

TABEL CONCORDANȚĂ

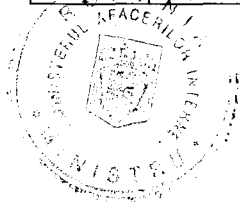
<p align="center">Directiva (UE) 2016/681 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave</p>	<p align="center">Proiect de lege privind utilizarea datelor din registrul cu numele pasagerilor pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave</p>	<p align="center">Observații</p>
<p>CAPITOLUL I - Dispoziții generale Articolul 1 - Obiectul și domeniul de aplicare (1) Prezenta directivă reglementează: (a) transferul de către transportatorii aerieni al datelor din registrul cu numele pasagerilor (PNR) ale pasagerilor zborurilor extra-UE; (b) prelucrarea datelor menționate la litera (a), inclusiv colectarea, utilizarea și păstrarea acestora de către statele membre și schimbul de astfel de date între statele membre.</p>	<p>Art.1 - Domeniul de aplicare (1) Prezenta lege reglementează: a) transmiterea datelor din registrul cu numele pasagerilor, prevăzute la art.14, denumite în continuare date PNR aferente zborurilor extra-UE și intra-UE, de la transportatorii aerieni la Unitatea națională de informații privind pasagerii prevăzută la art.4 alin.(1), denumită în continuare UNIP; b) prelucrarea datelor PNR, inclusiv colectarea, utilizarea și păstrarea acestora de către UNIP; c) schimbul de date PNR cu alte state; d) condițiile de acces al Oficiului European de Poliție, denumit în continuare EUROPOL, la datele PNR colectate de UNIP. </p>	
<p>(2) Datele din PNR colectate în conformitate cu prezenta directivă pot fi prelucrate doar în scopul prevenirii, depistării, investigării și urmării penale a infracțiunilor de terorism și a infracțiunilor grave, astfel cum este prevăzut la articolul 6 alineatul (2) literele (a), (b) și (c).</p>	<p>Art.18 - Scopul utilizării datelor PNR Datele PNR cuprinse în Sistemul de evidență a datelor PNR se utilizează doar pentru următoarele scopuri: a) prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism sau a infracțiunilor grave; </p>	
<p>Articolul 2 - Aplicarea prezentei directivei în cazul zborurilor intra-UE (1) Dacă un stat membru decide să aplice prezenta directivă în cazul zborurilor intra-UE, acesta notifică în scris Comisia. Un stat membru poate transmite sau revoca o astfel de notificare în orice</p>	<p>Art.2 - Notificarea colectării și utilizării datelor PNR aferente zborurilor intra-UE În termen de 30 de zile de la intrarea în vigoare a prezentei legi, prin grija Ministerului Afacerilor Interne, se transmite Comisiei Europene o notificare scrisă privind prelucrarea datelor PNR</p>	



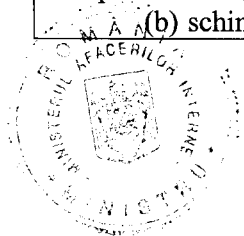
<p>moment. Comisia publică respectiva notificare și orice revocare a acesteia în Jurnalul Oficial al Uniunii Europene.</p> <p>(2) Atunci când se transmite o notificare menționată la alineatul (1), toate dispozițiile prezentei directive se aplică zborurilor intra-UE ca și cum ar fi zboruri extra-UE și datelor din PNR de la zborurile intra-UE ca și cum ar fi date PNR de la zboruri extra-UE.</p>	<p>aferente zborurilor intra-UE.</p>	
<p>(3) Un stat membru poate decide să aplice prezenta directivă numai anumitor zboruri intra-UE. În luarea unei astfel de decizii, statul membru alege zborurile pe care le consideră necesare pentru urmărirea obiectivelor prezentei directive. Statul membru poate decide în orice moment modificarea selecției zborurilor intra-UE.</p>		<p>Se aplică tuturor zborurilor intra-UE</p>
<p>Articolul 3 - Definiții</p> <p>În sensul prezentei directive, se aplică următoarele definiții:</p> <p>1. „transportator aerian” înseamnă o întreprindere de transport aerian care deține o licență de operare valabilă sau un document echivalent care îi permite să efectueze activități de transport aerian de pasageri;</p>	<p>Art.3 - Definirea unor termeni și expresii</p> <p>În sensul prezentei legi, termenii și expresiile de mai jos au următoarele semnificații:</p> <p>a) transportator aerian - orice persoană fizică sau juridică, română sau străină, deținătoare a unui certificat de operator aerian în termen de valabilitate și, după caz, a unei licențe de operare, al cărei obiect de activitate îl reprezintă asigurarea transportului pasagerilor pe calea aerului;</p>	
<p>2. „zbor extra-UE” înseamnă orice zbor regulat sau neregulat al unui transportator aerian cu proveniența dintr-o țară terță și planificat să aterizeze pe teritoriul unui stat membru sau să decoleze de pe teritoriul unui stat membru și planificat să aterizeze într-o țară terță, inclusiv, în ambele cazuri, zboruri cu orice escală pe teritoriul statelor membre sau al țărilor terțe;</p>	<p>b) zbor extra-UE - orice zbor regulat sau neregulat al unui transportator aerian cu punctul de plecare sau tranzit într-o țară terță și planificat să aterizeze pe teritoriul României sau să decoleze de pe teritoriul României și planificat să aterizeze într-o țară terță, inclusiv zboruri pentru care sunt desemnate aeroporturi sau aerodromuri de rezervă situate pe teritoriul României;</p>	
<p>3. „zbor intra-UE” înseamnă orice zbor regulat sau neregulat al unui transportator aerian cu proveniența de pe teritoriul unui stat membru și planificat să aterizeze pe teritoriul unuia sau mai</p>	<p>c) zbor intra-UE - orice zbor regulat sau neregulat al unui transportator aerian cu punctul de plecare sau tranzit de pe teritoriul unui stat membru al Uniunii Europene, inclusiv</p>	



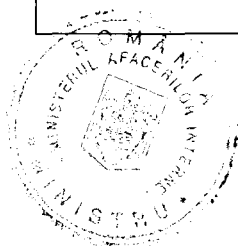
multor state membre, fără escală pe teritoriul unei țări terțe;	România, și planificat să aterizeze pe teritoriul României, sau să decoleze de pe teritoriul României și planificat să aterizeze pe teritoriul unui stat membru al Uniunii Europene, inclusiv România, în ambele cazuri fără escală pe teritoriul unei țări terțe;	
4. „ pasager ” înseamnă orice persoană, inclusiv persoanele aflate în transfer sau în tranzit și 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;	d) pasager - orice persoană fizică, inclusiv persoanele aflate în transfer sau în tranzit, cu excepția membrilor 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;	
5. „ registru cu numele pasagerilor ” sau „ PNR ” înseamnă un registru al cerințelor de călătorie ale fiecărui pasager, care conține informațiile necesare pentru a permite prelucrarea și controlul rezervărilor de către transportatorii aerieni care efectuează rezervările și de către cei 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 utilizat pentru verificarea pasagerilor la îmbarcarea în avion, sau în sisteme echivalente care oferă aceleași funcționalități;	e) registru cu numele pasagerilor sau PNR - registru al cerințelor de călătorie ale fiecărui pasager, 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 sisteme echivalente care oferă aceleași funcționalități;	
6. „ sistem de rezervare ” înseamnă sistemul intern al transportatorului aerian, în care datele din PNR sunt colectate pentru gestionarea rezervărilor;	f) sistem de rezervare - sistemul intern al transportatorului aerian, în care datele PNR sunt colectate pentru gestionarea rezervărilor;	
7. „ metoda de tip push ” înseamnă metoda prin care transportatorii aerieni transferă datele din PNR, enumerate în anexa I, în baza de date a autorității solicitante;	g) metoda de tip push - metoda prin care transportatorii aerieni transferă datele PNR către UNIP, care presupune realizarea unei transmisiuni active de date din sistemele transportatorilor aerieni în Sistemul de evidență a datelor PNR;	
8. „ infrațiuni de terorism ” înseamnă infrațiunile prevăzute de dreptul intern menționate la articolele 1-4 din Decizia-cadru	h) infrațiuni de terorism - infrațiunile prevăzute în Legea nr.535/2004 privind prevenirea și combaterea terorismului, cu	



