Proiect UE

GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. ____

din _____ 2023

Chișinău

pentru aprobarea proiectului de lege privind utilizarea datelor din registrul cu numele pasagerilor (călătorilor) (PNR)

Guvernul HOTĂRĂȘTE:

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

Prim-ministru **DORIN RECEAN**

Contrasemnează:

Ministrul infrastructurii
și dezvoltării regionale Lilia DABIJA

Ministrul afacerilor interne Ana REVENCO

Ministrul justiției Veronica MIHAILOV-MORARU

Proiect UE

P A R L A M E N T U L R E P U B L I C I I M O L D O V A

L E G E nr._____
din_____ 2023
Chișinău

privind utilizarea datelor din registrul cu numele pasagerilor (călătorilor) (PNR)

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;

- 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.

Parlamentul adoptă prezenta lege.

Capitolul I

DISPOZIȚII GENERALE

Articolul 1. Obiectul de reglementare

(1) Prezenta lege reglementează:

a) transmiterea către autoritățile competente a datelor din registrul cu numele pasagerilor (în continuare - *PNR*) de către transportatorii aerieni la unitatea de informații privind pasagerii (în continuare - *UIP*);

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 contiuare - 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.122/2022.

(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 și conform acordurilor internaționale la care Republica Moldova face 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 grave 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 abstractă a 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, etc.;
depersonalizare prin mascarea elementelor de date – acțiune care are drept scop ca acele elemente ale datelor PNR care servesc la identificarea directă a unei persoanei să nu fie vizibile pentru utilizatorii sistemului informațional „Registrul cu numele pasagerilor (PNR)”;
date prealabile despre pasageri (date API) - set de date despre zbor și datele biografice ale unui călător, conținute de actul de călătorie al acestuia, prevăzute ca parte componentă a datelor PNR, oferite/puse la dispoziție de transportatorii aerieni;
infracțiuni cu caracter terorist – infracțiunile prevăzute în art. 134^{11} din Codul Penal al Republicii Moldova nr. 985/2002;
infracțiuni grave – infracțiunile, pentru care pedeapsa prevăzută de lege este detențiunea pe viață sau închisoarea pentru o perioadă maximă de cel puțin 3 ani, corespunzătoare formelor de criminalitate prevăzute în anexa nr. 2;

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 sistemul informațional „Registrul cu numele pasagerilor (PNR)";
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 şi vinde şi eliberează bilete pentru respectivul zbor;
rezultat pozitiv – verificarea manuală, efectuată de către personalul UIP, în diverse surse și sisteme informaționale (baze de date, OSINT etc.), în vederea validării rezultatului obținut în mod automatizat (soluția soft);
sistem de control al plecărilor – sistem automat de înregistrare a pasagerilor, bagajelor și încărcăturii cargo, îmbarcate la bordul unei aeronave;
sistemul informațional „Registrul cu numele pasagerilor" – registru al cerințelor de călătorie ale fiecărui călător, care conține informațiile necesare pentru a permite prelucrarea și controlul 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 operațini de transport aerian;
Unitate de informație privind pasagerii – subdiviziune structurală în subordinea Inspectoratului General al Poliției de Frontieră, fără personalitate juridică, desemnată pentru prelucrarea datelor despre călători;
zbor spre/dinspre Republica Moldova – orice zbor regulat, neregulat sau operațiuni necomerciale (aviație generală) 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 se înființează în cadrul Inspectoratului General al Poliției de Frontieră (în continuare - *IGPF*) și 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) schimbul de date PNR și schimbul de rezultate ale prelucrării datelor PNR cu UIP din alte state și cu Europol.

Articolul 4. Personalul UIP

(1) UIP este condusă de un șef, numit în funcție de șeful Inspectoratului General al Poliției de Frontieră.

(2) Personalul UIP este constituit din funcționari publici cu statut special și angajați din cadrul autorităților competente, detașați în scopul efectuării evaluării datelor în conformitate cu art. 10-12.

