



CANCELARIA DE STAT A REPUBLICII MOLDOVA

Nr. 26/3-76-10906

Chișinău

11 octombrie 2023

Biroul Permanent al Parlamentului

În temeiul art.73 din Constituția Republicii Moldova, se prezintă spre examinare pentru aprobarea proiectului de lege privind utilizarea datelor din registrul cu numele pasagerilor, aprobat prin Hotărârea Guvernului nr. 768 din 11.10.2023.

În context, comunică, că Ministerul Afacerilor Interne este responsabil de prezentarea proiectului.

Anexe:

1. Hotărârea Guvernului nr. 768/2023 privind aprobarea proiectului de lege privind utilizarea datelor din registrul cu numele pasagerilor, (în limba română – 1 filă și în limba rusă – 1 filă);
2. Proiectul de lege privind utilizarea datelor din registrul cu numele pasagerilor (în limba română – 23 file și în limba rusă – 27 file);
3. Nota informativă (4 file);
4. Avizele recepționate în procesul avizării (58 file);
5. Sinteza obiecțiilor și propunerilor (recomandărilor) la proiectul hotărârii Guvernului pentru aprobarea proiectului de lege privind utilizarea datelor din registrul cu numele pasagerilor (44 file);
6. Tabel de concordanță Decizia de punere în aplicare (UE) 2017/759 a Comisiei din 28.04.2023 (4 file);
7. Tabel de concordanță Directiva (UE) nr. 2016/681 al Parlamentului European și a Consiliului din 27.04.2026 (39 file)
8. Analiza impactului la proiectul de lege privind utilizarea datelor din registrul cu numele pasagerilor (29 file);
9. Raportul de expertiză juridică (6 file);
10. Raportul de expertiză anticorupție (5).

Secretar general adjunct al Guvernului

Roman CAZAN

Ex. O. Zglavoci
Tel. 0(22) 250-465
e-mail: olga.zglavoci@gov.md

Casa Guvernului,
MD-2033, Chișinău,
Republica Moldova

Telefon:
+ 373 22 250 101

Fax:
+ 373 22 242696

SECRETARIATUL PARLAMENTULUI REPUBLICII MOLDOVA		
P.D.P. Nr. 365		
- 12 -	10	2023
Ora _____		



GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. 768

din 11 octombrie 2023

Chișinău

**Pentru aprobarea proiectului de lege privind utilizarea
datelor din registrul cu numele pasagerilor**

Guvernul HOTĂRĂȘTE:

Se aprobă și se prezintă Parlamentului spre examinare proiectul de lege privind utilizarea datelor din registrul cu numele pasagerilor.

Prim-ministru



DORIN RECEAN

Contrasemnează:

Ministrul afacerilor interne

Adrian Efros

Ministrul justiției

Veronica Mihailov-Moraru

PARLAMENTUL REPUBLICII MOLDOVA**LEGE****privind utilizarea datelor din registrul cu numele pasagerilor**

Prezenta lege transpune:

- Directiva (UE) nr. 2016/681 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave, publicat în Jurnalul Oficial al Uniunii Europene seria L nr.119 din 4 mai 2016;

- 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, publicat în Jurnalul Oficial al Uniunii Europene seria L nr. 113 din 29 aprilie 2017.

Parlamentul adoptă prezenta lege ordinară.

Capitolul I
DISPOZIȚII GENERALE**Articolul 1. Obiectul de reglementare**

(1) Prezenta lege reglementează:

a) transmiterea de către transportatorii aerieni a datelor din registrul cu numele pasagerilor (în continuare - *PNR*) prevăzute în Anexa nr. 1, la unitatea de informații privind pasagerii (în continuare - *UIP*) prevăzută la art. 3;

b) prelucrarea datelor PNR, inclusiv colectarea, utilizarea și păstrarea acestora de către UIP;

c) schimbul de date PNR cu alte state;

d) transmiterea datelor PNR prelucrate de UIP către Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (în continuare - *Europol*).

(2) Prezenta lege nu limitează drepturile entităților publice de a solicita și de a obține de la transportatorii aerieni datele din registrele cu numele pasagerilor deținute de acestea, în condițiile Codului de procedură penală al Republicii Moldova nr.122/2003.

(3) Prevederile prezentei legi nu afectează drepturile și obligațiile părților care sunt prevăzute în Acordul privind cooperarea operațională și strategică dintre Republica Moldova și Oficiul European de Poliție, ratificat prin Legea nr. 116/2015.

Articolul 2. Noțiuni

În sensul prezentei legi se utilizează următoarele noțiuni:

călător – orice pasager și/sau membru al echipajului;

cerere temeinic justificată – solicitare, inclusiv conform acordurilor internaționale la care Republica Moldova este parte, din partea unei autorități competente care efectuează activități speciale de investigații și/sau exercită urmărire penală în legătură cu o persoană de interes, suspectată în activitatea infracțională, cu o legătură obiectivă, chiar și indirectă, în perioada de referință, pentru furnizarea datelor PNR sau rezultatul prelucrării acestora în scopul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor cu caracter terorist, infracțiunilor transnaționale sau pentru prevenirea și contracararea amenințărilor la adresa securității statului;

criterii prestabilite – criterii de căutare predeterminate, bazate pe investigații penale și informații anterioare și în curs, stabilite de către UIP în cooperare cu autoritățile competente, care permit profilarea pasagerilor și care corespund anumitor caracteristici cum ar fi, dar care nu se limitează la: pasager care călătorește pe anumite rute utilizate în mod obișnuit pentru traficul de droguri, procurarea biletului în ultimul moment, achitarea cu bani cash;

depersonalizare prin mascarea elementelor de date – acțiuni care are drept scop ca acele elemente ale datelor PNR care servesc la identificarea directă a unei persoane să nu fie vizibile pentru utilizatorii registrului cu numele pasagerilor;

date prelabile despre pasageri (date API) – set de date despre zbor și datele biografice ale unui călător, conținute de documentul de călătorie al titularului în zona de citire automată cu caractere identificabile optic, prevăzute ca parte componentă a datelor PNR, oferite/puse la dispoziție de transportatorii aerieni;

infracțiuni cu caracter terorist – infracțiunile prevăzute la art. 134¹¹ din Codul Penal al Republicii Moldova nr. 985/2002;

infracțiuni transnaționale – infracțiunile, pentru care pedeapsa prevăzută de legea penală este detențiunea pe viață sau închisoarea pentru o perioadă maximă de cel puțin 3 ani, corespunzătoare formelor de criminalitate prevăzute în Anexa nr. 2;

Se consideră că o infracțiune are caracter transnațional în special în cazul în care:

(1) este comisă în mai multe țări;

(2) este comisă într-o țară, dar pregătirea, planificarea, conducerea sau controlul său are loc, în mare parte, în altă țară;

(3) este săvârșită într-o țară, dar implică un grup infracțional organizat care desfășoară activități infracționale în mai multe țări;

(4) este comisă într-o țară, dar are efecte semnificative în altă țară; sau

(5) este comisă într-o țară, dar infractorul se află sau intenționează să călătorească în altă țară.

membru al echipajului – orice persoană aflată la bordul unei aeronave în timpul zborului, altele decât pasagerii, care activează pe și operează o aeronavă, inclusiv membrii echipajului de zbor și membrii echipajului de cabină;

metoda de tip push – metodă prin care transportatorii aerieni transmit datele PNR către UIP și care presupune realizarea unei transmisiuni active de date din sistemele transportatorilor aerieni în registrul cu numele pasagerilor;

pasager – orice persoană fizică, inclusiv persoanele aflate în transfer sau în tranzit, excluzând membrii echipajului, transportată sau care urmează să fie transportată într-o aeronavă cu consimțământul transportatorului aerian, acest consimțământ fiind exprimat prin înregistrarea persoanei respective pe lista pasagerilor;

profilul „client fidel” – înregistrările cu privire la persoane fizice realizate de transportatori aerieni în cadrul programelor de fidelitate derulate de către aceștia;

partajare de coduri (code share) – acord în temeiul căruia un operator atribuie codul său de identificare unui zbor efectuat de alt operator și vinde și eliberează bilete pentru respectivul zbor;

rezultat pozitiv – verificarea manuală, efectuată de către personalul UIP, în diverse surse și sisteme informaționale din gestiune în vederea validării rezultatului obținut în mod automatizat (soluția soft);

rezultat negativ – situații în care o comparație a datelor unui pasager cu o bază de date sau cu o listă de urmărire, generează o potrivire care nu este confirmată prin prelucrare ulterioară;

sistem de control al plecărilor – sistem automat de înregistrare a pasagerilor, bagajelor și încărcăturii cargo, îmbarcate la bordul unei aeronave;

registrul cu numele pasagerilor – resursă informațională instituită în scopul păstrării, prelucrării și furnizării de informații necesare controlului rezervărilor de către transportatorii aerieni care efectuează rezervările și de către transportatorii aerieni participanți, pentru fiecare călătorie rezervată de către sau în numele oricărei persoane, indiferent că este conținut în sistemele de rezervare, în sistemele de control al plecărilor utilizate pentru verificarea pasagerilor la îmbarcarea în avion sau în sistemele echivalente care oferă aceleași funcționalități;

sistem de rezervare – sistemul intern al transportatorului aerian, în care datele PNR sunt colectate pentru gestionarea rezervărilor;

transportator aerian – orice persoană fizică sau juridică, din Republica Moldova sau străinătate, deținătoare a unui certificat de operator aerian valabil, și după caz, a unei licențe de operare, care îi permite să efectueze operațiuni de transport aerian;

Unitate de informații privind pasagerii – subdiviziune creată în cadrul Poliției de Frontieră, fără personalitate juridică;
zbor – orice zbor regulat sau neregulat efectuat de transportatorii aerieni.

Capitolul II

FUNCȚIILE OPERAȚIONALE

Secțiunea I

Unitatea de informații privind pasagerii

Articolul 3. Înființarea unității de informații privind pasagerii

Unitatea de informații privind pasagerii exercită următoarele atribuții:

- a) colectează datele PNR de la transportatorii aerieni, asigură stocarea și prelucrarea acestor date, precum și transferul datelor respective sau al rezultatului prelucrării acestora autorităților competente menționate la art. 13;
- b) asigură schimbul de date PNR și schimbul de rezultate ale prelucrării datelor PNR cu UIP din alte state, organizații internaționale și cu Europol.