2002/475/JAI;	modificările și completările ulterioare;	
9. „ infrațiuni grave ” înseamnă infracțiunile enumerate în anexa II, care sunt pasibile de pedepse cu închisoarea sau cu o măsură privativă de libertate pe o perioadă maximă de cel puțin trei ani în temeiul dreptului intern al unui stat membru;	i) infrațiuni grave – infracțiunile pentru care pedeapsa prevăzută de lege este detențiunea pe viață sau închisoarea al cărei maxim special este de cel puțin trei ani, corespunzătoare formelor de criminalitate prevăzute în Anexa care face parte integrantă din prezenta lege;	
10. „ a depersonaliza prin mascarea elementelor de date ” înseamnă a face ca acele elemente ale datelor care ar putea servi la identificarea directă a persoanei vizate să nu fie vizibile pentru un utilizator.	j) depersonalizare prin mascarea elementelor de date - acțiunea prin care acele elemente ale datelor PNR care ar putea servi la identificarea directă a unei persoane să nu fie vizibile pentru utilizatorii Sistemului de evidență a datelor PNR;	
CAPITOLUL II - Responsabilitățile statelor membre Articolul 4 - Unitatea de informații despre pasageri (1) Fiecare stat membru instituie sau desemnează o autoritate competentă pentru prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave sau o filială a unei astfel de autorități, care să acționeze ca unitate de informații despre pasageri (UIP).	CAP. II – Cadrul organizatoric &.1 Unitatea națională de informații privind pasagerii Art.4 - Înființarea și atribuțiile principale ale UNIP (1) În cadrul Inspectoratului General al Poliției de Frontieră, denumit în continuare IGPF, se înființează UNIP, ca structură de specialitate, fără personalitate juridică, prin preluarea activității și a personalului Unității naționale de informații privind pasagerii înființată potrivit art.8 alin.(1) din Ordonanța Guvernului nr.13/2015 privind utilizarea unor date din registrele cu numele pasagerilor în cadrul cooperării transfrontaliere pentru prevenirea și combaterea actelor de terorism, a infracțiunilor conexe acestora și a infracțiunilor contra securității naționale, precum și pentru prevenirea și înlăturarea amenințărilor la adresa securității naționale.	
(2) UIP este responsabilă de: (a) colectarea datelor din PNR de la transportatorii aerieni, stocarea și prelucrarea acestor date și transferul datelor respective sau al rezultatului prelucrării acestora autorităților competente menționate la articolul 7; (b) schimbul de date din PNR, precum și de schimbul de	(2) UNIP îndeplinește următoarele atribuții principale: a) colectarea datelor PNR de la transportatorii aerieni, stocarea și prelucrarea acestor date și transferul datelor respective sau al rezultatului prelucrării acestora către autoritățile competente, în condițiile stabilite la art.20 – 22; b) schimbul de date PNR și schimbul de rezultate ale prelucrării	



<p>rezultate ale prelucrării acestora cu UIP din alte state membre și cu Europol, în conformitate cu articolele 9 și 10.</p>	<p>datelor PNR cu Unitățile de informații privind pasagerii din alte state membre ale Uniunii Europene și cu EUROPOL, în condițiile stabilite la art.24, art.26 și art.27; c) schimbul de date PNR cu state terțe, în condițiile stabilite la art.28 și art.29.</p>	
<p>(3) Membrii personalului UIP pot fi detașați de la autoritățile competente. Statele membre furnizează UIP resurse adecvate pentru ca acestea să-și îndeplinească sarcinile.</p>	<p>Art.7 - Personalul UNIP (3) În cadrul UNIP poate fi detașat sau delegat, în condițiile legii, personal de la autoritățile competente, în scopul efectuării evaluărilor prevăzute la art.20 - 22, cu respectarea principiului necesității de a cunoaște.</p>	
<p>(4) Două sau mai multe state membre (denumite în continuare „statele membre participante”) pot stabili sau desemna o singură autoritate în calitate de UIP. O astfel de UIP se înființează într-unul dintre statele membre participante și este considerată UIP națională a tuturor statelor membre participante. Statele membre participante convin împreună asupra normelor detaliate privind funcționarea UIP și respectă cerințele stabilite în prezenta directivă.</p>	<p>Art.5 - Tratatate privind desemnarea Unității naționale de informații privind pasagerii (1) Prin tratate încheiate cu alte state membre ale Uniunii Europene se poate stabili ca UNIP să fie desemnată ca Unitate națională de informații privind pasagerii a respectivului stat sau a respectivelor state membre ale Uniunii Europene. (2) Prin tratate încheiate cu alte state membre ale Uniunii Europene se poate stabili ca Unitatea națională de informații privind pasagerii a unuia dintre respectivele state membre să fie desemnată ca Unitate națională de informații privind pasagerii a României. (3) Prin tratatele prevăzute la alin.(1) și (2) se stabilesc norme detaliate privind funcționarea Unității naționale de informații privind pasagerii comună statelor membre ale Uniunii Europene între care se încheie respectivul tratat și se respectă dreptul Uniunii Europene în materie, inclusiv cerințele stabilite prin Directiva (UE) 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.</p>	



	(4) În cazul prevăzut la alin.(2), aspectele privind desființarea UNIP se stabilesc prin actul normativ de ratificare a tratatului în cauză.	
(5) În termen de o lună de la înființarea UIP, fiecare stat membru transmite o notificare Comisiei cu privire la acest lucru și poate să își modifice notificarea în orice moment. Comisia publică notificarea și eventualele modificări ale acesteia, în Jurnalul Oficial al Uniunii Europene.	<p>Art.6 - Notificarea privind înființarea sau desemnarea UNIP</p> <p>(1) În termen de 30 de zile de la intrarea în vigoare a prezentei legi, prin grija Ministerului Afacerilor Interne, se transmite Comisiei Europene o notificare scrisă privind înființarea UNIP.</p> <p>(2) În cazul modificării situației notificate potrivit alin.(1), în termen de 30 de zile de la intervenirea modificării, prin grija Ministerului Afacerilor Interne, se transmite Comisiei Europene o nouă notificare scrisă.</p>	
<p>Articolul 5 - Responsabilul cu protecția datelor în cadrul UIP</p> <p>(1) UIP numește un responsabil cu protecția datelor pentru monitorizarea prelucrării datelor din PNR și punerea în aplicare a garanțiilor relevante.</p>	<p>&.2 Responsabilul cu protecția datelor în cadrul UNIP</p> <p>Art.8 - Responsabilul cu protecția datelor în cadrul UNIP</p> <p>(1) La nivelul IGPF se înființează funcția de responsabil cu protecția datelor în cadrul UNIP.</p> <p>(2) Responsabilul cu protecția datelor în cadrul UNIP este numit de inspectorul general al IGPF, cu îndeplinirea condițiilor prevăzute la alin.(3).</p> <p>(3) Poate fi desemnat responsabil cu protecția datelor în cadrul UNIP un polițist - funcționar public cu statut special cu studii superioare, care are o experiență de minim doi ani în domeniul protecției datelor cu caracter personal sau care a urmat un curs de specializare în acest domeniu.</p> <p>.....</p> <p>(6) Pentru sprijinirea activității curente a responsabilului cu protecția datelor în cadrul UNIP, la nivelul IGPF se pot înființa una sau mai multe funcții de asistent al responsabilului cu protecția datelor în cadrul UNIP. Alin.(2) se aplică în mod corespunzător.</p> <p>Art.9 - Principalele atribuții ale responsabilului cu protecția datelor în cadrul UNIP</p>	



(1) Responsabilul cu protecția datelor în cadrul UNIP are următoarele atribuții principale:

a) informarea și consilierea personalului UNIP care efectuează prelucrări de date PNR, cu privire la obligațiile care le revin în temeiul legislației privind protecția datelor cu caracter personal;

b) monitorizarea respectării de către UNIP a obligațiilor ce-i revin în conformitate cu dispozițiile legislației privind protecția datelor cu caracter personal și a politicilor UNIP în materia protecției datelor cu caracter personal, în special a alocării responsabilităților, a creșterii gradului de conștientizare a acestora în rândul personalului UNIP și a acțiunilor de formare a personalului implicat în operațiunile de prelucrare;

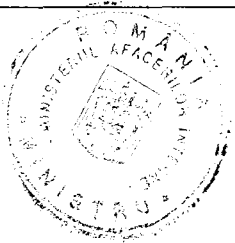
c) realizarea verificărilor necesare în scopul determinării nivelului de respectare a rigorilor impuse de cadrul normativ privind protecția datelor cu caracter personal;

d) furnizarea de consiliere în ceea ce privește evaluarea impactului măsurilor de protecție a datelor cu caracter personal prelucrate în cadrul Sistemului de evidență a datelor PNR și monitorizarea modului în care principiile prelucrării datelor cu caracter personal sunt implementate în cadrul operațiunilor realizate în cadrul UNIP;

e) cooperarea cu Autoritatea națională de supraveghere și îndeplinirea funcției de punct de contact pentru această instituție;

.....

(2) Atunci când în exercitarea atribuțiilor prevăzute la alin.(1) lit.b) și c) constată efectuarea unei operațiuni de prelucrare a datelor cu caracter personal în cadrul Sistemului de evidență a datelor PNR care nu este conformă cu legislația în materia protecției datelor cu caracter personal, responsabilul cu protecția datelor în cadrul UNIP informează conducerea IGPF. În cazul în care pentru remedierea situației nu sunt suficiente măsurile adoptate la nivelul IGPF, responsabilul cu protecția datelor în cadrul UNIP notifică, de îndată, Autoritatea națională de supraveghere.



