confidenţialitate, care presupune următoarele acţiuni:

1) limitarea numărului persoanelor cu drept de acces la datele din SIIPF;

2) monitorizarea procedurii de admitere şi delimitarea funcţională a responsabilităţilor persoanelor care au acces la informaţia din SIIPF;

3) identificarea şi autentificarea participanţilor la SIIPF cu folosirea mijloacelor moderne de autentificare;

4) executarea măsurilor de protecţie a informaţiei în cadrul păstrării, prelucrării şi transmiterii acesteia prin intermediul canalelor de comunicaţii.

VIII. PROTECŢIA DATELOR CU CARACTER PERSONAL, CONTROLUL ŞI RESPONSABILITATEA

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

58. Persoanele împuternicite cu drept de acces la SIIPF sînt obligate de a nu divulga informaţia cu accesibilitate limitată la care au primit acces în legătură cu exercitarea atribuţiilor funcţionale, inclusiv după încetarea activităţii. Pentru încălcarea clauzei de confidenţialitate, persoanele vinovate răspund în conformitate cu legislaţia în vigoare.

59. Responsabilitatea pentru organizarea şi funcţionarea SIIPF se atribuie deţinătorului, care elaborează tipul şi modelul documentelor aferente, instrucţiunile privind modul de completare şi alte materiale necesare pentru funcţionarea SIIPF.

La prelucrarea datelor cu caracter personal, posesorul asigură măsuri organizatorice şi tehnice necesare pentru protecţia datelor cu caracter personal împotriva distrugerii, a modificării, a blocării, a copierii, a răspândirii, precum şi împotriva altor acţiuni ilicite, măsuri menite să asigure un nivel de securitate adecvat în ceea ce priveşte riscurile prezentate de prelucrare şi 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 informaţionale de date cu caracter personal, deţinătorul întreprinde, de comun acord cu autorităţile competente, conform actelor normative, măsurile necesare pentru depistarea sursei de producere a incidentului, efectuează analiza acestuia şi înlătură cauzele incidentului de securitate, cu informarea autorităţilor 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]