Articolul 4. Personalul UIP

(1) UIP este condusă de un șef, numit în funcție de către Șeful Inspectoratului General al Poliției de Frontieră (în continuare IGPF), în condițiile legii.

(2) Personalul UIP este constituit din funcționari publici cu statut special. În cadrul UIP pot fi detașați, în condițiile legii, angajați din cadrul autorităților competente prevăzute la art. 13, în scopul efectuării evaluării datelor în conformitate cu art. 10-12.

(3) Acordarea personalului UIP a drepturilor de acces la datele PNR, în scopul efectuării evaluărilor prevăzute la art. 10-12, se efectuează cu respectarea principiului necesității de a cunoaște.

Secțiunea II

Responsabilul de protecția datelor în cadrul UIP

Articolul 5. Persoana responsabilă de protecția datelor

(1) Pentru monitorizarea operațiunilor de prelucrare a datelor cu caracter personal și respectării actelor normative privind protecția datelor cu caracter personal, șeful IGPF desemnează o persoană responsabilă cu atribuții de protecție a datelor cu caracter personal.

(2) Responsabilul cu protecția datelor este desemnat din cadrul IGPF pe baza calităților profesionale și, în special, a cunoștințelor de specialitate în domeniul dreptului și practicilor din domeniul protecției datelor, precum și pe baza capacității de a îndeplini sarcinile prevăzute la art. 7.

(3) În exercitarea sarcinilor privind respectarea cadrului normativ privind protecția datelor cu caracter personal, responsabilul de protecția datelor este independent și imparțial, precum și nu primește instrucțiuni pe cale ierarhică pentru îndeplinirea sarcinilor sale.

(4) La nivelul IGPF se pot înființa una sau mai multe funcții pentru oferirea asistenței persoanei responsabile de protecția datelor.

(5) Responsabilul cu protecția datelor în cadrul UIP își desfășoară activitatea în subordinea nemijlocită a șefului IGPF. În cazul absenței responsabilului cu protecția datelor de la serviciu pentru o perioadă mai mare de 5 zile, șeful IGPF asigură preluarea sarcinilor de serviciu a responsabilului în cadrul UIP.

(6) IGPF publică datele responsabilului cu protecția datelor pe pagina web oficială și le comunică Centrului Național pentru Protecția Datelor cu Caracter Personal (în continuare - *Centrul*).

(7) Personalul UIP poartă răspundere conform actelor normative privind protecția datelor cu caracter personal pentru încălcarea cadrului normativ cu privire la prelucrarea datelor PNR.

Articolul 6. Asigurarea condițiilor adecvate de muncă ale responsabilului cu protecția datelor

(1) IGPF asigură responsabilul cu protecția datelor cu resurse necesare pentru executarea sarcinilor menționate la art. 7.

(2) Pentru executarea eficientă a sarcinilor și perfecționarea cunoștințelor de specialitate, responsabilul cu protecția datelor, cel puțin o dată la 6 luni este instruit prin participare la cursuri de specialitate la nivel național și internațional.

Articolul 7. Sarcinile responsabilului de protecția datelor în cadrul UIP

(1) Responsabilul cu protecția datelor are următoarele sarcini:

a) informarea și consilierea angajaților UIP care se ocupă de prelucrarea datelor PNR cu privire la obligațiile care le revin în temeiul cadrului normativ privind protecția datelor cu caracter personal;

b) monitorizarea respectării de către personalul UIP a prevederilor cadrului normativ cu privire la protecția datelor cu caracter personal, inclusiv privind acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare și auditurile aferente;

c) oferirea consilierii la cerere privind evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia;

d) realizarea verificărilor necesare în scopul determinării nivelului de respectare a rigorilor impuse de cadrul normativ privind protecția datelor cu caracter personal;

e) cooperarea cu Centrul și asumarea rolului de punct de contact cu această autoritate publică autonomă;

f) îndeplinirea funcției de punct unic de contact în relația cu subiecții de date, cu privire la toate aspectele legate de prelucrarea datelor cu caracter personal în cadrul registrului cu numele pasagerilor.

(2) Responsabilul de protecția datelor informează conducerea IGPF, în termen de până la 72 de ore de la data la care a luat cunoștință de aceasta, atunci când în exercitarea sarcinilor prevăzute la alin. (1) lit. b) și d) constată efectuarea unei operațiuni de prelucrare a datelor cu caracter personal în cadrul registrului cu numele pasagerilor care nu este conformă cu cadrul normativ privind protecția datelor cu caracter personal. Dacă în rezultatul informării nu s-au luat măsurile de rigoare, responsabilul de protecția datelor informează, imediat, Centrul.

Secțiunea III **Evaluarea datelor despre călători**

Articolul 8. Scopul utilizării datelor despre călători

Datele PNR cuprinse în registrul cu numele pasagerilor colectate în conformitate cu prezenta lege se utilizează exclusiv pentru următoarele scopuri:

a) prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor cu caracter terorist și a infracțiunilor transnaționale;

b) prevenirea și contracararea amenințărilor la adresa securității statului prevăzute la art. 4 din Legea securității statului nr. 618/1995.

Articolul 9. Registrul cu numele pasagerilor

(1) Modalitatea de ținere a registrului cu numele pasagerilor și de interacțiune a acestuia cu alte sisteme și resurse informaționale de stat se aprobă de către Guvern în conformitate cu cadrul normativ care reglementează domeniul tehnologiei informației și comunicațiilor și prezenta lege.

(2) Sistemele și resursele informaționale cu care registrul cu numele pasagerilor realizează schimbul de date pentru efectuarea evaluărilor sunt stabilite de Guvern.

Articolul 10. Prelucrarea datelor PNR

(1) UIP prelucrează datele despre călători pentru realizarea scopurilor menționate la art. 8 prin:

a) efectuarea unei evaluări a călătorilor înainte de sosirea sau de plecarea programată a acestora în/din Republica Moldova, în vederea identificării persoanelor în privința cărora este necesară o examinare suplimentară de către autoritățile competente și, după caz, de către Europol, având în vedere faptul că respectivele persoane pot fi implicate într-o infracțiune cu caracter terorist, a unei infracțiuni transnaționale sau într-o activitate care constituie amenințare la adresa securității statului;

b) oferirea de răspunsuri, numai în cazul unei cereri temeinic justificate, în temeiul actelor normative, din partea autorităților competente prevăzute la art. 13,

după caz Europol vizând furnizarea și prelucrarea datelor PNR, în cazuri concrete, în scopurile prevăzute la art. 8, și comunicarea rezultatelor acestei prelucrări;

c) analizarea datelor PNR în vederea actualizării sau a definirii de noi criterii ce urmează a fi utilizate pentru evaluările efectuate în temeiul alin. (2) lit. b) în scopul identificării oricăror persoane care pot fi implicate în săvârșirea unei infracțiuni cu caracter terorist, a unei infracțiuni transnaționale sau într-o activitate care constituie amenințare la adresa securității statului.

(2) În momentul efectuării evaluării menționate la alin. (1) lit. a), UIP este în drept:

a) să contrapună datele PNR cu cele din alte resurse informaționale, în scopurile prevăzute la art. 8, inclusiv resurse informaționale privind persoane sau obiecte căutate sau care fac obiectul unei alerte, în conformitate cu normele internaționale și naționale aplicabile unor astfel de resurse informaționale;

b) să prelucreze datele PNR în conformitate cu criterii prestabilite de prezenta lege.

Articolul 11. Criteriile prestabilite

(1) Orice evaluare a călătorilor înainte de sosirea sau plecarea programată, efectuată în temeiul art. 10 alin. (2) lit. b) pe baza unor criterii prestabilite, se realizează în mod nediscriminatoriu.

(2) Criteriile prestabilite se stabilesc și se revizuiesc periodic, de către UIP în cooperare cu autoritățile competente, respectând următoarele condiții:

a) criteriile sunt țintite, proporționale și specifice, raportat la infracțiunile unde potențiala implicare a persoanei poate fi determinată conform criteriilor sau scopurilor prevăzute la art. 8;

b) criteriile prestabilite nu se întemeiază pe rasă sau originea etnică a unei persoane, opiniile sale politice, religia sau convingerile sale filozofice, apartenența la sindicat, starea de sănătate, viața sexuală sau orientarea sexuală.

Articolul 12. Rezultatele pozitive

(1) Toate rezultatele pozitive obținute printr-o prelucrare automatizată a datelor PNR realizată în temeiul art. 10 alin. (1) lit. a) sunt reexamine individual prin mijloace neautomatizate, exclusiv de către personalul UIP, pentru a verifica dacă este necesar transferul respectivelor date PNR către autoritățile competente pentru realizarea unei examinări suplimentare în scopurile prevăzute la art. 8 și pentru a determina căror autorități competente să le fie transmise datele PNR, în funcție de atribuțiile stabilite în sarcina acestora conform actelor normative.

(2) UIP transferă către autoritățile competente datele PNR sau rezultatul pozitiv al prelucrării datelor PNR în situațiile în care constată că este necesară realizarea unei examinări suplimentare în oricare dintre scopurile prevăzute la art. 8. Este interzisă transmiterea către autoritățile competente de date PNR care nu au fost reexamine individual de personalul UIP prin mijloace neautomatizate.

(3) IGPF încheie acorduri de cooperare sau schimb informațional cu fiecare dintre autoritățile competente pentru stabilirea procedurii aferente transferului prevăzut la alin. (2).

Secțiunea IV

Autorități competente

Articolul 13. Autoritățile competente

(1) Autoritățile competente care au dreptul să solicite sau să primească de la UIP date sau rezultatul prelucrării datelor PNR, pentru a utiliza ulterior datele recepționate sau de a lua măsurile necesare în scopurile prevăzute la art. 8, sunt următoarele:

1) Ministerul Afacerilor Interne prin:

- a) Inspectoratul General al Poliției de Frontieră;
- b) Inspectoratul General al Poliției;
- c) Serviciul Protecție Internă și Anticorupție;
- 2) Serviciul de Informații și Securitate;
- 3) Serviciul Vamal;
- 4) Serviciul Prevenirea și Combaterea Spălării Banilor;
- 5) Centrul Național Anticorupție;
- 6) Procuratura.