<p>(2) Statele membre pun la dispoziția responsabililor cu protecția datelor mijloacele necesare pentru ca aceștia să își exercite în mod eficient și independent îndatoririle și atribuțiile în conformitate cu prezentul articol.</p>	<p>.....</p> <p>Art.8 - Responsabilul cu protecția datelor în cadrul UNIP</p> <p>(4) Responsabilul cu protecția datelor în cadrul UNIP își desfășoară activitatea în subordinea nemijlocită a inspectorului general al IGPF. Inspectorul general al IGPF asigură preluarea atribuțiilor responsabilului cu protecția datelor personale în cadrul UNIP, 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.</p> <p>(5) În exercitarea sarcinilor de serviciu privind respectarea legislației în materia protecției datelor cu caracter personal, responsabilul cu protecția datelor în cadrul UNIP este independent și nu poate primi instrucțiuni pe cale ierarhică.</p> <p>.....</p> <p>Art.9 - Principalele atribuții ale responsabilului cu protecția datelor în cadrul UNIP</p> <p>(4) În îndeplinirea atribuțiilor de serviciu, responsabilul cu protecția datelor are drept de acces în încăperile UNIP și la informațiile cuprinse în Sistemul de evidență a datelor PNR, potrivit legii.</p> <p>Art.10 - Asigurarea condițiilor de muncă ale responsabilului cu protecția datelor în cadrul UNIP</p> <p>(1) IGPF pune la dispoziția responsabilului cu protecția datelor în cadrul UNIP dotările tehnice și logistice necesare îndeplinirii atribuțiilor de serviciu, potrivit normelor de dotare aplicabile unei funcții de șef birou.</p> <p>(2) În scopul asigurării exercitării drepturilor de către persoana vizată, IGPF pune la dispoziția responsabilului cu protecția datelor în cadrul UNIP un spațiu special amenajat pentru relații cu publicul.</p> <p>(3) IGPF asigură participarea responsabilului cu protecția datelor</p>	
---	---	--



	<p>în cadrul UNIP la cursuri de instruire de specialitate organizate în Uniunea Europeană, cel puțin o dată la doi ani.</p> <p>(4) Măsurile dispuse la nivelul IGPF cu privire la asigurarea condițiilor de muncă ale responsabilului cu protecția datelor în cadrul UNIP au în vedere asigurarea exercitării în mod eficient și independent de către acesta a atribuțiilor stabilite de prezenta lege.</p>	
<p>(3) Statele membre se asigură că persoana vizată are dreptul de a contacta responsabilul cu protecția datelor, ca punct unic de contact, cu privire la toate aspectele legate de prelucrarea datelor din PNR ale persoanei vizate.</p>	<p>Art.8 - Responsabilul cu protecția datelor în cadrul UNIP </p> <p>(7) Datele de contact ale responsabilului cu protecția datelor în cadrul UNIP, respectiv nume, prenume, adresă poștală, adresă de poștă electronică, telefon și fax se comunică Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, denumită în continuare Autoritatea națională de supraveghere și se publică la avizierul și pe pagina de internet a IGPF.</p> <p>Art.9 - Principalele atribuții ale responsabilului cu protecția datelor în cadrul UNIP</p> <p>(1) Responsabilul cu protecția datelor în cadrul UNIP are următoarele atribuții principale: </p> <p>f) îndeplinirea funcției de punct unic de contact în relația cu persoanele vizate, cu privire la toate aspectele legate de prelucrarea datelor cu caracter personal în cadrul Sistemului de evidență a datelor PNR. </p> <p>(3) Îndeplinirea funcției de punct unic de contact în relația cu persoanele vizate presupune realizarea următoarelor activități principale:</p> <p>a) primirea și înregistrarea într-un registru special a cererilor formulate de către persoanele vizate în exercitarea drepturilor prevăzute de legislația privind protecția datelor cu caracter personal;</p> <p>b) solicitarea realizării de către UNIP a verificărilor necesare</p>	



	<p>pentru soluționarea cererilor prevăzute la lit.a); c) întocmirea răspunsurilor la cererile persoanelor vizate, pe baza rezultatului verificărilor prevăzute la lit.b), și transmiterea acestora către solicitanți.</p>	
<p>Articolul 6 - Prelucrarea datelor din PNR (1) Datele din PNR transferate de către transportatorii aerieni sunt colectate de către UIP a statului membru relevant, astfel cum este prevăzut la articolul 8. În cazul în care datele din PNR transferate de transportatorii aerieni includ date diferite față de cele enumerate în anexa I, UIP șterge aceste date imediat și definitiv la primirea lor.</p>	<p>Art.14 - Datele PNR (3) În cazul în care datele transmise de transportatorii aerieni includ orice date suplimentare față de cele prevăzute la alin.(1), Sistemul de evidență a datelor PNR șterge în mod automat și ireversibil aceste date imediat după primirea lor.</p>	
<p>(2) UIP prelucrează datele din PNR doar în următoarele scopuri: (a) efectuarea unei evaluări a pasagerilor înainte de sosirea sau de plecarea programată a acestora din statul membru, în vederea identificării persoanelor care necesită o examinare suplimentară de către autoritățile competente menționate la articolul 7 și, după caz, de către Europol, în conformitate cu articolul 10, având în vedere faptul că respectivele persoane pot fi implicate într-o infracțiune de terorism sau într-o infracțiune gravă; (b) oferirea de răspunsuri, de la caz la caz, unei cereri temeinic justificate bazate pe motive suficiente din partea autorităților competente vizând furnizarea și prelucrarea datelor din PNR în cazuri specifice în scopul prevenirii, depistării, investigării și urmării penale a infracțiunilor de terorism sau a infracțiunilor grave și comunicarea rezultatelor acestei prelucrări autorităților competente sau, după caz, Europol; și (c) analizarea datelor din PNR în vederea actualizării sau a defnirii de noi criterii ce urmează a fi utilizate pentru evaluările efectuate în temeiul alineatului (3) litera (b) în scopul identificării oricăror persoane care pot fi implicate într-o infracțiune de</p>	<p>&.2 Evaluarea datelor PNR de către UNIP Art.20 - Prelucrarea datelor PNR de către UNIP (1) UNIP prelucrează datele cuprinse în Sistemul de evidență a datelor PNR, exclusiv în următoarele scopuri: a) efectuarea unei evaluări a pasagerilor înainte de sosirea sau de plecarea programată a acestora în/din România, în vederea identificării persoanelor cu privire la care 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 în săvârșirea unei infracțiuni de terorism, a unei infracțiuni grave sau într-o activitate care constituie amenințare la adresa securității naționale; b) oferirea de răspunsuri, de la caz la caz, unei cereri temeinic justificate bazate pe motive suficiente din partea autorităților competente vizând furnizarea și prelucrarea datelor PNR, în cazuri concrete, în scopurile prevăzute la art.18 și comunicarea rezultatelor acestei prelucrări autorităților competente sau, după caz, EUROPOL; c) analizarea datelor PNR în vederea actualizării sau a defnirii de noi criterii ce urmează a fi utilizate pentru evaluările efectuate în</p>	



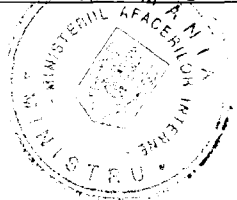
<p>terrorism sau într-o infracțiune gravă.</p>	<p>temeiul alin.(2) lit.(b) în scopul identificării oricăror persoane care pot fi implicate în săvârșirea unei infracțiuni de terorism, a unei infracțiuni grave sau într-o activitate care constituie amenințare la adresa securității naționale.</p> <p>.....</p>	
<p>(3) În momentul efectuării evaluării menționate la alineatul (2) litera (a), UIP poate:</p> <p>(a) să compare datele din PNR cu bazele de date relevante în scopul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de terorism și a infracțiunilor grave, inclusiv cu bazele de date privind persoane sau obiecte căutate sau care fac obiectul unei alerte, în conformitate cu normele Uniunii și cu normele internaționale și naționale aplicabile unor astfel de baze de date; sau</p> <p>(b) să prelucreze date din PNR în conformitate cu anumite criterii prestabilite.</p>	<p>Art.20 - Prelucrarea datelor PNR de către UNIP</p> <p>.....</p> <p>(2) În momentul efectuării evaluării menționate la alin.(1) lit.a), UNIP poate:</p> <p>a) să compare datele PNR cu bazele de date relevante, în scopurile prevăzute la art.18;</p> <p>b) să prelucreze date PNR în conformitate cu anumite criterii prestabilite.</p> <p>(3) În scopul aplicării alin.(2) lit.a), bazele de date relevante se stabilesc prin hotărâre a Guvernului, la propunerea Ministerului Afacerilor Interne.</p>	
<p>(4) Orice evaluare a pasagerilor înainte de sosirea programată în statul membru sau de plecarea programată a acestora din statul membru, efectuată în temeiul alineatului (3) litera (b) pe baza unor criterii prestabilite, se realizează în mod nediscriminatoriu. Respectivul criterii prestabilite trebuie să fie personalizate, proporționale și specifice. Statele membre se asigură că UIP stabilesc aceste criterii și le revizuiesc periodic în cooperare cu autoritățile competente menționate la articolul 7. Aceste criterii nu se întemeiază în niciun caz pe rasa sau originea etnică a unei persoane, opiniile sale politice, religia sau convingerile sale filozofice, apartenența la un sindicat, starea sa de sănătate, viața sexuală sau orientarea sexuală.</p>	<p>Art.21 - Evaluarea datelor PNR potrivit unor criterii prestabilite</p> <p>(1) Criteriile utilizate pentru prelucrarea datelor PNR potrivit art.20 alin.(2) lit.b) se stabilesc și se revizuiesc periodic, de către UNIP în cooperare cu autoritățile competente, respectând următoarele condiții:</p> <p>a) criteriile sunt țintite, proporționale și specifice, raportat la scopurile prevăzute la art.18;</p> <p>b) criteriile nu se întemeiază pe rasa sau originea etnică a unei persoane, opiniile sale politice, religia sau convingerile sale filozofice, apartenența la un sindicat, starea sa de sănătate, viața sexuală sau orientarea sexuală.</p> <p>(2) Orice evaluare a pasagerilor înainte de sosirea/plecarea programată a acestora în/din România, efectuată potrivit art.20 alin.(2) lit.b) pe baza unor criterii prestabilite, se realizează în mod nediscriminatoriu.</p>	