(3) Acordarea personalului UIP a drepturilor de acces la datele PNR este guvernat de principiul necesității de a cunoaște.

Secțiunea II

Responsabilul cu protecția datelor în cadrul UIP

Articolul 5. Persoana responsabilă cu protecția datelor

(1) Persoana responsabilă cu protecția datelor din cadrul IGPF este responsabilă pentru monitorizarea operațiunilor de prelucrare a datelor cu caracter personal și respectarea drepturilor și garanțiilor prevăzute de actele normative privind protecția datelor cu caracter personal.

(2) Responsabilul cu protecția datelor este desemnat 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) IGPF asigură că persoana responsabilă cu protecția datelor nu primește instrucțiuni cu privire la îndeplinirea sarcinilor. În exercitarea sarcinilor privind respectarea cadrului normativ privind protecția datelor cu caracter personal, responsabilul cu protecția datelor este independent și imparțial.

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

(5) Responsabilul cu protecția datelor în cadrul UIP își desfășoară activitatea în subordinea nemijlocită a șefului IGPF. Șeful IGPF asigură preluarea atribuțiilor responsabilului cu protecția datelor în cadrul UIP, în cazul absenței acestuia de la serviciu pentru o perioadă mai mare de 5 zile, de către o persoană calificată în domeniul protecției datelor cu caracter personal.

(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*).

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 cu 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 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 sistemului informațional „Registrul cu numele pasagerilor (PNR)” (în continuare – sistemul PNR).

(2) Responsabilul cu protecția datelor informează conducerea IGPF, în timp de 72 de ore, 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 sistemului PNR 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 cu protecția datelor informează, imediat, Centrul.

Capitolul III

Utilizarea datelor despre călători

Articolul 8. Scopul utilizării datelor despre călători

Datele PNR cuprinse în sistemul PNR 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 grave;

b) prevenirea și contracararea amenințărilor la adresa securității statului prevăzute la art. 4 din Legea securității statului nr. 618/1999.

Secțiunea III

Evaluarea datelor despre călători

Articolul 9. Sistemul informațional de evidență a datelor PNR

(1) Sistemul informațional „Registrul cu numele pasagerilor (PNR)” este reglementat de Guvern.

(2) IGPF, ca posesor al sistemului, asigură condițiile financiare și organizatorice pentru administrarea, mentenanța și dezvoltarea sistemului informațional „Registrul cu numele pasagerilor (PNR)”.

(3) Resursele informaționale utilizate pentru efectuarea evaluărilor sunt stabilite de Guvern.

Articolul 10. Prelucrarea datelor PNR

(1) UIP prelucrează datele despre călători doar în următoarele scopuri:

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 grave sau într-o activitate care constituie amenințare la adresa securității statului;

b) oferirea de răspunsuri, în cazul unei cereri temeinic justificate, în temeiul actelor normative, din partea autorităților competente vizând furnizarea și prelucrarea datelor PNR, în cazuri concrete, în scopurile prevăzute la art. 8, și comunicarea rezultatelor acestei prelucrări autorităților competente sau, după caz, Europol;

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 grave 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. (1) lit. a) 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 reexaminate 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 reexaminate 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 doar în scopurile prevăzute la art. 8, sunt următoarele:

1) Din cadrul Ministerului Afacerilor Interne:
   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 normative administrative comune:

a) subdiviziunile structurale din cadrul fiecărei autorități competente abilitate să solicite, să primească și să prelucreze date PNR;

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).

(2) 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 aplicabile activităților în cadrul cărora sunt utilizate datele respective.

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 sistemului PNR pentru o perioadă de 5 ani de la momentul finalizării transmiterii active a respectivelor date PNR din sistemele transportatorilor aerieni în sistemul informațional „Registrul cu numele pasagerilor (PNR)”, 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, prevăzut 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) din prezentul articol.