(2) Conducătorii autorităților competente prevăzute la alin. (1) stabilesc prin acte administrative normative comune cu grad de secretizare:

a) subdiviziunile structurale din cadrul fiecărei autorități competente abilitate să solicite, să primească și să prelucreze date PNR corespunzător scopurilor indicate în art. 8;

b) persoanele abilitate de a solicita, primi și prelucra datele sau rezultatul pozitiv prelucrării datelor despre călători pentru îndeplinirea atribuțiilor funcționale;

c) limitele concrete în exercitarea atribuțiilor funcționale de prelucrare a datelor PNR de către persoanele stabilite potrivit lit. b).

(3) Pentru stabilirea limitelor concrete în exercitarea atribuțiilor de prelucrare a datelor PNR potrivit alin. (2) lit. c), conducătorii autorităților competente prevăzute la alin. (1) au în vedere următoarele:

a) prelucrarea datelor PNR să fie necesară pentru îndeplinirea competențelor instituționale;

b) datele PNR să fie prelucrate potrivit procedurilor și prin mijloacele prevăzute de dispozițiile legale aplicabile activităților în cadrul cărora sunt utilizate datele respective;

c) prelucrarea datelor PNR să respecte actele normative privind protecția datelor cu caracter personal.

Articolul 14. Utilizarea datelor PNR de către autoritățile competente

(1) Autoritățile competente utilizează în cadrul activităților proprii datele PNR și rezultatele prelucrării datelor PNR primite de la UIP, exclusiv în vederea analizării suplimentare a acestora pentru a stabili dacă este necesară sau nu dispunerea unor măsuri în oricare dintre scopurile prevăzute la art. 8.

(2) La nivelul autorităților competente, datele PNR se prelucrează exclusiv de către persoanele desemnate potrivit art. 13 alin. (2).

Secțiunea V

Păstrarea datelor PNR și depersonalizarea

Articolul 15. Perioada de păstrare a datelor

(1) Datele PNR transmise de transportatorii aerieni sunt păstrate în cadrul registrului cu numele pasagerilor pentru o perioadă de 5 ani de la momentul finalizării transmiterii active a respectivelor date PNR din sistemele transportatorilor aerieni în registrul cu numele pasagerilor, care reprezintă momentul furnizării.

(2) La expirarea termenului de 6 luni din momentul furnizării datelor PNR de către transportatorii aerieni, acestea sunt depersonalizate prin mascarea următoarelor elemente de date:

- a) numele, inclusiv numele altor călători, precum și numărul pasagerilor care călătoresc împreună;
- b) adresa și informațiile de contact asociate rezervării;
- c) toate informațiile privind forma de plată, inclusiv adresa de facturare, în măsură în care acestea conțin informații care ar putea servi la identificarea directă a călătorului la care se referă PNR sau a oricăror altor persoane;
- d) informațiile din profilul „client fidel” („frequent flyer”);
- e) mențiunile cu caracter general, prevăzute în anexa nr. 1, în măsura în care acestea conțin informații care ar putea servi la identificarea directă a călătorului;
- f) date API colectate.

(3) La expirarea termenului prevăzut la alin. (1), datele se distrug prin procedură ireversibilă, în mod automatizat, în ordinea în care au fost înregistrate.

(4) Dispozițiile alin. (3) nu se aplică în cazurile de transfer unei autorități competente, utilizate în contextul scopurilor prevăzute la art. 8. Păstrarea datelor PNR de către autoritățile competente respectă regimul juridic aplicabil cazului concret în care au fost prelucrate.

(5) Rezultatul prelucrării efectuate potrivit art. 10 alin. (1) lit. a) se păstrează de către UIP numai pentru perioada necesară transferului acestora către autoritățile competente potrivit art. 12 alin. (2) sau către UIP ale altor state potrivit art. 18 alin. (2).

(6) În cazul în care rezultatul unei prelucrări automatizate s-a dovedit negativ, după o reexaminare individuală prin mijloace neautomatizate în conformitate cu art. 12 alin. (1), acesta poate fi stocat pentru a se evita viitoare

răspunsuri pozitive „false” pe durata în care datele de bază nu sunt șterse în temeiul alin. (3).

Articolul 16. Dezvăluirea datelor

După expirarea termenului prevăzut la art. 15 alin. (2), dezvăluirea datelor complete PNR este permisă numai în cazul în care:

- a) se consideră în mod rezonabil că este necesară în scopul menționat la art. 10 alin. (1) lit. b);
- b) dezvăluirea este aprobată de instanța de judecată (judecător de instrucție).

Articolul 17. Obligațiile transportatorilor aerieni de a transmite datele despre călători

(1) Transportatorul aerian transmite gratuit către UIP, datele PNR stabilite în Anexa nr. 1 pentru fiecare călător și pentru fiecare zbor, în măsura în care aceștia colectează deja aceste date.

(2) În cazul zborului al cărui cod este partajat de unul sau mai mulți transportatori aerieni, obligația de a transmite datele PNR ale tuturor călătorilor aparține transportatorului aerian care operează zborul.

(3) Datele PNR sunt transmise pentru fiecare călător pentru operațiunile de transport aerian comercial, pe rute regulate și neregulate, precum și pentru operațiunile necomerciale (aviație generală) pentru aeronavele care:

- a) decolează de pe teritoriul Republicii Moldova și aterizează în alt stat;
- b) decolează din alt stat și aterizează pe teritoriul Republicii Moldova ca punct de tranzit sau ca destinație finală.

(4) Transportatorii aerieni au obligația de a transmite datele PNR către UIP:

a) cu 48 ore până la 24 ore înainte de ora programată pentru plecarea fiecărui zbor;

b) date API despre călători, imediat după închiderea zborului, adică imediat după îmbarcarea călătorilor în aeronava care se pregătește de decolare și când nici un călător nu se mai poate îmbarca sau nu mai poate debarca, transportatorii aerieni transmit către UIP toate modificările sau completările intervenite cu privire la datele PNR aferente respectivului zbor de la momentul transmiterii realizate potrivit lit. a);

c) dacă nu sunt date PNR disponibile a pasagerilor conform lit. a), va transmite date cu 2 ore înainte de ora programată pentru zbor, dacă deține astfel de date la acel timp.

(5) Datele menționate la alin. (3) sunt transmise aferent pentru întreaga listă a fiecărui zbor.

(6) La solicitarea UIP, exclusiv ca urmare a unei cereri din partea unei autorități competente, transportatorii aerieni vor furniza date despre călători în alți timpi decât cei indicați la alin. (4). UIP poate solicita astfel de date doar dacă este strict necesar pentru a răspunde unei amenințări specifice și concrete privind

comiterea unei infracțiuni cu caracter terorist, a unei infracțiuni transnaționale ori pentru prevenirea și contracararea amenințărilor la adresa securității statului.

(7) UIP nu dispune de drept de acces direct la sistemele de rezervare și control al plecărilor ale transportatorilor aerieni.

(8) Transportatorii aerieni transmit datele PNR către UIP, exclusiv prin metoda push, prin mijloace electronice de comunicare capabile să asigure protecția datelor PNR prin măsuri tehnice de securitate și prin măsuri organizatorice aplicate transmiterii datelor PNR sau, în caz de defecțiune tehnică, prin orice alte mijloace de comunicație care asigură același nivel de protecție a datelor PNR, precum și respectarea dispozițiilor legale privind protecția datelor cu caracter personal aplicabile.

(9) Transportatorii aerieni transmit datele PNR către UIP în unul din formatele și protocoalele de date stabilite de Guvern.

(10) Atunci când transmit datele PNR către UIP, transportatorii aerieni sunt obligați:

a) să notifice UIP protocolul comun și formatul de date compatibil, dintre cele cuprinse în lista aprobată de Guvern, pe care urmează să le utilizeze pentru transmiterea datelor PNR;

b) să utilizeze metode securizate, conforme cu protocolul comun notificat potrivit lit. a), pentru transmiterea datelor PNR către UIP prin mijloace electronice de comunicație;

c) să utilizeze formatul de date compatibil notificat potrivit lit. a) pentru transmiterea datelor PNR către UIP. Dacă transportatorii aerieni colectează date indicate la pct. 19 din Anexa nr. 1 (date API), aceștia le transferă indiferent dacă păstrează datele API prin alte mijloace tehnice decât pentru alte date PNR.

(11) Prin derogare de la alin. (9) și (10), transportatorii aerieni care nu dispun de infrastructura necesară pentru a putea folosi formatele și protocoalele de transmitere a datelor stabilite de Guvern, transmit datele PNR prin mijloace electronice care oferă garanții suficiente privind respectarea măsurilor de securitate tehnică și convenite la nivel bilateral, între transportatorul aerian și autoritățile competente din Republica Moldova în sensul prezentei legi.

Capitolul III

FLUXURI TRANSFRONTALIERE DE DATE PNR

Articolul 18. Schimbul de date PNR cu state membre UE prin intermediul UIP

(1) UIP reprezintă punctul național de contact cu unitățile de informații privind pasagerii ale altor state, inclusiv state membre ale Uniunii Europene (în continuare – UE) și este responsabilă pentru schimbul de date PNR cu acestea, potrivit prevederilor prezentei legi.

(2) În cazul în care prelucrarea datelor PNR potrivit art. 10 alin. (1) conduce la identificarea unor persoane, UIP transmite toate datele PNR relevante

și necesare sau rezultatul prelucrării respectivelor date PNR către UIP ale celorlalte state, cu excepția situațiilor care privesc securitatea statului.

(3) În cazul în care primește de la UIP din state membre ale UE date PNR sau rezultatul prelucrării datelor PNR, UIP le transmite către autoritățile competente. Art. 12 alin. (2) se aplică în mod corespunzător.