<p>(5) Statele membre se asigură că toate rezultatele pozitive obținute printr-o prelucrare automatizată a datelor din PNR realizată în temeiul alineatului (2) litera (a) sunt reexamine individual prin mijloace neautomatizate pentru a verifica dacă autoritatea competentă menționată la articolul 7 trebuie să aplice măsuri în temeiul dreptului intern.</p>	<p>Art.22 - Utilizarea rezultatelor pozitive ale evaluării datelor PNR</p> <p>(1) Toate rezultatele pozitive obținute printr-o prelucrare automatizată a datelor PNR realizată potrivit art.20 alin.(1) lit.a) sunt reexamine individual prin mijloace neautomatizate, exclusiv de către personalul UNIP, pentru a verifica dacă este necesar transferul respectivelor date PNR către autoritățile competente pentru realizarea unei examinări suplimentare în oricare dintre scopurile prevăzute la art.18 și pentru a determina căror autorități competente să le fie transmise datele PNR, în funcție de atribuțiile stabilite în sarcina acestora de legislația în vigoare.</p> <p>.....</p>	
<p>(6) UIP a unui stat membru transmite datele din PNR ale persoanelor identificate conform alineatului (2) litera (a) sau rezultatul prelucrării datelor respective autorităților competente menționate la articolul 7 ale aceluiași stat membru, pentru examinare suplimentară. Aceste transferuri se fac doar de la caz la caz și, în cazul prelucrării automatizate a datelor din PNR, după reexaminarea individuală prin mijloace neautomatizate.</p>	<p>Art.22 - Utilizarea rezultatelor pozitive ale evaluării datelor PNR</p> <p>.....</p> <p>(2) UNIP transferă către autoritățile competente ale căror atribuții sunt vizate datele PNR sau rezultatul prelucrării datelor PNR în situațiile în care constată că este necesară realizarea unei examinări suplimentare în oricare dintre scopurile prevăzute la art.18. Este interzisă transmiterea către autoritățile competente de date PNR care nu au fost reexamine individual prin mijloace neautomatizate de personalul UNIP.</p>	
<p>(7) Statele membre se asigură că responsabilul cu protecția datelor are acces la toate datele prelucrate de către UIP. În cazul în care responsabilul cu protecția datelor consideră că prelucrarea oricăror date nu a fost legală, acesta poate sesiza în acest sens autoritatea națională de supraveghere.</p>	<p>Art.9 - Principalele atribuții ale responsabilului cu protecția datelor în cadrul UNIP</p> <p>(1) Responsabilul cu protecția datelor în cadrul UNIP are următoarele atribuții principale:</p> <p>a) informarea și consilierea personalului UNIP care efectuează prelucrări de date PNR, cu privire la obligațiile care le revin în temeiul legislației privind protecția datelor cu caracter personal;</p> <p>b) monitorizarea respectării de către UNIP a obligațiilor ce-i revin în conformitate cu dispozițiile legislației privind protecția datelor</p>	



	<p>cu caracter personal și a politicilor UNIP în materia protecției datelor cu caracter personal, în special a alocării responsabilităților, a creșterii gradului de conștientizare a acestora în rândul personalului UNIP și a acțiunilor de formare a personalului implicat în operațiunile de prelucrare;</p> <p>.....</p> <p>(2) Atunci când în exercitarea atribuțiilor prevăzute la alin.(1) lit.b) și c) constată efectuarea unei operațiuni de prelucrare a datelor cu caracter personal în cadrul Sistemului de evidență a datelor PNR care nu este conformă cu legislația în materia protecției datelor cu caracter personal, responsabilul cu protecția datelor în cadrul UNIP informează conducerea IGPF. În cazul în care pentru remedierea situației nu sunt suficiente măsurile adoptate la nivelul IGPF, responsabilul cu protecția datelor în cadrul UNIP notifică, de îndată, Autoritatea națională de supraveghere.</p> <p>.....</p> <p>(4) În îndeplinirea atribuțiilor de serviciu, responsabilul cu protecția datelor are drept de acces în încăperile UNIP și la informațiile cuprinse în Sistemul de evidență a datelor PNR, potrivit legii.</p>	
<p>(8) Stocarea, prelucrarea și analiza datelor din PNR de către UIP se realizează exclusiv într-un loc sigur sau în locuri sigure de pe teritoriul statelor membre.</p>	<p>&.1 Sistemul de evidență a datelor PNR</p> <p>Art.19 - Sistemul de evidență a datelor PNR</p> <p>.....</p> <p>(3) Stocarea, prelucrarea și analiza datelor PNR prin intermediul Sistemului de evidență a datelor PNR se realizează exclusiv într-un spațiu care dispune de infrastructura adecvată pentru asigurarea securității prelucrărilor, în raport cu stadiul evoluției tehnologice, situat pe teritoriul României sau al altui stat membru al Uniunii Europene.</p>	
<p>(9) Consecințele evaluărilor pasagerilor menționate la alineatul (2) litera (a) din prezentul articol nu periclitează dreptul</p>	<p>Art.22 - Utilizarea rezultatelor pozitive ale evaluării datelor PNR</p>	



<p>persoanelor care se bucură de dreptul la liberă circulație pe teritoriul Uniunii de a intra pe teritoriul statului membru respectiv, conform Directivei 2004/38/CE a Parlamentului European și a Consiliului.</p> <p>În plus, atunci când evaluările se efectuează în cazul unor zboruri intra-UE între state membre cărora li se aplică Regulamentul (CE) nr. 562/2006 al Parlamentului European și al Consiliului, consecințele acestor evaluări respectă regulamentul menționat.</p>	<p>.....</p> <p>(4) Rezultatele evaluării pasagerilor potrivit art.20 alin.(1) lit.a) nu pot fi utilizate ca unic motiv pentru limitarea în orice fel a exercitării dreptului la liberă circulație potrivit OUG nr.102/2005 privind libera circulație pe teritoriul României a cetățenilor statelor membre ale Uniunii Europene, Spațiului Economic European și a cetățenilor Confederației Elvețiene, republicată, cu modificările și completările ulterioare.</p> <p>(5) De la data aplicării în totalitate de către România a dispozițiilor acquis-ului Schengen, în temeiul deciziei Consiliului emise în acest sens, în cazul în care evaluarea pasagerilor potrivit art.20 alin.(1) lit.a) privește zboruri intra-UE între România și un alt stat membru care aplică în totalitate dispozițiile acquis-ul Schengen, rezultatele respectivelor evaluări produc efecte cu privire la exercitarea dreptului la liberă circulație a persoanelor numai în condițiile respectării Regulamentului (UE) 2016/399 al Parlamentului European și al Consiliului din 9 martie 2016 cu privire la Codul Uniunii privind regimul de trecere a frontierelor de către persoane (Codul Frontierelor Schengen).</p>	
<p>Articolul 7 - Autorități competente</p> <p>(1) Fiecare stat membru adoptă o listă a autorităților competente îndreptățite să solicite sau să primească date din PNR sau rezultatul prelucrării acestor date de la UIP în vederea examinării suplimentare a acestor informații sau a adoptării măsurilor necesare în vederea prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de terorism sau a infracțiunilor grave.</p> <p>(2) Autoritățile menționate la alineatul (1) sunt autoritățile competente în materie de prevenire, depistare, investigare sau urmărire penală a infracțiunilor de terorism sau a infracțiunilor grave.</p>	<p>&.3 Autoritățile competente</p> <p>Art.11 - Autoritățile competente</p> <p>(1) Autoritățile competente să solicite sau să primească de la UNIP și să utilizeze date PNR sau rezultatul prelucrării datelor PNR în condițiile art.23 sunt următoarele:</p> <ul style="list-style-type: none"> a) Poliția Română; b) Poliția de Frontieră Română; c) Direcția Generală de Protecție Internă; d) Direcția Generală Anticorupție; e) Serviciul Român de Informații; f) Serviciul de Informații Externe; g) Ministerul Apărării Naționale: Direcția generală de informații a apărării; h) Ministerul Public; 	