Articolul 16. Dezvăluirea datelor

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

a) se consideră în mod rezonabil că este necesară în scopul menționat la art. 10 lit. b);

b) dezvăluirea este aprobată de instanța de judecată (judecător de instrucție), cu informarea responsabilului cu protecția datelor din cadrul UIP și a revizuirii ulterioare de către acesta.

CAPITOLUL IV

Obligațiile transportatorilor aerieni de a transmite datele despre călători

Articolul 17. Transmiterea datelor despre călători

(1) Transportatorul aerian transmite gratuit către UIP, prin metoda push, întreaga listă a datelor despre fiecare călător individual pentru fiecare zbor, în măsura în care aceștia colectează deja aceste date.

(2) Dacă este vorba de un zbor 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) nu mai devreme de 48 ore și numai târziu cu 24 ore înainte de ora programată pentru plecarea fiecărui zbor;

b) 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 („wheels-up”), 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 călătorului conform lit. a), transportatorul aerian 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 grave 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 aplicare 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 protecița datelor cu caracter personal aplicabile.

(9) Protocoalele comune și formatul de date compatibile sunt transmise conform Deciziei 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 (în continuare - Decizie).

(10) În cazul în care transportatorii aerieni transferă date API separat de datele PNR transferate pentru același zbor, aceștia utilizează formatul de date EDIFACT PAXLST, astfel cum este descris în ghidul de punere în aplicare a mesajului OMV/IATA/OACI privind lista pasagerilor, versiunea 2003 sau ulterioară.

(11) Prin derogare de la alineatele 9 și 10, transportatorii aerienei care nu dispun de infrastructura necesară pentru a putea folosi formatele și protocoalele de transmitere a datelor enumerate în anexa la Decizie, transmit datele PNR prin mijloace electronice care oferă garanții suficiente în ceea ce privește respectarea măsurilor de securitate tehnică și care urmează a fi convenite la nivel bilateral, între transportatorul aerian și Republica Moldova.

CAPITOLUL V

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 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 membre, cu excepția situațiilor care privesc securitatea statului.

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

(4) UIP poate solicita, în condițiile alin. (5), din proprie inițiativă sau la cerere temeinic justificată a unei autorități competente, UIP a altui stat membru al Uniunii Europene 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 grave.

(6) În cazul în care primește, din partea UIP a altui 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 grave, 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 Uniunii Europene, dacă solicitarea cuprinde mențiuni din care să rezulte că datele PNR sunt necesare într-un caz urgent. Solicitările 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 grave, 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 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 grave.

(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 alte state membre ale Uniunii Europene se poate realiza prin intermediul oricărui canal de coopeare existent între autoritățile competente ale statelor membre ale Uniunii Europene. 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 grave către Europol, prin intermediul Centrului de Cooperare Polițienească Internațională din cadrul Inspectoratului General al Poliției. Art. 16 se aplică mutadis mutandis.

(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 grave, în măsura în care infracțiunea respectivă intră în sfera de competență a Europol, în temeiul legislației Uniunii Europene 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 Uniunii Europene 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 țări terțe, cu consimțământul judecătorului de instrucție, dacă sunt îndeplinite următoarele condiții:

a) țările terțe 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 din prezenta lege;

c) țara terță 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 terță 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 mutatis mutandis;

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 grave, la adresa unui stat membru sau a unei țări terțe; 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 terțe 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 VI

Protecția datelor

Articolul 23. Desemnarea operatorului

(1) Inspectoratul General al Poliției de Frontieră se desemnează în calitate de operator al Sistemului informațional „Registrul cu numele pasagerilor (PNR)” în sensul actelor normative privind protecția datelor cu caracter personal.

(2) Personalul UIP au calitate de utilizatori ai Sistemului PNR. 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 sistemului PNR 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) domiciliul;

c) adresa de poștă sau adresa de poștă electronică dacă se solicită răspuns pe această cale;

d) obiectul cererii și motivarea acesteia;

e) semnătura subiectului de date ori a reprezentantului său legal sau împuternicit, iar în cazul cererii transmise în formă electronică – semnătura electronică în conformitate cu prevederile Legii nr. 124/2022 privind identificarea electronică și serviciile de încredere.