(4) UIP poate solicita, în condițiile alin. (5), din proprie inițiativă sau la cerere temeinic justificată a unei autorități competente, UIP a unui stat membru al UE să îi comunice datele PNR care nu au fost depersonalizate prin mascarea elementelor de date, precum și, dacă este necesar, rezultatele prelucrării respectivelor date PNR.

(5) Solicitarea prevăzută la alin. (4) trebuie să fie motivată corespunzător și să indice elementele de date sau o combinație a elementelor de date necesare într-un caz concret de prevenire, depistare, investigare și urmărire penală a infracțiunilor cu caracter terorist sau a infracțiunilor transnaționale.

(6) În cazul în care primește, din partea UIP a unui stat membru UE, o solicitare motivată corespunzător și care indică elementele de date sau o combinație a elementelor de date necesare într-un caz concret de prevenire, depistare, investigare și urmărire penală a infracțiunilor cu caracter terorist sau a infracțiunilor transnaționale, UIP transmite datele PNR și rezultatul prelucrării datelor PNR, dacă acest rezultat există și a fost solicitat, necesare în respectivul caz concret.

(7) UIP transmite răspunsul la solicitările prevăzute la alin. (6) în cel mai scurt timp posibil, dar nu mai târziu de 72 de ore. În cazul în care datele solicitate au fost depersonalizate prin mascarea elementelor de date, UIP comunică datele PNR complete numai dacă sunt prezentate indicii rezonabile că acest lucru este necesar în scopul realizării prelucrării prevăzute la art. 10 alin. (1) lit. b) și numai dacă utilizarea respectivelor date PNR este aprobată potrivit art. 16 lit. b).

(8) Prevederile alin. (6) și (7) se aplică și în cazul în care UIP primește o solicitare direct din partea unei autorități competente a unui stat membru al UE, dacă solicitarea cuprinde mențiuni din care să rezulte că datele PNR sunt necesare într-un caz urgent. Solicitățile din partea autorităților competente trebuie să fie motivate. O copie a solicitării se trimite întotdeauna UIP a statului membru UE solicitant. În toate celelalte cazuri, autoritățile competente își transmit solicitările prin UIP din propriul stat membru UE.

(9) Cu titlu excepțional, în cazul în care accesul la datele PNR este necesar pentru a răspunde unei amenințări concrete privind comiterea unei infracțiuni cu caracter terorist sau a unei infracțiuni transnaționale, UIP poate solicita UIP a unui stat membru UE să obțină datele PNR aferente unui zbor, conform art. 17 alin. (6) într-un anumit moment expres indicat și să le comunice UIP.

(10) În cazul în care primește, de la UIP a unui stat membru UE, o solicitare din care rezultă, cu titlu excepțional, că este necesar accesul la datele PNR aferente unui anumit zbor în alte momente decât cele prevăzute la art. 17

alin. (4), UIP aplică în mod corespunzător dispozițiile art. 17 alin. (6) și transmite UIP a unui stat membru UE solicitant datele PNR imediat după obținerea acestora de la transportatorul aerian.

Articolul 19. Solicitarea de date PNR de la UIP ale statelor membre UE de către autoritățile competente

(1) Dacă datele PNR sunt necesare într-un caz urgent, autoritățile competente prevăzute la art. 13 pot transmite direct UIP a unui stat membru UE o solicitare motivată corespunzător, care să indice elementele de date sau o combinație a elementelor de date necesare într-un caz concret de prevenire, depistare, investigare și urmărire penală a infracțiunilor cu caracter terorist sau a infracțiunilor transnaționale.

(2) Atunci când transmit o solicitare potrivit alin. (1), autoritățile competente transmit o copie a acesteia către UIP.

Articolul 20. Canale de cooperare cu statele membre UE

(1) Schimbul de date PNR cu state membre ale UE se poate realiza prin intermediul oricărui canal de cooperare existent între autoritățile competente ale statelor membre ale UE, corespunzător prevederilor art. 21. Limba folosită în solicitare și în schimbul de informații este cea aplicabilă canalului utilizat.

(2) Atunci când se transmit notificări potrivit art. 34, acestea conțin și informații cu privire la coordonatele punctelor de contact cărora le pot fi adresate solicitări în caz de urgență.

Articolul 21. Schimbul de date PNR cu Europol

(1) UIP are dreptul, în baza unei cereri temeinic justificate din partea Europol, de a furniza datele sau rezultatul prelucrării datelor PNR, pentru prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor cu caracter terorist sau a infracțiunilor transnaționale către Europol, prin intermediul Centrului de Cooperare Polițienească Internațională din cadrul Inspectoratului General al Poliției. Art. 16 se aplică în mod corespunzător.

(2) De la caz la caz, Europol poate adresa UIP, prin intermediul Centrului de Cooperare Polițienească Internațională al Inspectoratului General al Poliției, o cerere în format electronic și justificată corespunzător de transmitere a unor anumite date PNR sau a rezultatului prelucrării respectivelor date.

(3) Europol poate adresa o cerere potrivit alin. (2) atunci când acest lucru este strict necesar pentru sprijinirea și consolidarea acțiunii statelor membre ale UE în vederea prevenirii, depistării sau investigării unei anumite infracțiuni cu caracter terorist sau a unei anumite infracțiuni transnaționale, în măsura în care infracțiunea respectivă intră în sfera de competență a Europol, în temeiul legislației UE care stabilește organizarea și atribuțiile Europol.

(4) Cererea prevăzută la alin. (2) trebuie să conțină motive rezonabile pe baza cărora Europol consideră că transmiterea datelor PNR sau a rezultatului

prelucrării datelor PNR va contribui în mod substanțial la prevenirea, depistarea sau investigarea infracțiunii în cauză.

(5) Schimbul de informații în temeiul prezentului articol are loc prin intermediul aplicației de rețea pentru schimbul securizat de informații, în conformitate cu legislația UE ce stabilește organizarea și atribuțiile Europol.

Articolul 22. Schimbul de date PNR cu țări non-membre UE

(1) Datele despre călători sau rezultatul prelucrării datelor despre călători pot fi transmise către alte țări, cu autorizarea judecătorului de instrucție, dacă sunt îndeplinite cumulativ următoarele condiții:

- a) țările asigură un nivel de protecție adecvat;
- b) datele sau rezultatul prelucrării datelor sunt necesare pentru prevenirea, depistarea sau investigarea unei fapte care este considerată de legea țării terțe solicitante drept infracțiune de terorism sau care este sancționată ca infracțiune de legea țării terțe solicitante cu o pedeapsă privativă de libertate a cărei durată maximă este de cel puțin 3 ani și care este corespunzătoare uneia din formele de criminalitate prevăzute în anexa nr. 2;
- c) țara comunică în scris că acceptă să nu transmită datele sau rezultatul prelucrării datelor despre călători către alt stat doar dacă acest lucru este strict necesar în scopurile prevăzute la alin. (2);
- d) țara anunță imediat, dar nu mai târziu de 72 ore despre transmiterea datelor sau rezultatul prelucrării datelor despre călători către un alt stat în cazul când datele transmise sunt necesare pentru prevenirea unui atac terorist sau o amenințare reală la viața unei persoane;
- e) sunt îndeplinite condițiile prevăzute la art. 18 alin. (5)-(7), care se aplică în mod corespunzător;
- f) nu este afectată securitatea statului.

(2) Transferul de date PNR fără consimțământul prealabil al statului membru UE de la care sunt obținute datele este permis în circumstanțe excepționale și numai dacă:

- a) astfel de transferuri sunt esențiale pentru a răspunde unei amenințări specifice și reale, având legătura cu infracțiuni cu caracter terorist sau cu infracțiuni transnaționale, la adresa unui stat membru sau a unei țări; și
- b) consimțământul prealabil nu poate fi obținut în timp util.

(3) Datele PNR sunt transferate numai în condiții conforme cu prezenta lege și numai după ce se asigură că destinatarii intenționează să utilizeze datele PNR în conformitate cu condițiile și garanțiile prevăzute de prezenta lege.

(4) Responsabilul cu protecția datelor este informat de fiecare dată cu privire la transferul de date PNR conform prezentului articol.

(5) UIP are dreptul de a solicita și de a primi din partea unei țări sau organizație internațională date PNR sau rezultatul oricărei prelucrări a datelor PNR, în cazul în care acest transfer este necesar pentru oricare dintre scopurile

prevăzute la art. 8, în baza tratatelor internaționale încheiate în acest sens de către Republica Moldova.

Capitolul IV PROTECȚIA DATELOR

Articolul 23. Desemnarea operatorului

(1) Inspectoratul General al Poliției de Frontieră se desemnează în calitate de operator al registrului cu numele pasagerilor în sensul actelor normative privind protecția datelor cu caracter personal.

(2) Personalul UIP au calitate de utilizatori ai registrului cu numele pasagerilor. Procesul de definire a drepturilor de acces în calitate de utilizatori este guvernat de principiul necesității de a cunoaște.

Articolul 24. Drepturile subiectului datelor cu caracter personal

(1) Drepturile subiectului datelor cu caracter personal în contextul prelucrării datelor cu caracter personal în cadrul registrului cu numele pasagerilor se exercită potrivit actelor normative privind protecția datelor cu caracter personal și Codului administrativ al Republicii Moldova nr.116/2018.

(2) Cererile formulate în exercitarea drepturilor subiectului de date se adresează UIP. Cererea se examinează dacă conține cumulativ următoarele elemente:

- a) numele și prenumele;
- b) ziua, luna, anul nașterii;
- c) cetățenia sau apartenența etnică,
- d) domiciliul și/sau reședința temporară;
- e) adresa de poștă sau adresa de poștă electronică dacă se solicită răspuns pe această cale;
- f) obiectul cererii și motivarea acesteia;
- g) semnătura subiectului de date cu caracter personal ori a reprezentantului său legal sau împuternicit, desemnat prin procură a cărui semnătură se legalizează de notar sau de alte persoane abilitate prin lege cu astfel de funcție sau creată în cadrul Registrului împuternicirilor de reprezentare în baza semnăturii electronice.