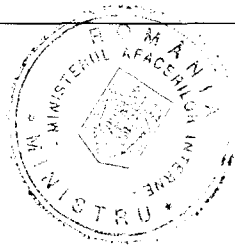
	<p>i) Agenția Națională de Administrare Fiscală: Direcția Generală a Vămilelor.</p> <p>(2) Prin ordine sau dispoziții ale conducătorilor autorităților competente prevăzute la alin.(1) se stabilesc:</p> <p>a) departamentele/structurile din cadrul fiecărei autorități competente abilitate să solicite sau să primească și să prelucreze date PNR;</p> <p>b) persoanele din cadrul departamentelor/structurilor abilitate potrivit lit.a) cu atribuții de prelucrare a datelor PNR;</p> <p>c) limitele concrete în exercitarea atribuțiilor de prelucrare a datelor PNR de către persoanele stabilite potrivit lit.b).</p> <p>(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:</p> <p>a) prelucrarea datelor PNR să fie necesară pentru îndeplinirea atribuțiilor de serviciu;</p> <p>b) datele PNR să fie prelucrate potrivit procedurilor și prin mijloacele prevăzute de dispozițiile legale aplicabile activităților în cadrul cărora sunt utilizate datele respective;</p> <p>c) prelucrarea datelor PNR să respecte dispozițiile legale privind protecția datelor cu caracter personal aplicabile activităților în cadrul cărora sunt utilizate datele respective.</p>	
<p>(3) În sensul articolului 9 alineatul (3), fiecare stat membru notifică Comisiei lista autorităților sale competente până la 25 mai 2017, și poate modifica notificarea sa în orice moment. Comisia publică această notificare și orice modificări ale acesteia în Jurnalul Oficial al Uniunii Europene.</p>	<p>Art.12 - Notificarea listei cu autoritățile competente</p> <p>(1) În termen de 30 de zile de la intrarea în vigoare a prezentei legi, prin grija Ministerului Afacerilor Interne, se transmite Comisiei Europene o notificare scrisă privind lista autorităților competente.</p> <p>(2) În cazul modificării situației notificate potrivit alin.(1), prin grija Ministerului Afacerilor Interne, în termen de 30 de zile de la intervenirea modificării, se transmite Comisiei Europene o nouă notificare scrisă.</p>	



<p>(4) Datele din PNR și rezultatul prelucrării acestor date primite de la UIP pot face obiectul unei prelucrări ulterioare de către autoritățile competente ale statelor membre doar în scopul specific al prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor de terorism și a infracțiunilor grave.</p>	<p>&.3 Utilizarea datelor PNR de către autoritățile competente Art.23 - 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 UNIP, 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.18. (2) La nivelul autorităților competente, datele PNR se prelucrează exclusiv de către persoanele desemnate potrivit art.11 alin.(2) lit.b) și în limitele stabilite prin ordinele sau dispozițiile conducătorilor autorităților competente emise în temeiul art.11 alin.(2) lit.c). </p>	
<p>(5) Alineatul (4) nu aduce atingere competențelor naționale de aplicare a legii sau judiciare în cazul în care alte infracțiuni sau indicii privind astfel de infracțiuni sunt depistate în cursul acțiunilor de aplicare a legii, ca urmare a unei astfel de prelucrări.</p>	<p>Art.23 - Utilizarea datelor PNR de către autoritățile competente (3) Dispozițiile alin.(1) nu aduc atingere exercitării atribuțiilor autorităților competente în situațiile în care alte infracțiuni sau indicii privind alte infracțiuni sunt descoperite în cursul aplicării măsurilor dispuse ca urmare a analizării datelor PNR și a rezultatelor prelucrării datelor PNR primite de la UNIP.</p>	
<p>(6) Autoritățile competente nu iau doar pe baza prelucrării automatizate a datelor PNR nicio decizie care produce efecte juridice adverse asupra unei persoane sau care afectează în mod semnificativ o persoană. Astfel de decizii nu se iau pe baza rasei sau originii etnice a unei persoane, a opiniilor sale politice, a religiei sau a convingerilor sale filozofice, a apartenenței la un sindicat, a stării sale de sănătate, a vieții sexuale sau orientării sexuale.</p>	<p>Art.23 - Utilizarea datelor PNR de către autoritățile competente (4) Dispunerea de către autoritățile competente a oricărei măsuri cu caracter obligatoriu împotriva unei persoane exclusiv în baza prelucrării automatizate a datelor PNR ori pe baza rasei sau originii etnice a unei persoane, a opiniilor sale politice, a religiei sau a convingerilor sale filozofice, a apartenenței la un sindicat, a stării sale de sănătate, a vieții sexuale sau orientării sexuale este interzisă.</p>	



<p>Articolul 8 - Obligațiile transportatorilor aerieni privind transferurile de date</p> <p>(1) Statele membre adoptă măsurile necesare pentru a se asigura că transportatorii aerieni transferă, prin „metoda push”, datele din PNR <u>enumerat</u>e în anexa I, în măsura în care aceștia colectează deja astfel de date în cadrul activităților lor obișnuite, către baza de date a UIP a statului membru pe teritoriul căruia va sosi sau de pe teritoriul căruia va pleca zborul.</p> <p>Dacă este vorba de un zbor al cărui cod este partajat de unul sau mai mulți transportatori aerieni, obligația de a transfera datele din PNR ale tuturor pasagerilor aparține transportatorului aerian care operează zborul.</p> <p>În cazul în care un zbor extra-UE are una sau mai multe escale pe aeroporturi din state membre diferite, transportatorii aerieni transferă datele din PNR referitoare la toți pasagerii către UIP din toate statele membre în cauză. Acest lucru este valabil și în cazul în care un zbor intra-UE are una sau mai multe escale pe aeroporturi din state membre diferite, dar numai în ceea ce privește statele membre care colectează date din PNR de la zborurile intra-UE.</p>	<p>CAP. III – Transmiterea datelor PNR de la transportatorii aerieni la UNIP</p> <p>Art.13 - Obligația de transmitere a datelor PNR</p> <p>(1) Transportatorii aerieni transmit corect și complet către UNIP datele PNR prevăzute la art.14 alin.(1) pe care le colectează deja în cadrul activităților lor obișnuite, aferente zborurilor extra-UE și intra-UE pe care le operează.</p> <p>(2) În cazul în care codul de identificare al unui zbor extra-UE sau intra-UE este partajat de unul sau mai mulți transportatori aerieni, obligația prevăzută la alin.(1) revine transportatorului aerian care operează zborul.</p> <p>(3) Obligațiile prevăzute la alin.(1) și (2) se execută și în cazul în care un zbor extra-UE sau intra-UE tranzitează unul sau mai multe aeroporturi din alte state membre ale Uniunii Europene.</p> <p>(4) Este interzisă transmiterea datelor PNR în condițiile prezentei legi către alte autorități sau instituții publice române.</p> <p>Art.14 - Datele PNR</p> <p>(1) Transportatorii aerieni transmit către UNIP, în condițiile prevăzute la art.15 și art.16, următoarele date din registrul cu numele pasagerilor:</p> <ul style="list-style-type: none"> a) codul de rezervare; b) data rezervării sau a emiterii biletului; c) data (datele) programată (programate) a (ale) călătoriei; d) numele și prenumele asociate rezervării; e) adresa și informațiile de contact (număr de telefon, adresă de e-mail) asociate rezervării; f) toate informațiile privind forma de plată, inclusiv adresa de facturare; g) itinerarul complet de călătorie; h) informațiile din profilul „client fidel”; i) agenția sau agentul de turism prin care a fost făcută rezervarea sau a fost cumpărat biletul; 	
---	---	--

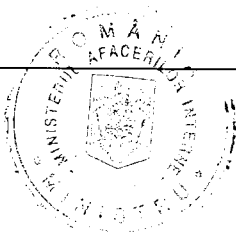


- j) situația de călătorie a pasagerului, inclusiv confirmările, situația înregistrării pentru zbor, informații privind neprezentarea pasagerului la îmbarcare sau privind prezentarea acestuia în ultimul moment la îmbarcare fără rezervare prealabilă;
- k) informațiile scindate sau divizate din registrul cu numele pasagerilor;
- l) mențiunile cu caracter general, inclusiv toate informațiile disponibile despre minorii neînsoțiți cu vârsta sub 18 ani, precum numele 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;
- m) informațiile despre bilet, inclusiv numărul biletului, data emiterii biletului și bilete dus simplu și câmpurile aferente furnizării automate a prețului unui bilet de călătorie;
- n) numărul locului și alte informații privind locul;
- o) informațiile cu privire la codurile partajate;
- p) toate informațiile cu privire la bagaje;
- q) numărul pasagerilor înregistrați în PNR și alte nume ale acestora;
- r) orice date API colectate, inclusiv tipul, numărul, țara de emiterie și data expirării oricărui document de identitate, cetățenia, numele de familie, prenumele, sexul, data nașterii, compania aeriană, numărul zborului, data plecării, data sosirii, aeroportul de plecare, aeroportul de sosire, ora plecării și ora sosirii;
- s) un istoric al tuturor modificărilor datelor PNR prevăzute la lit.a) – r).