(3) Pentru a comunica subiectului de date informații cu privire la datele cu caracter personal prelucrate în cadrul sistemului, în situația prelucrărilor prevăzute la art. 18-22, UIP solicită, după caz, acordul autorităților competente către care au fost transferate datele, acordul EUROPOL sau acordul entității publice similare 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 situația în care entitatea publică similară din străinătate consultată potrivit alin. (3) nu comunică un răspuns în considerarea termenelor de răspuns la cererile subiecților de date, UIP răspunde solicitantului fără a indica proveniența datelor.

(6) În situația în care o entitate publică similară din străinătate 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 similară din străinătate, UIP consultă respectiva autoritate competentă indicând și eventualul termen precizat de entitatea publică solicitantă.

Articolul 25. Securitatea și confidențialitatea datelor cu caracter personal

(1) Asigurarea securității și confidențialității datelor cu caracter personal în cadrul sistemului PNR 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 sistemului PNR, 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 este interzisă dacă dezvăluie originea rasială sau etnică, opiniile politice, religia sau convingerile filozofice, apartenența la un sindicat, sănătatea, viața sexuală sau orientarea sexuală a unei persoane.

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

(3) Prelucrarea datelor PNR după criterii legate de categoriile de informații prevăzute la alin. (1) este interzisă.

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 membre;

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

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

Articolul 28. Trasabilitatea prelucrărilor

(1) Sistemul PNR 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) Sistemul PNR asigură cel puțin trasabilitatea operațiunilor de prelucrare a datelor cu caracter personal conform cadrului normativ prin protecția datelor.

(3) Fișierul de trasabilitate generat de sistemul 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 sistemul PNR pot fi accesate doar pentru următoarele scopuri:

a) verificarea și monitorizarea legalității efectuării prelucrărilor;

b) asigurarea funcționării tehnice corespunzătoare a sistemului PNR;

c) asigurarea integrității și securității datelor PNR.

(5) Utilizarea fișierelor de trasabilitate generate de către sistemul PNR în alte scopuri decât cele prevăzute la alin. (4) este interzisă.

(6) Fișierele de trasabilitate generate de către sistemul PNR 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 sistemului PNR, 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 sistemului PNR, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ de persoane viza 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. (6), 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, explicite 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 sistemului PNR, 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 sistemului PNR 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. 6 alin. (3).

Articolul 33. Sancțiuni

(1) Încălcarea prevederilor prezentei legi atrage, după caz, răspunderea contravențională, penală sau alte tipuri de răspundere în conformitate cu legislația.

(2) În cazul nerespectării prevederilor prevăzute la art. 17, față de transportatorii aerieni sînt aplicate următoarele tipuri de sancţiuni:

a) prescripția de a transmite datele conform actelor normative;

b) amendă;

c) retragerea sau suspendarea temporară a certificatului de operator aerian valabil, și după caz, a licenței de operare conform actelor normative.

CAPITOLUL VII
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 6 luni de la data publicării în Monitoriul Oficial al Republicii Moldova.

2. Guvernul, în termen de 6 luni de la data intrării în vigoare a prezentei legi va prezenta propuneri Parlamentului privind aducerea în concordanță a actelor normative cu prezenta lege;

3. De la data publicării prezentei legi, Guvernul va întreprinde măsurile necesare pentru desemnarea autorității responsabile, în cadrul căreia se înființează UIP, precum și pentru reglementarewa modului de organizare și funcționare, precum și va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normaive necesare punerii în aplicare a prevederilor prezentei legi.

PREȘEDINTELE PARLAMENTULUI

Igor GROSU

Anexa nr. 1

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. Situația de călătorie a pasagerului, 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. Orice date API colectate, inclusiv tipul, numărul, țara sau denumirea organizației de emitere și data expirării oricărui act 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 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 1-18.

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.

Anexa nr. 2

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.