(3) Pentru a comunica subiectului de date informații cu privire la datele cu caracter personal prelucrate în cadrul registrului cu numele pasagerilor, în situația prelucrărilor prevăzute la art. 18-22, UIP solicită, după caz, acordul autorităților competente către care au fost transferate datele, acordul Europol, acordul entității publice din străinătate responsabilă de colectarea, prelucrarea și utilizarea datelor PNR care a furnizat datele.

(4) Autoritățile competente comunică opțiunea în termen de 30 de zile de la data primirii solicitării din partea UIP.

(5) În cazul în care entitatea publică din străinătate consultată potrivit alin. (3) nu comunică un răspuns, în vederea respectării termenilor de răspuns conform legislației, la cererile subiecților de date, UIP răspunde solicitantului fără indicarea provenienței datelor.

(6) În situația în care o entitate publică din străinătate stipulată în alin. (3) solicită UIP, în urma transmiterii unor date PNR, acordul pentru comunicarea unor informații solicitate de subiectul de date, UIP comunică acordul în termen de 30 de zile de la primirea solicitării sau, după caz, în termenul indicat de entitatea publică solicitantă. Dacă datele au fost transferate unei autorități competente, înainte de a transmite răspunsul către entitatea publică din străinătate stipulată în alin. (3), Unitatea consultă respectiva autoritate competentă indicând și eventualul termen precizat de entitatea publică solicitantă cu respectarea legislației în domeniu.

Articolul 25. Securitatea și confidențialitatea datelor cu caracter personal

(1) Asigurarea securității și confidențialității datelor cu caracter personal în cadrul registrului cu numele pasagerilor se realizează potrivit actelor normative privind protecția datelor cu caracter personal.

(2) Este interzisă prelucrarea datelor PNR prin intermediul persoanelor împuternicite de către operator, în sensul actelor normative privind protecția datelor cu caracter personal.

(3) Operatorul prevăzut la art. 23 alin. (1) are obligația de a implementa măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel ridicat de securitate a datelor cu caracter personal prelucrate în cadrul registrului cu numele pasagerilor, ținând seama de riscurile asociate prelucrării datelor PNR și de natura respectivelor date.

Articolul 26. Interzicerea prelucrării unor categorii speciale de date cu caracter personal

(1) Prelucrarea datelor PNR după criterii legate de categoriile de informații care dezvăluie originea rasială sau etnică, opiniile politice, religia sau convingerile filozofice, apartenența la un sindicat, sănătatea, viața sexuală sau orientarea sexuală a unei persoane este interzisă.

(2) În cazul în care UIP primește categorii de date de la transportatorii aerieni prevăzute la alin. (1), aceste set de date este șters.

Articolul 27. Evidențele activităților de prelucrare

(1) UIP păstrează o evidență a tuturor categoriilor de activitate de prelucrare a datelor PNR aflate în responsabilitatea sa. Această evidență cuprinde următoarele informații:

a) numele și datele de contact ale entității publice și ale personalului care are sarcina de a prelucra datele PNR și diferitele niveluri de autorizare a accesului;

b) cererile depuse de autoritățile competente și UIP ale altor state;

c) cererile de date PNR și transferurile de asemenea date către o altă țară.

(2) Evidența prevăzută la alin. (1) se pune la dispoziția Centrului, la cererea acestuia conform actelor normative.

Articolul 28. Trasabilitatea prelucrărilor

(1) Registrul cu numele pasagerilor asigură trasabilitatea prelucrărilor efectuate la nivelul UIP, astfel încât să fie posibilă identificarea personalului care a realizat activitățile de prelucrare și identificarea autorității competente care a avut acces la datele PNR și la rezultatele prelucrărilor realizate de către UIP.

(2) Registrul cu numele pasagerilor asigură cel puțin trasabilitatea operațiunilor de prelucrare a datelor cu caracter personal conform cadrului normativ prin protecția datelor.

(3) Fișierul de trasabilitate generat de PNR trebuie să conțină cel puțin următoarele informații:

a) scopul prelucrării;

b) data și ora operațiunilor de prelucrare;

c) utilizatorul;

d) destinatarul datelor PNR, atunci când este cazul;

e) datele accesate și categoria de operațiune efectuată asupra datelor potrivit actelor normative privind protecția datelor cu caracter personal.

(4) Fișierele de trasabilitate generate de registrul cu numele pasagerilor pot fi accesate doar pentru următoarele scopuri:

a) verificarea și monitorizarea legalității efectuării prelucrărilor;

b) asigurarea funcționării tehnice corespunzătoare a registrului cu numele pasagerilor;

c) asigurarea integrității și securității datelor PNR.

(5) Utilizarea fișierelor de trasabilitate generate de către registrul cu numele pasagerilor în alte scopuri decât cele prevăzute la alin. (4) este interzisă.

(6) Fișierele de trasabilitate generate de către registrul cu numele pasagerilor se păstrează pentru o perioadă de 5 ani și se pun la dispoziția Centrului, la cererea acestuia.

Articolul 29. Verificarea calității datelor PNR transferate

(1) În situația în care au fost transferate în condițiile prezentei legi date incorecte sau neactualizate, UIP are obligația de a informa destinatarii respectivelor date asupra neconformității acestora, cu menționarea datelor care au fost modificate sau, dacă este cazul, cu precizarea că datele transmise trebuie rectificate, șterse ori restricționate la prelucrare.

(2) În situația în care se constată că au fost transferate date PNR cu nerespectarea condițiilor impuse de prezenta lege, UIP are obligația de a-i informa pe destinatarii acestor date, cu precizarea că datele transmise trebuie șterse imediat.

(3) În situația în care se constată că UIP a primit date PNR incorecte ori neactualizate, acestea nu pot fi utilizate și datele se rectifică sau după caz, se șterg și nu pot fi utilizate. Dacă transferul a fost realizat în mod eronat ori cu nerespectarea condițiilor impuse de prezenta lege, datele se șterg sau, după caz, se blochează imediat. Entitatea publică care a transmis datele este informată cu privire la măsura adoptată și la motivul adoptării acesteia.

Articolul 30. Notificarea Centrului Național pentru Protecția Datelor cu Caracter Personal în cazul încălcării securității datelor

(1) UIP notifică Centrul imediat, dar nu mai târziu de 72 de ore de la constatare, încălcarea securității datelor cu caracter personal din cadrul registrului cu numele pasagerilor, cu excepția cazului în care încălcarea securității datelor nu este susceptibilă să genereze un risc la adresa drepturilor și libertăților persoanelor fizice.

(2) Notificarea prevăzută la alin. (1) trebuie să conțină cel puțin următoarele informații:

a) o descriere a caracterului încălcării securității datelor cu caracter personal prelucrate în cadrul registrului cu numele pasagerilor, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ de subiecți de date în cauză, precum și categoriile și numărul aproximativ de înregistrări de date cu caracter personal în cauză;

b) numele și datele de contact ale responsabilului cu protecția datelor în cadrul UIP sau alt punct de contact de unde se pot obține mai multe informații;

c) consecințele probabile ale încălcării securității datelor cu caracter personal;

d) măsurile luate sau propuse de operator pentru a remedia încălcarea securității datelor cu caracter personal, inclusiv, dacă este cazul, măsuri pentru a atenua eventualele efecte adverse ale acesteia.

(3) UIP ține evidența tuturor cazurilor de încălcare a securității datelor cu caracter personal, inclusiv o descriere a situației în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor acesteia și a măsurilor de remediere întreprinse.

(4) În cazul în care încălcarea securității datelor implică date cu caracter personal care au fost transmise de un operator dintr-un alt stat sau către un astfel de operator, informațiile prevăzute la alin. (3) se comunică imediat operatorului respectiv.

(5) În cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru protecția datelor cu caracter personal

sau la adresa drepturilor și libertăților persoanelor fizice, operatorul informează subiectul de date cu privire la încălcarea securității datelor cu caracter personal.

(6) Informarea subiectului de date, prevăzută la alin. (5), nu este necesară în cazul în care este îndeplinită oricare din următoarele condiții:

a) operatorul a pus în aplicare măsuri tehnice și organizatorice adecvate de protecție, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securității acestor date, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea;

b) operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat la adresa drepturilor și libertăților subiecților de date nu este susceptibil să se materializeze;

c) notificarea ar necesita un efort disproporționat;

d) contactarea subiectului de date nu este posibilă.

Articolul 31. Obligațiile transportatorilor aerieni privind protecția datelor cu caracter personal

(1) În cadrul activităților necesare pentru transmiterea datelor PNR către UIP, transportatorii aerieni rămân responsabili, în temeiul dispozițiilor legale din domeniul protecției datelor cu caracter personal aplicabile acestora, în ceea ce privește:

a) adoptarea măsurilor tehnice și organizatorice necesare pentru asigurarea protejării datelor PNR împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, precum și împotriva oricărei altei forme de prelucrare ilegală;

b) prelucrarea datelor PNR în mod legal, echitabil și transparent față de subiectul de date, inclusiv informarea călătorilor, prealabilă colectării datelor PNR, cu privire la faptul că acestea sunt transmise către UIP;

c) colectarea datelor PNR în scopuri determinate, explicate și legitime și abținerea de la prelucrarea ulterioară într-un mod incompatibil cu aceste scopuri;

d) colectarea de date PNR adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate;

e) prelucrarea de date PNR exacte și actualizate;

f) păstrarea datelor PNR într-o formă care permite identificarea subiecților de date pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate.

Articolul 32. Monitorizarea aplicării actului normativ

(1) Prelucrarea datelor cu caracter personal în cadrul registrului cu numele pasagerilor, inclusiv transferul acestor date în străinătate, este monitorizată și se supune controlului Centrului.

(2) Pentru realizarea monitorizării și controlului prevăzut la alin. (1), Centrul îndeplinește următoarele atribuții:

a) primește plângerile depuse de orice subiect de date, investighează aspectele semnalate și informează subiecții de date cu privire la evoluția și la soluționarea plângerilor lor;

b) verifică legalitatea prelucrării datelor cu caracter personal în cadrul registrului cu numele pasagerilor și desfășoară investigații în conformitate cu actele normative privind protecția datelor cu caracter personal;

c) verifică respectarea modului de punere în aplicare a prevederilor art. 5 alin. (3).