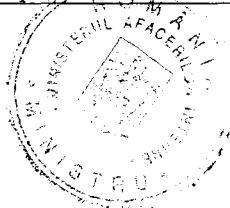
.....

Art.16 - Măsuri tehnice privind transmiterea datelor PNR

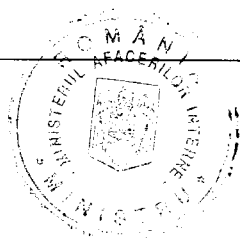
(1) Transportatorii aerieni transmit datele PNR către UNIP, exclusiv prin metoda de tip push, prin mijloace electronice de comunicație capabile să asigure protecția datelor PNR prin



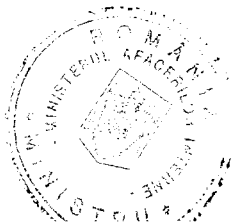
	<p>măsurile tehnice de securitate și prin măsurile organizatorice aplicate transmiterii datelor PNR, sau, în caz de defecțiune tehnică, prin orice alte mijloace de comunicației care asigură același nivel de protecție a datelor PNR, precum și respectarea dispozițiilor legale privind protecția datelor cu caracter personal aplicabile.</p> <p>(2) Până la aplicarea dispozițiilor alin.(3), datele PNR se transmit către UNIP în formatul/formatele de date stabilit/stabilite prin dispoziția inspectorului general al IGPF.</p> <p>.....</p> <p>Art.17 - Monitorizarea respectării obligațiilor aferente transmiterii datelor PNR</p> <p>UNIP monitorizează respectarea obligațiilor transportatorilor aerieni prevăzute la art.13 – 16, fără a aduce atingere atribuțiilor Autorității naționale de supraveghere.</p>	
<p>(2) În cazul în care transportatorii aerieni au colectat date privind informații prelabile referitoare la pasageri (API) enumerate la punctul 18 din anexa I, dar nu păstrează datele respective prin aceleași mijloace tehnice ca alte date din PNR, statele membre adoptă măsurile necesare pentru a se asigura că transportatorii aerieni transferă, prin „metoda push”, datele respective către UIP a statelor membre menționate la alineatul (1). În cazul unui astfel de transfer, toate dispozițiile prezentei directive se aplică în privința respectivelor date API.</p>	<p>Art.14 - Datele PNR</p> <p>.....</p> <p>(2) Datele PNR prevăzute la alin.(1) lit.r) se transmit UNIP în condițiile prezentei legi inclusiv în cazul în care transportatorii aerieni nu le păstrează prin mijloacele tehnice utilizate pentru celelalte date PNR.</p> <p>.....</p>	
<p>(3) Transportatorii aerieni transferă datele din PNR prin mijloace electronice utilizând protocoale comune și formate de date compatibile, care urmează a fi adoptate în conformitate cu procedura de examinare menționată la articolul 17 alineatul (2) sau, în caz de defecțiune tehnică, prin orice alte mijloace adecvate care asigură un nivel adecvat de securitate a datelor:</p> <p>(a) cu 24 până la 48 de ore înainte de ora programată pentru</p>	<p>Art.15 - Momentul transmiterii datelor PNR</p> <p>(1) Transportatorii aerieni transmit datele PNR către UNIP cu 48 până la 24 de ore înainte de ora programată pentru plecarea zborului.</p> <p>(2) Imediat după închiderea zborului, adică imediat după îmbarcarea pasagerilor în aeronava care se pregătește de decolare și când niciun pasager nu se mai poate îmbarca sau nu mai poate</p>	



<p>plecarea zborului; și (b) imediat după închiderea zborului, adică imediat după îmbarcarea pasagerilor în aeronava care se pregătește de decolare și când niciun pasager nu se mai poate îmbarca sau nu mai poate debarca.</p> <p>(4) Statele membre permit transportatorilor aerieni să limiteze transferul menționat la alineatul (3) litera (b) la actualizări ale transferurilor menționate la litera (a) din alineatul respectiv.</p>	<p>debarca, transportatorii aerieni transmit către UNIP toate modificările sau completările intervenite cu privire la datele PNR aferente respectivului zbor de la momentul transmiterii realizate potrivit alin.(1).</p> <p>Art.16 - Măsurile tehnice privind transmiterea datelor PNR (1) Transportatorii aerieni transmit datele PNR către UNIP, exclusiv prin metoda de tip push, prin mijloace electronice de comunicație capabile să asigure protecția datelor PNR prin măsurile tehnice de securitate și prin măsurile 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. (2) Până la aplicarea dispozițiilor alin.(3), datele PNR se transmit către UNIP în formatul/formatele de date stabilit/stabilite prin dispoziția inspectorului general al IGPF.</p>	
<p>(5) Dacă accesul la datele din PNR este necesar pentru a răspunde unei amenințări specifice și reale având legătură cu infracțiuni de terorism sau cu infracțiuni grave, la solicitarea unei UIP efectuată în conformitate cu dreptul intern, transportatorii aerieni transferă de la caz la caz date din PNR în alte momente decât cele menționate la alineatul (3).</p>	<p>Art.15 - Momentul transmiterii datelor PNR</p> <p>(3) În cazul în care evaluarea datelor PNR aferente unui zbor programat este necesară pentru a răspunde unei amenințări concrete privind comiterea unei infracțiuni de terorism sau a unei infracțiuni grave ori pentru prevenirea și înlăturarea unei amenințări la adresa securității naționale, UNIP, exclusiv ca urmare a unei cereri din partea unei autorități competente, solicită transportatorilor aerieni să transmită datele PNR aferente zborului în cauză în alte momente decât cele prevăzute la alin.(1) și (2). (4) Transportatorii aerieni transmit datele PNR către UNIP, în termenul indicat prin solicitarea prevăzută la alin.(3).</p>	



<p>Articolul 9 - Schimbul de informații dintre statele membre</p> <p>(1) Statele membre se asigură că, în ceea ce privește persoanele identificate de o UIP în conformitate cu articolul 6 alineatul (2), toate datele din PNR relevante și necesare sau rezultatul prelucrării respectivelor date este transmis de respectiva UIP către UIP omoloage ale celorlalte state membre. UIP ale statelor membre destinatare transmit informațiile primite către autoritățile lor competente, în conformitate cu articolul 6 alineatul (6).</p>	<p>&.4 Schimbul de date PNR cu alte state membre ale Uniunii Europene</p> <p>Art.24 - Schimbul de date PNR cu alte state membre ale Uniunii Europene prin intermediul UNIP</p> <p>(1) UNIP reprezintă punctul național de contact cu unitățile de informații privind pasagerii, denumite în continuare UIP, ale altor state membre ale Uniunii Europene și este responsabilă pentru schimbul de date PNR cu acestea, potrivit prevederilor prezentei legi.</p> <p>(2) În cazul în care prelucrarea datelor PNR potrivit art.20 alin.(1) conduce la identificarea unor persoane, UNIP 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 națională.</p> <p>(3) În cazul în care primește de la UIP ale altor state membre ale Uniunii Europene date PNR sau rezultatul prelucrării datelor PNR, UNIP le transmite către autoritățile competente respectând dispozițiile art.22 alin.(2).</p> <p>.....</p>	
<p>(2) UIP a unui stat membru are dreptul de a solicita, dacă este necesar, ca UIP a oricărui alt stat membru să îi comunice datele din PNR care sunt păstrate în baza de date a acesteia din urmă și care nu au fost încă depersonalizate prin mascarea elementelor de date în temeiul articolului 12 alineatul (2) și, de asemenea, dacă este necesar, rezultatul oricărei prelucrări a acestora, dacă a fost deja efectuată în temeiul articolului 6 alineatul (2) litera (a). O astfel de solicitare trebuie să fie motivată corespunzător. Aceasta se poate baza pe oricare dintre elementele de date sau o combinație a acestora, după cum consideră necesar UIP solicitantă într-un caz specific de prevenire, depistare, investigare și urmărire penală a infracțiunilor de terorism sau a infracțiunilor grave. UIP comunică informațiile solicitate cât de repede posibil. În cazul în care datele solicitate au fost depersonalizate prin</p>	<p>Art.24 - Schimbul de date PNR cu alte state membre ale Uniunii Europene prin intermediul UNIP</p> <p>.....</p> <p>(4) UNIP poate solicita, în condițiile alin.(5), din proprie inițiativă sau la cererea motivată a unei autorități competente, UIP a altui stat membru al Uniunii Europene să îi comunice date PNR care nu au fost depersonalizate prin mascarea elementelor de date, precum și, dacă este necesar, rezultatele prelucrării respectivelor date PNR.</p> <p>(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 de terorism sau a infracțiunilor grave.</p>	



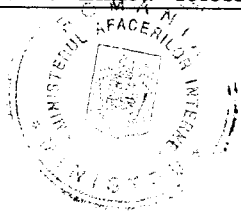
<p>mascarea elementelor de date în conformitate cu articolul 12 alineatul (2), UIP comunică datele din PNR complete numai dacă se consideră în mod rezonabil că este necesar în scopul menționat la articolul 6 alineatul (2) litera (b) și numai dacă este autorizată în acest sens de o autoritate menționată la articolul 12 alineatul (3) litera (b).</p>	<p>(6) În cazul în care primește, din partea UIP a altui stat membru al Uniunii Europene, 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 de terorism sau a infracțiunilor grave, UNIP transmite datele PNR și rezultatul prelucrării datelor PNR, dacă acest rezultat există și a fost solicitat, necesare în respectivul caz concret.</p> <p>(7) UNIP transmite răspunsul la solicitările prevăzute la alin.(6) în cel mai scurt timp posibil. În cazul în care datele solicitate au fost depersonalizate prin mascarea elementelor de date, UNIP comunică datele PNR complete numai dacă sunt prezentate indicii rezonabile că acest lucru este necesar în scopul realizării prelucrării prevăzute la art.20 alin.(1) lit.(b) și numai dacă utilizarea respectivelor date PNR este autorizată potrivit art.31 alin.(1) lit.b).</p> <p>.....</p>	
<p>(3) Autoritățile competente ale unui stat membru pot solicita direct UIP a oricărui alt stat membru să comunice datele din PNR care sunt păstrate în baza de date a acesteia numai atunci când este necesar în cazuri de urgență și în condițiile prevăzute la alineatul (2). Solicitățile din partea autorităților competente trebuie să fie motivate. O copie a solicitării se trimite întotdeauna UIP a statului membru solicitant. În toate celelalte cazuri, autoritățile competente își transmit solicitările prin UIP din propriul stat membru.</p>	<p>Art.24 - Schimbul de date PNR cu alte state membre ale Uniunii Europene prin intermediul UNIP</p> <p>.....</p> <p>(8) Prevederile alin.(6) și (7) se aplică și în cazul în care UNIP primește o solicitare direct din partea unei autorități competente a altui stat membru, dacă solicitarea cuprinde mențiuni din care să rezulte că datele PNR sunt necesare într-un caz urgent.</p> <p>Art.25 - Solicitarea de date PNR de la UIP ale altor state membre ale Uniunii Europene direct de către autoritățile competente</p> <p>(1) Dacă datele PNR sunt necesare într-un caz urgent, autoritățile competente pot transmite direct UIP a altui stat membru 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</p>	



	<p>infrafracțiunilor de terorism sau a infrafracțiunilor grave.</p> <p>(2) Atunci când transmit o solicitare potrivit alin.(1), autoritățile competente transmit o copie a acesteia către UNIP.</p>	
<p>(4) Cu titlu excepțional, în cazul în care accesul la datele din PNR este necesar pentru a răspunde unei amenințări specifice și reale având legătură cu infracțiuni de terorism sau cu infracțiuni grave, UIP a unui stat membru are dreptul de a solicita UIP a unui alt stat membru să obțină date din PNR în conformitate cu articolul 8 alineatul (5) și să le comunice UIP solicitante.</p>	<p>Art.24 - Schimbul de date PNR cu alte state membre ale Uniunii Europene prin intermediul UNIP</p> <p>(9) Cu titlu excepțional, în cazul în care accesul la datele PNR este necesar pentru a răspunde unei amenințări concrete privind comiterea unei infracțiuni de terorism sau a unei infracțiuni grave, UNIP poate solicita UIP a unui alt stat membru al Uniunii Europene să obțină datele PNR aferente unui zbor într-un anumit moment expres indicat și să le comunice UNIP.</p> <p>(10) În cazul în care primește, de la UIP a altui stat membru al Uniunii Europene, 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.15 alin.(1) și (2), UNIP aplică în mod corespunzător dispozițiile art.15 alin.(3) și transmite UIP solicitante datele PNR imediat după obținerea acestora de la transportatorul aerian.</p>	
<p>(5) Schimbul de informații în temeiul prezentului articol se poate derula prin intermediul oricărui canal de cooperare existent între autoritățile competente ale statelor membre. Limba folosită în solicitare și în schimbul de informații este cea aplicabilă canalului utilizat. Atunci când se transmit notificări conform articolului 4 alineatul (5), statele membre informează și Comisia cu privire la coordonatele punctelor de contact cărora le pot fi adresate solicitări în caz de urgență. Comisia comunică aceste detalii statelor membre.</p>	<p>Art.26 - Canale de cooperare pentru schimbul de date PNR cu alte state membre ale Uniunii Europene</p> <p>(1) Schimbul de date PNR cu alte state membre ale Uniunii Europene se poate realiza prin intermediul oricărui canal de cooperare existent între autoritățile competente ale statelor membre ale Uniunii Europene. Limba folosită în solicitare și în schimbul de informații este cea aplicabilă canalului utilizat.</p> <p>(2) Atunci când se transmit notificări potrivit art.6, acestea conțin și informații cu privire la coordonatele punctelor de contact cărora le pot fi adresate solicitări în caz de urgență.</p>	
<p>Articolul 10 - Condițiile de acces al Europol la datele din PNR</p> <p>(1) Europol are competența de a solicita date din PNR sau</p>	<p>&.6 Accesul EUROPOL la datele PNR</p> <p>Art.27 - Accesul EUROPOL la datele PNR</p>	



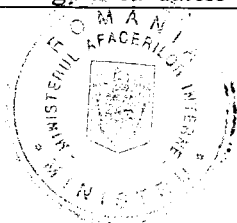
<p>rezultatul prelucrării respectivelor date de la UIP din statele membre, în limitele competențelor sale și în vederea îndeplinirii atribuțiilor sale.</p>	<p>(1) EUROPOL are dreptul de a solicita și de a primi date PNR sau rezultatul prelucrării respectivelor date de la UNIP, în limitele competențelor sale și în vederea îndeplinirii atribuțiilor sale.</p>	
<p>(2) De la caz la caz, Europol poate adresa UIP a oricărui stat membru, prin intermediul unității naționale Europol, o cerere în format electronic și justificată corespunzător de transmitere a unor date specifice din PNR sau a rezultatului prelucrării respectivelor date. Europol poate adresa o astfel de cerere atunci când acest lucru este strict necesar pentru sprijinirea și consolidarea acțiunii statelor membre în vederea prevenirii, depistării sau investigării unei anumite infracțiuni de terorism sau a unei anumite infracțiuni grave, în măsura în care infracțiunea respectivă intră în sfera de competență a Europol, în temeiul Deciziei 2009/371/JAI. Cererea respectivă conține motive rezonabile pe baza cărora Europol consideră că transmiterea datelor din PNR sau a rezultatului prelucrării datelor din PNR va contribui în mod substanțial la prevenirea, depistarea sau investigarea infracțiunii în cauză.</p>	<p>Art.27 - Accesul EUROPOL la datele PNR (2) De la caz la caz, EUROPOL poate adresa UNIP, prin intermediul Unității Naționale Europol, o cerere în format electronic, 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 Uniunii Europene în vederea prevenirii, depistării sau investigării unei anumite infracțiuni de terorism 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.</p>	
<p>(3) Europol informează responsabilul cu protecția datelor, numit în conformitate cu articolul 28 din Decizia 2009/371/JAI, în legătură cu toate schimburile de informații în temeiul prezentului articol.</p>		
<p>(4) Schimbul de informații în temeiul prezentului articol are loc prin intermediul SIENA și în conformitate cu Decizia 2009/371/JAI. Limba folosită în cerere și în schimbul de</p>	<p>Art.27 - Accesul EUROPOL la datele PNR (5) Schimbul de informații în temeiul prezentului articol are loc</p>	