Articolul 33. Sancțiuni

(1) Încălcarea prevederilor prezentei legi atrage, după caz, răspunderea contravențională, dacă nu sunt săvârșite în astfel de condiții încât să constituie infracțiuni.

(2) Transportatorii aerieni nu sunt pasibili de sancțiuni, în cazul unor erori cauzate de ieșirea din funcțiune a registrului cu numele pasagerilor, care ar putea conduce la netransmiterea sau transmiterea eronată a datelor PNR către UIP, în cazul în care au informat imediat UIP despre defecțiunile tehnice și au luat măsurile corespunzătoare pentru înlăturarea acestora.

Capitolul V DISPOZIȚII FINALE

Articolul 34. Notificarea Comisiei Europene

În termen de 30 de zile lucrătoare de la data intrării în vigoare a prezentei legi, Ministerul Afacerilor Interne asigură transmiterea notificării scrise către Comisia Europeană privind înființarea UIP.

Articolul 35. Intrarea în vigoare și măsuri de implementare

(1) Prezenta lege intră în vigoare la expirarea a 12 luni de la data publicării în Monitorul Oficial al Republicii Moldova.

(2) Guvernul:

a) în termen de 6 luni de la data publicării, va prezenta propuneri Parlamentului privind aducerea în concordanță a actelor normative cu prezenta lege;

b) de la data publicării prezentei legi, va întreprinde măsurile necesare pentru reglementarea modului de organizare și funcționare a UIP, precum și va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi.

Președintele Parlamentului

**Datele și informațiile din registrul cu numele pasagerilor în măsura
în care au fost colectate de transportatorii aerieni**

1. Cod de reper al dosarului pasagerului/codul de rezervare.
2. Data rezervării/emiterii biletului.
3. Data/datele programată/programate a/ale călătoriei.
4. Numele, prenumele, numele la naștere și data nașterii ale pasagerului asociate rezervării, titlul/grad științific.
5. Alte informații cu privire la nume.
6. Adresa și informațiile de contact indicate în rezervare (număr de telefon, adresă de e-mail).
7. Toate informațiile privind forma de plată, inclusiv adresa de facturare (numerar, card de credit, numărul și data expirării cardului de credit, notificare de plată în avans (PTA), valuta, datele despre persoană/agenție care efectuează plata, codurile reducerilor de serviciu pentru personal).
8. Itinerarul complet de călătorie (îmbarcare inițială, escală, debarcare finală).
9. Informațiile din profilul „client fidel” („frequent flyer”).
10. Datele agenției sau agentul de turism (numele, adresa, detaliile de contact, codul IATA) prin care a fost făcută rezervarea sau a fost cumpărat biletul.
11. 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.
12. Informațiile scindate sau divizate din registrul cu numele pasagerilor.
13. Mențiunile cu caracter general, inclusiv toate informațiile disponibile despre minorii neînsoțiți cu vârsta sub 18 ani, precum numele și sexul minorului, vârsta, limba/limbile vorbită/vorbite, numele și datele de contact ale persoanei care îl însoțește la plecare și relația sa cu minorul, numele și datele de contact ale persoanei care îl așteaptă la sosire și relația sa cu minorul, agentul prezent la plecare și la sosire.
14. Informațiile despre bilet, inclusiv numărul biletului, data emiterii biletului și bilete dus simplu, câmpurile aferente furnizării automate a prețului unui bilet de călătorie.
15. Numărul locului și alte informații privind locul (locul solicitat și locul efectiv după închiderea zborului).
16. Informațiile cu privire la partajarea de coduri.
17. 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) combinate, codul

transportatorului bagajului, statutul bagajului, punctul de destinație/descărcare a bagajului.

18. Numărul pasagerilor înregistrați în PNR și alte nume ale acestora.

19. Date API colectate, tipul, numărul, țara sau denumirea organizației de emitere și data expirării oricărui document de călătorie, cetățenia, numele de familie, prenumele, sexul, data nașterii, compania aeriană, numărul zborului, data plecării și sosirii (data planificată de plecare și sosire a aeronavei în baza timpului local a plecării), aeroportul de plecare, aeroportul de tranzit, aeroportul de sosire, ora plecării și ora sosirii (în baza orelor locale de plecare și sosire).

20. Un istoric al tuturor modificărilor datelor PNR enumerate la punctele 1-19.

21. Numele persoanei care a făcut rezervarea.

22. Așteptarea locului (standby).

23. Toate informațiile despre înregistrarea pasagerului la ghișeu (check-in) – numărul de control la check-in, ID agentului de check-in, timpul check-in-ului, statutul check-in-lui, statutul de confirmare, numărul de îmbarcare, indicatorul de îmbarcare, ordinea check-in-ului.

24. Numărul total de persoane transportate în aeronavă.

Forme de criminalitate la care se referă articolul 2

1. Participarea la un grup infracțional organizat;
2. Traficul de ființe umane;
3. Exploatarea sexuală a copiilor și pornografia infantilă;
4. Traficul ilicit de droguri, stupefiante și substanțe psihotrope;
5. Traficul ilegal de arme, muniții și material explozibile;
6. Infracțiunile de corupție prevăzute la cap. XV și XVI din Codul penal al Republicii Moldova nr. 985/2002;
7. Frauda, inclusiv frauda care aduce atingere intereselor financiare ale Uniunii Europene;
8. Spălarea banilor sau a produselor infracțiunii și falsificarea de monedă, inclusiv falsificarea monedei euro;
9. Infracțiuni informatice și criminalitatea cibernetică;
10. Infracțiuni împotriva mediului, inclusiv traficul ilicit de specii de animale pe cale de dispariție și traficul ilicit de specii și soiuri de plante pe cale de dispariție;
11. Facilitarea intrării și șederii neautorizate;
12. Omorul și vătămarea corporală gravă;
13. Traficul ilicit de organe și țesuturi umane;
14. Răpirea, lipsirea de libertate în mod ilegal și luarea de ostatici;
15. Furtul organizat și tâlhăria prin folosirea unei arme;
16. Traficul ilicit de bunuri culturale, inclusiv antichități și opera de artă;
17. Contrafacerea și pirateria produselor;
18. Falsificarea de documente administrative și uzul de fals;
19. Traficul ilicit de substanțe hormonale și alți factori de creștere;
20. Traficul ilicit de materiale nucleare sau radioactive;
21. Violul;
22. Infracțiunile de competența Curții Penale Internaționale;
23. Sechestrarea ilicită a aeronavelor/navelor;
24. Sabotajul;
25. Traficul de autovehicule furate;
26. Spionajul industrial;
27. Infracțiuni contra autorităților publice și a securității de stat;
28. Contrabanda, contrabanda cu mărfuri accizate, eschivarea de la achitarea drepturilor de import.
29. Finanțarea terorismului.

Formele de criminalitate prevăzute la art. 2 și prezenta Anexă sunt evaluate de către autoritățile competente în conformitate cu legislația penală, precum și cu prevederile Legii nr. 116/2015 pentru ratificarea Acordului privind cooperarea operațională și strategică dintre Republica Moldova și Oficiul European de Poliție.

NOTĂ INFORMATIVĂ

la proiectul de hotărâre de Guvern pentru aprobarea proiectului de lege privind utilizarea datelor din registrul cu numele pasagerilor

1. Denumirea autorului și, după caz, a participanților la elaborarea proiectului
Proiectul a fost elaborat de către Ministerul Afacerilor Interne.
2. Condițiile ce au impus elaborarea proiectului de act normativ și finalitățile urmărite
<p>Luptătorii teroriști străini (în continuare - FTF) reprezintă o amenințare acută și în creștere la adresa păcii și securității internaționale. Activitățile lor pot crește intensitatea, durata, insolubilitatea și imprevizibilitatea conflictelor și reprezintă o amenințare gravă pentru statele lor de origine, statele pe care le tranzitează și statele în care călătoresc, precum și statele învecinate cu zonele de conflict armat din care acei luptători sunt activi. Imaginea Republicii Moldova va avea de suferit prin prisma cooperării cu diferite organizații internaționale de aplicare a legii în special în contextul oferirii unei centuri de securitate la hotarele Uniunii Europene.</p> <p>Prevenirea activităților teroriste și lupta cu criminalitatea sunt principalele elemente în utilizarea datelor din registrul cu numele pasagerilor (în continuare - PNR).</p> <p>Datele PNR reprezintă denumirea generică dată <i>înregistrărilor</i> create de operatori aerieni sau agenții de handling pentru fiecare călătorie <i>rezervată</i> de către sau în numele oricărui pasager. Datele sunt utilizate de operatori în propriile scopuri comerciale și operaționale în furnizarea de servicii de transport aerian.</p> <p>După 24 februarie 2022, schimbările geopolitice și consecințele războiului hibrid au un impact direct asupra securității și a vieții oricărui cetățean al Republicii Moldova. Astfel, pentru depășirea și prevenirea acestui fenomen, este imperioasă implementarea mecanismului de verificare a datelor PNR.</p> <p>Proiectul de lege <i>cu privire la utilizarea datelor din registrul cu numele pasagerilor</i> a fost elaborat în vederea executării prevederilor Rezoluțiilor Consiliului de Securitate al Organizației Națiunilor Unite (în continuate - CSONU) 2178/2014, 2396/2017 și 2482/2019, a standardelor și practicilor recomandate cu privire la facilități din Anexa nr. 9 (SARPs) a Convenției Organizației Aviației Civile Internaționale privind aviația civilă din 7 decembrie 1944 (în continuare - Convenția OACI), a orientărilor relevante, precum și pentru armonizarea legislației Republicii Moldova cu prevederile Directivei (UE) 2016/681 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave (în continuare – <i>Directiva PNR</i>).</p> <p>Totodată, implementarea utilizării datelor prealabile despre pasageri rezidă din angajamentele Republicii Moldova de participare la diferite organizații internaționale; precum și din Agenda de Asocieră dintre Uniunea Europeană și Republica Moldova pentru anii 2021-2027.¹</p> <p>În același context, proiectul legii a fost elaborat pentru <i>consolidarea asigurării securității interne, consolidarea capacităților cooperării internaționale și regionale în lupta contra terorismului, a criminalității organizate și a securității transfrontaliere, protejării vieții și siguranței și crearea unui cadru normativ pentru protecția datelor cu</i></p>

¹ <https://eur-lex.europa.eu/legal-content/RO/EXT/PDF/?uri=CELEX:22022D1997> pag. 16 (accesat 21.04.2023)

caracter personal în ceea ce privește datele pasagerilor și prelucrarea acestora de către autoritățile competente cu respectarea deplină a drepturilor omului și libertăților fundamentale proclamate, în special în Convenția europeană pentru apărarea drepturilor omului și libertăților fundamentale, încheiată la Roma la 4 noiembrie 1950, ratificată de Republica Moldova prin Hotărârea Parlamentului nr. 1298/1997 și protocoalele sale adiționale, Pactului internațional privind drepturile civile și politice, ratificat de Republica Moldova prin Hotărârea Parlamentului nr. 217/1990, în Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, a dreptului la viața privată și a principiului proporționalității.

Conform paragrafului 9 din Rezoluția CSONU 2178/2014, *se solicită ca statele membre să impună companiilor aeriene care operează pe teritoriile lor să furnizeze în prealabil autorităților naționale competente informații despre pasageri (date API)*. Or, aceasta decide că statele membre, în conformitate cu legislația internațională privind drepturile omului, dreptul internațional al refugiaților, precum și dreptul internațional umanitar, să prevină și să elimine recrutarea, organizarea, transportul sau dotarea persoanelor care călătoresc într-un alt stat decât statul lor de reședință sau decât statul a cărui cetățenie o au, în vederea săvârșirii, planificării, pregătirii sau participării la acte de terorism sau care asigură antrenament pentru săvârșirea actelor de terorism sau participă la acesta, precum și finanțarea călătoriei și a activităților acestor persoane.

Rezoluția CSONU 2396/2017 decide că, în conformitate cu paragraful 9 din rezoluția 2178 (2014) și standardul stabilit de OACI, statele sale membre stabilesc sisteme de informații prealabile despre pasageri (API), pentru a detecta intrarea, ieșirea sau tranzitul pe/de pe/prin teritoriile lor, cu ajutorul aeronavelor civile, a FTF. Or, aceasta decide că statele membre trebuie să dezvolte capacitatea de a colecta, procesa și analiza, în conformitate cu SARPs OACI, datele din registrul cu numele pasagerilor (PNR) și să se asigure că datele PNR sunt utilizate și partajate cu toate autoritățile lor naționale competente, cu respectarea drepturilor omului și a libertăților fundamentale în scopul prevenirii, detectării și investigării infracțiunilor de terorism și călătoriilor aferente.

Rezoluția CSONU 2482/2019 solicită ca statele membre să implementeze obligațiuni de a colecta și analiza date API și de a dezvolta capacități de a colecta, procesa și analiza date PNR, conform SARPs, de a le furniza autorităților competente pentru a face conexiuni între persoanele asociate cu criminalitatea organizată, națională sau transnațională, și cu teroriștii, de a stopa călătoriile teroriste și de a urmări penal terorismul și criminalitatea organizată națională sau transnațională.

Utilizarea datelor PNR din domeniul transporturilor aeriene va permite analiza acestor date, precum și rezultatele analizelor pentru a fi transmise ulterior autorităților competente din țară, din alte state, precum și Europol.

Informațiile prealabile referitoare la pasageri (API), care sunt datele biografice ale pasagerilor colectate de companiile aeriene în timpul înregistrării, sunt la fel de valoroase, inclusiv datorită complementarității acestora cu datele PNR.

Cifrele pentru argumentarea utilității datelor API și PNR sunt extrem de dificil de cuantificat deoarece spectrul de forme de criminalitate, 28 la număr conform anexei nr. 2 din proiectul de lege, poate fi foarte vast, de exemplu de la traficul de ființe umane și traficul ilegal de arme, până la cazuri de corupție și infracțiuni ce țin de competența Curții Penale Internaționale. În contextul războiului din Ucraina acest aspect este cât se

poate de actual și important pentru securitatea nu numai a Republicii Moldova, dar și pentru cea regională.

Fără îndoială, schimbările geopolitice și consecințele războiului de agresiune al Rusiei împotriva Ucrainei vor avea un *impact de durată asupra securității*, nu numai a Republicii Moldova, dar și a Uniunii Europene în anii următori de aceea este necesar de a avea capacitatea de a răspunde prompt și hotărât noilor provocări și de a contracara riscurile și amenințările la adresa statului.

În această ordine de idei, implementarea API și PNR va eficientiza realizarea măsurilor de asigurare a securității pe palierul antiterorist, în scopul detectării și/sau descurajării tentativelor de tranzitare sau intrare/ieșire pe/de pe teritoriul țării a persoanelor afiliate grupărilor și formațiunilor teroriste, suspectate de comitere a acțiunilor teroriste sau conexe acestora, precum și a celor indivizi, ce prezintă riscuri la adresa securității naționale.

În același context, implementarea API/PNR, în special prelucrarea datelor PNR a devenit un instrument de aplicare a legii larg utilizat, în cadrul Uniunii Europene și nu numai, pentru a preveni și combate terorismul și alte forme de criminalitate gravă, cum ar fi infracțiunile legate de droguri, traficul de persoane și exploatarea sexuală a copiilor. În Uniunea Europeană, în mai puțin de doi ani de la termenul limită de transpunere, Directiva PNR și-a dovedit deja necesitatea în efortul de a realiza o Uniune a Securității eficace și autentică, care să protejeze în mod corespunzător drepturile și libertățile cetățenilor.²

Evaluarea datelor PNR permite identificarea persoanelor *care nu erau suspectate* de implicare în infracțiuni de terorism sau în infracțiuni grave înainte de o astfel de evaluare, și care trebuie să facă obiectul unor cercetări suplimentare desfășurate de către autoritățile competente. Prin utilizarea datelor PNR se poate contracara amenințarea reprezentată de infracțiunile cu caracter terorist și de infracțiunile transnaționale grave dintr-o altă perspectivă decât prin prelucrarea altor categorii de date cu caracter personal. Subsecvent, asocierea dintre terorism și criminalitate se datorează și faptului că, finanțarea activităților teroriste este efectuată inclusiv și din activități criminale. Cu toate acestea, pentru a asigura faptul că prelucrarea datelor PNR rămâne limitată la ceea ce este necesar, definirea și aplicarea de criterii de evaluare ar trebui să fie limitate la infracțiuni cu caracter terorist, infracțiuni grave și amenințări la adresa securității statului pentru care este relevantă utilizarea unor astfel de criterii. Mai mult decât atât, criteriile de evaluare ar trebui definite într-un mod care să reducă la minimum numărul persoanelor nevinovate, identificate greșit prin intermediul acestui sistem.

Utilizarea eficientă a datelor despre pasageri poate contracara diferite amenințări reprezentate de infracțiuni cu caracter terorist și infracțiuni pentru care legea penală prevede în calitate de pedeapsă minimă pedeapsa cu închisoarea pe un termen de trei ani sau mai mult, precum și amenințări la adresa securității statului.

Prin proiect se urmărește îmbunătățirea și dezvoltarea mecanismului deja instituit prin art. 41 din Legea nr. 215/2011 cu privire la frontiera de stat a Republicii Moldova și art. 21 din Legea nr. 120/2017 cu privire la prevenirea și combaterea terorismului referitor la transmiterea datelor API și PNR.

² <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020SC0128>

Colectarea și utilizarea datelor API/PNR permite identificarea persoanelor de interes înainte de a ajunge la punctul de trecere a frontierei și luarea unor decizii cu privire la măsurile suplimentare care ar trebui aplicate înainte de sosirea acestora.

Beneficiul pentru cetățeni – minimizarea riscurilor ce țin de asigurarea securității antiteroriste și sporirea nivelului de siguranță.

Problematicile care se consideră a fi soluționate sunt:

- amenințări la pacea internațională și securitate cauzate de actele teroriste;
- efectele negative ale războiului din Ucraina pun accent pe securitatea națională a Republicii Moldova prin diferite activități necontrolate, ce necesită intervenții concrete în reziliența economică și socială, în statul de drept și anticorupție,
- eficientizarea realizării măsurilor de asigurare a securității pe palierul antiterorist;
- sporirea măsurilor de detectare și/sau descurajare a tentativelor de tranzitare sau intrare/ieșire pe/de pe teritoriul țării a persoanelor afiliate grupărilor și formațiunilor teroriste, suspectate de comitere a acțiunilor teroriste sau conexe acestora, precum și a celor indivizi, ce prezintă riscuri la adresa securității naționale;
- identificarea persoanelor de interes înainte de a ajunge la punctul de trecere a frontierei și luarea deciziilor corespunzătoare.

3. Descrierea gradului de compatibilitate pentru proiectele care au ca scop armonizarea legislației naționale cu legislația Uniunii Europene

Proiectul de lege transpune:

Directiva (UE) nr. 2016/681 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave, publicat în Jurnalul Oficial al Uniunii Europene seria L nr. 119 din 4 mai 2016;

parțial Decizia de punere în aplicare (UE) 2017/759 a Comisiei 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.

Implementarea API/PNR în Republica Moldova datează încă din anul 2014 când a fost introdus în Hotărârea Guvernului nr. 808/2014 cu privire la aprobarea planului național de acțiuni pentru implementarea Acordului de Asociere Republica Moldova – Uniunea Europeană în perioada 2014-2016, Titlul III. Justiție, libertate și securitate, articolul 14 din Acordul de Asociere, Cooperarea în domeniul migrației, al azilului și al gestionării frontierelor, măsura de implementare 55 „Implementarea sistemului avansat de informații despre pasageri (API) în punctul de trecere a frontierei ”Aeroport-Chișinău”³.

4. Principalele prevederi ale proiectului și evidențierea elementelor noi

Prin proiectul de lege se reglementează transmiterea datelor despre călători de la transportatorii aerieni la Unitatea de Informații privind Pasagerii prin crearea unui ghișeu unic pentru transmiterea datelor, ca fiind un instrument cost-efectiv și care reduce din povara transmiterii datelor de către companiile aeriene conform SARPs ICAO. Conform experienței unor țări din UE, datele API sunt transmise de două ori, odată la autoritatea de aplicare a legii și odată la unitatea de informații privind pasagerii.

³ https://www.legis.md/căutare/getResults?doc_id=88616&lang=ro

Inspectoratul General al Poliției de Frontieră (IGPF) va colecta datele despre pasageri conform principiului ghișeului unic. Unitatea de Informații privind Pasagerii (UIP) va fi instituită în cadrul Poliției de Frontieră.

Regulamentul de activitate al UIP va fi instituit printr-un act normativ administrativ comun care va avea grad de secretizare conform informațiilor atribuite la secret de stat.

Numirea responsabilului pentru protecția datelor în cadrul UIP va asigura că datele PNR, precum și rezultatul prelucrării datelor PNR vor fi utilizate strict pentru scopurile stabilite și vor fi respectate drepturile fundamentale ale omului, respectând actele normative în materia protecției datelor cu caracter personal.

Obligațiile companiilor aeriene de a transmite datele despre pasageri, la intervale de timp:

- a) între 48 ore până la 24 ore până la ora programată a zborului;
- b) dacă nu sunt date PNR disponibile conform lit. a), transportatorul aerian va transmite actualizări la 2 ore;
- c) imediat după închiderea zborului, adică imediat după îmbarcarea călătorilor în aeronava care se pregătește pentru decolare, și când nici un călător nu se mai poate îmbarca sau debarca.

Transmiterea datelor va fi efectuată exclusiv prin metoda de tip „push”, care se consideră că oferă un grad mai mare de protecție și este obligatorie pentru companiile aeriene.

Transferul datelor către alte state și organizații internaționale, inclusiv Europol, se va efectua conform prevederilor proiectului legii, precum și în temeiul tratatelor internaționale la care Republica Moldova este parte.

În același context, se instituie prevederi referitor la protecția datelor cu caracter personal: perioada de păstrare a datelor și depersonalizarea acestora. Din cauza naturii datelor și scopurilor pentru care acestea sunt utilizate, este necesar ca datele din PNR să fie păstrate o perioadă de 5 ani, suficientă pentru efectuarea de analize și pentru utilizarea în investigații. Depersonalizarea se va efectua, după 6 luni de la transmiterea datelor, prin mascarea datelor care permit identificarea directă a persoanei.

Funcționalitatea API/PNR va fi efectuată prin implementarea, instalarea, îmbunătățirea și suportul de întreținere a soluției soft goTravel, care este o versiune configurată de ONU a sistemului Travel Information Portal (TRIP), donat de Regatul Țărilor de Jos fiind o soluție eficientă în vederea colectării și procesării datelor despre pasageri, cum ar fi API și PNR, utilizând principiul ghișeului unic. INTERPOL susține conectarea goTravel la bazele sale de date a teroriștilor cunoscuți/suspecți și criminalilor. Software-ul estimat la 12-15 milioane de dolari este disponibil cu titlu gratuit, donat de ONU, pentru primii 2 ani de utilizare de la momentul semnării Memorandumului de înțelegere pentru utilizarea soluției soft AIR goTravel și furnizarea serviciilor aferente (în continuare - MoA). Soluția soft goTravel va fi găzduită pe platforma guvernamentală MCloud și va fi gestionată de către IGPF, care va avea rolul de posesor și deținător a acestei resurse informaționale.

Un alt element important al proiectului îl constituie includerea termenului „călător” care înglobează și membrii echipajului. Acest lucru este menționat în „Manualul pentru sistemele de informare prealabilă despre pasagerilor” (API) adoptat de OMV, OACI și IATA, ediția iunie 2022, ceea ce permite colectarea datelor API despre pasageri și membrii echipajului. Plus la aceasta capitolul I. B, pag. 4 a Manualului prevede

asemenea noțiune ca „Călător”⁴. Este de menționat faptul că în Directiva PNR termenul „pasager” exclude datele despre membrii echipajului, dar instrumentele juridice internaționale permit acest lucru.

Odată cu stabilirea parcursului european al Republicii Moldova, utilizarea definiției de infracțiuni transnaționale grave și a listei formelor de criminalitate rezidă, inclusiv și, din prevederile Regulamentului (UE) 2016/794 privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol), Deciziei-cadru a Consiliului 2002/584/JAI privind mandatul european de arestare, Legii nr. 15/2005 pentru ratificarea Convenției Națiunilor Unite împotriva criminalității transnaționale organizate, precum și a Legii nr. 116/2015 pentru ratificarea Acordului privind cooperarea operațională și strategică dintre Republica Moldova și Oficiul European de Poliție și a Legii 118/2020 privind răspunderea civilă și cerințele de asigurare a operatorilor aerieni și a operatorilor de aeronave, precum și a Acordului dintre Statele Unite ale Americii și Uniunea Europeană privind utilizarea și transferul de date din registrele cu numele pasagerilor către Departamentul pentru Securitate Internă al Statelor Unite.

La elaborarea proiectului a fost studiată experiența statelor: România, Letonia, Regatul Țărilor de Jos, Germania, Franța, Lituania, Canada. De asemenea, a fost studiat Raportul completat de Organizația pentru Securitate și Cooperare în Europa privind experiența internațională și bunele practici cu privire la API/PNR⁵ și diferite rapoarte la nivelul Uniunii Europene privind revizuirea Directivelor cu privire la datele API/PNR.

Conform proiectului principiul necesității de a cunoaște este principiul conform căruia accesul la informațiile cu grad de secretizare se acordă în mod individual și exclusiv numai persoanelor care, conform atribuțiilor de serviciu, au dreptul să lucreze cu astfel de informații și/sau să aibă acces la acestea, în conformitate cu prevederile legale aplicabile acestor categorii de informații.

Proiectul intră în vigoare la expirarea a 12 luni de la data publicării acestuia. Acest termen este dedicat pentru operaționalizarea unității, a infrastructurii, cât și pentru a se aduce în concordanță actele normative menționate la pct. 6.

5. Fundamentarea economico-financiară

Costurile pentru operaționalizarea UIP vor fi acoperite de către Organizația Internațională pentru Migrație printr-un proiect care are un buget în jur de 195 000 \$, cum ar fi:

1. achiziționarea de echipamente și tehnici speciale pentru dotarea a 10 locuri de muncă pentru personalul unității;
2. repararea/dotarea sediului UIP;
3. organizarea instruirilor pentru personalul UIP și organizarea de vizite de studiu pentru a face cunoștință cu experiența altor țări care au implementat deja goTravel.

Soluția soft goTravel, oferită gratuit de ONU pentru primii doi ani de utilizare, după semnarea Memorandumului de Înțelegere (MoA) dintre Republica Moldova și ONU nu implică acces la datele cu caracter personal din partea ONU, iar Republica Moldova beneficiază de toată asistența/întreținerea/actualizările. Din anul trei de implementare

⁴ <https://www.iata.org/contentassets/18a5fdb2dc144d619a8c10dc1472ae80/api-guidelines.en.final.pdf>

⁵ <https://www.osce.org/project-coordinator-in-ukraine/510575>

se va examina oportunitatea sau inoportunitatea utilizării și întreținerii suplimentare. În cazul oportunității utilizării, costurile vor fi partajate pentru toate statele care utilizează sistemul (66 la număr), în funcție de PIB-ul țării, Republicii Moldova revenindu-i suma anuală de aproximativ 100.000 dolari SUA. Conform Hotărârii Guvernului nr. 408/2023 cu privire la aprobarea cadrului bugetar pe termen mediu (2024-2026), anual sunt preconizate câte 1000 mii lei la subprogramul 3506 „Managementul frontierei”, dezvoltarea/mentenanța sistemelor informaționale. Prioritățile Sectorului „ordine publice” (06) prevăd - modernizarea sistemului de coordonare a securității frontierei de stat prin implementarea sistemelor informaționale *avansate* în vederea identificării timpurii a riscurilor și a amenințărilor la adresa securității și ordinii publice.

6. Modul de încorporare a actului în cadrul normativ în vigoare

Adoptarea actului normativ necesită modificarea următoarelor acte normative:

1. Legea nr. 215/2011 cu privire la frontiera de stat;
2. Legea nr. 120/2017 cu privire la prevenirea și combaterea terorismului.
3. Codul contravențional al Republicii Moldova nr. 218/2008.

7. Avizarea și consultarea publică a proiectului

În scopul respectării prevederilor Legii nr. 239/2008 privind transparența în procesul decizional, decizia privind inițierea proiectului a fost plasată pe pagina web oficială a Ministerului Afacerilor Interne www.mai.gov.md, în rubrica: Transparență, secțiunea: Anunțuri privind consultările publice și pe platforma guvernamentală www.particip.gov.md, <https://particip.gov.md/ro/document/stages/proiectul-legii-privind-utilizarea-datelor-din-registrul-cu-numele-pasagerilor-pnr/10179>.

8. Constatările expertizei anticorupție

Conform raportului de expertiză anticorupție nr. ELO23/8952 din 10 august 2023, proiectul nu conține factori de risc care să genereze apariția riscurilor de corupție.

9. Constatările expertizei de compatibilitate

Proiectul a fost ajustat conform concluziilor expertizei de compatibilitate.

10. Constatările expertizei juridice

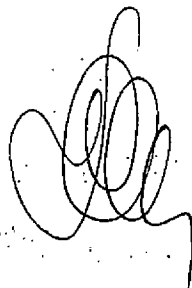
Proiectul a fost ajustat conform avizului remis de Ministerul Justiției.

11. Constatările altor expertize

Proiectul a fost supus expertizei de către Grupul de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător în sensul Legii nr. 235/2006 cu privire la principiile de bază de reglementare a activității de întreprinzător.

Proiectul nu necesită alte expertize.

Ministru al afacerilor interne



Adrian EFROS