<p>informații este cea aplicabilă SIENA.</p>	<p>prin intermediul SIENA și în conformitate cu legislația Uniunii Europene care stabilește organizarea și atribuțiile EUROPOL. Limba folosită în cerere și în schimbul de informații este cea aplicabilă SIENA.</p>	
<p>Articolul 11 - Transferul datelor către țări terțe (1) Un stat membru poate transfera unei țări terțe date din PNR și rezultatul prelucrării acestor date, care sunt stocate de UIP în conformitate cu articolul 12, doar de la caz la caz și dacă: (a) sunt îndeplinite condițiile prevăzute la articolul 13 din Decizia-cadru 2008/977/JAI; (b) transferul este necesar în scopul prezentei directive menționat la articolul 1 alineatul (2); (c) țara terță este de acord să transfere datele unei alte țări terțe doar în cazul în care acest lucru este strict necesar în scopul prezentei directive menționat la articolul 1 alineatul (2) și doar cu autorizarea expresă a statului membru respectiv; și (d) sunt îndeplinite aceleași condiții ca cele prevăzute la articolul 9 alineatul (2).</p>	<p>&.7 Schimbul de date PNR cu țări terțe Art.28 - Transferul datelor PNR către țări terțe (1) UNIP poate transfera date PNR sau rezultatul prelucrării datelor PNR către autoritățile unei țări terțe doar de la caz la caz și dacă sunt îndeplinite în mod cumulativ următoarele condiții: a) sunt respectate dispozițiile art.15 din Legea nr.238/2009 privind reglementarea prelucrării datelor cu caracter personal de către structurile/unitățile Ministerului Afacerilor Interne în activitățile de prevenire, cercetare și combatere a infracțiunilor, precum și de menținere și asigurare a ordinii publice, republicată; b) transferul este necesar în scopul prevenirii, depistării sau investigării 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 sau cu o măsură de siguranță privativă de libertate a cărei durată maximă este de cel puțin 3 ani și care este corespunzătoare uneia dintre formele de criminalitate prevăzute în Anexa la prezenta lege; c) autoritatea din țara terță comunică în scris că este de acord să transfere datele PNR unei alte țări terțe doar în cazul în care acest lucru este strict necesar în scopul prevăzut la lit.b) și doar cu autorizarea expresă a UNIP; d) sunt îndeplinite condițiile prevăzute la art.24 alin.(5) - (7), care se aplică în mod corespunzător; e) nu este afectată securitatea națională. </p>	
<p>(2) În pofida articolului 13 alineatul (2) din Decizia-cadru 2008/977/JAI, transferurile de date din PNR fără consimțământul prealabil al statului membru de la care sunt obținute datele este</p>	<p>Art.28 - Transferul datelor PNR către țări terțe (2) Prin derogare de la dispozițiile art.15 alin.(2) din Legea</p>	



<p>permis în circumstanțe excepționale și numai dacă:</p> <p>(a) astfel de transferuri sunt esențiale pentru a răspunde unei amenințări specifice și reale, având legătură cu infracțiuni de terorism sau cu infracțiuni grave, la adresa unui stat membru sau a unei țări terțe; și</p> <p>(b) consimțământul prealabil nu poate fi obținut în timp util. Autoritatea responsabilă de acordarea consimțământului este informată fără întârziere, iar transferul este înregistrat în mod corespunzător și face obiectul unei verificări ulterioare.</p>	<p>nr.238/2009, republicată, transferurile de date PNR fără consimțământul prealabil al UIP a statului membru al Uniunii Europene de la care au fost obținute datele este permis în circumstanțe excepționale și numai dacă sunt îndeplinite cumulativ următoarele condiții:</p> <p>a) transferul este esențial pentru a răspunde unei amenințări concrete, având legătură cu infracțiuni de terorism sau cu infracțiuni grave, la adresa unui stat membru al Uniunii Europene sau a unei țări terțe;</p> <p>b) consimțământul prealabil nu poate fi obținut în timp util.</p> <p>(3) În situația în care aplică dispozițiile alin.(2), UNIP informează fără întârziere UIP a statului membru al Uniunii Europene de la care provin datele PNR, iar transferul este înregistrat în mod corespunzător și face obiectul unei verificări ulterioare.</p> <p>.....</p>	
<p>(3) Statele membre transferă date din PNR autorităților competente din țările terțe numai în condiții conforme cu prezenta directivă și numai după ce se asigură că destinatarii intenționează să utilizeze datele din PNR în conformitate cu condițiile și garanțiile respective.</p>	<p>Art.28 - Transferul datelor PNR către țări terțe</p> <p>.....</p> <p>(4) UNIP transferă date PNR autorităților competente din țările terțe numai în condiții conforme cu prezenta lege și numai după ce destinatarii notifică în scris faptul că intenționează să utilizeze datele PNR în conformitate cu condițiile și garanțiile prevăzute de prezenta lege.</p> <p>.....</p>	
<p>(4) Responsabilul cu protecția datelor din UIP a statului membru care a transferat datele din PNR este informat de fiecare dată când statul membru transferă datele din PNR în temeiul prezentului articol.</p>	<p>Art.28 - Transferul datelor PNR către țări terțe</p> <p>.....</p> <p>(5) Responsabilul cu protecția datelor în cadrul UNIP este informat de fiecare dată când UNIP transferă date PNR în temeiul prezentului articol.</p>	
<p>Articolul 12 - Perioada de păstrare a datelor și depersonalizarea</p> <p>(1) Statele membre se asigură că datele din PNR furnizate de</p>	<p>&.8 Păstrarea datelor PNR</p> <p>Art.30 - Perioada de păstrare a datelor PNR și depersonalizarea</p>	



<p>transportatorii aerieni UIP sunt păstrate într-o bază de date la UIP pentru o perioadă de cinci ani după transferul lor către UIP a statului membru pe teritoriul căruia sosește sau de pe teritoriul căruia pleacă zborul.</p>	<p>(1) Datele PNR furnizate de transportatorii aerieni se păstrează în cadrul Sistemului de evidență a datelor PNR pentru o perioadă de cinci ani de la momentul finalizării transmisiunii active a respectivelor date PNR din sistemele transportatorilor aerieni în Sistemul de evidență a datelor PNR, denumit în continuare momentul furnizării.</p> <p>.....</p>	
<p>(2) La expirarea unei perioade de șase luni de la transferul datelor din PNR, menționat la alineatul (1), toate datele din PNR se depersonalizează prin mascarea următoarelor elemente de date care ar putea servi la identificarea directă a pasagerului la care se referă datele din PNR:</p> <p>(a) numele, inclusiv numele altor pasageri din PNR precum și numărul călătorilor din PNR care călătoresc împreună;</p> <p>(b) adresa și informațiile de contact;</p> <p>(c) toate informațiile privind plata, inclusiv adresa de facturare, în măsura în care acestea conțin informații care ar putea servi la identificarea directă a pasagerului la care se referă PNR sau a oricăror altor persoane;</p> <p>(d) informațiile din profilul „client fidel” („frequent flyer”);</p> <p>(e) mențiuni cu caracter general, în măsura în care acestea conțin informații care ar putea servi la identificarea directă a pasagerului la care se referă PNR; și</p> <p>(f) orice date API care au fost colectate.</p>	<p>Art.30 - Perioada de păstrare a datelor PNR și depersonalizarea</p> <p>.....</p> <p>(2) La împlinirea unui termen de 6 luni de la momentul furnizării datelor PNR de către transportatorii aerieni, acestea sunt depersonalizate prin mascarea următoarelor elemente de date:</p> <p>a) numele, inclusiv numele altor pasageri precum și numărul pasagerilor care călătoresc împreună;</p> <p>b) adresa și informațiile de contact asociate rezervării;</p> <p>c) toate informațiile privind forma de plată, inclusiv adresa de facturare;</p> <p>d) informațiile din profilul „client fidel”;</p> <p>e) mențiunile cu caracter general prevăzute la art.14 alin.(1) lit.1);</p> <p>f) orice date API colectate.</p> <p>.....</p>	



<p>(3) După expirarea perioadei de șase luni menționată la alineatul (2), dezvăluirea datelor complete din PNR este permisă numai dacă:</p> <p>(a) se consideră în mod rezonabil că este necesară în scopul menționat la articolul 6 alineatul (2) litera (b); și</p> <p>(b) este aprobată de către:</p> <p>(i) o autoritate judiciară; <u>sau</u></p> <p>(ii) o altă autoritate națională competentă, în temeiul dreptului intern, să verifice dacă sunt îndeplinite condițiile pentru dezvăluire, sub rezerva informării responsabilului cu protecția datelor din cadrul UIP și a revizuirii ulterioare de către acesta.</p>	<p>Art.31 - Utilizarea datelor PNR după depersonalizarea prin mascarea unor elemente de date</p> <p>(1) După împlinirea termenului prevăzut la art.30 alin.(2), dezvăluirea datelor PNR complete este permisă numai dacă:</p> <p>a) există indicii că dezvăluirea datelor PNR complete este necesară în scopul prevăzut la art.20 alin.(1) lit.b);</p> <p>b) dezvăluirea este aprobată de către inspectorul general al IGPF.</p> <p>(2) Inspectorul general al IGPF aprobă dezvăluirea datelor PNR complete în condițiile alin.(1) lit.a) și dacă responsabilul cu protecția datelor din cadrul UNIP a fost informat în prealabil cu privire la solicitarea dezvăluirii datelor PNR complete.</p> <p>(3) Aprobarea inspectorului general al IGPF este revizuită ulterior de către responsabilul cu protecția datelor din cadrul UNIP.</p>	
<p>(4) Statele membre asigură ștergerea definitivă a datelor din PNR după expirarea perioadei menționate la alineatul (1). Această obligație nu aduce atingere cazurilor în care date specifice din PNR au fost transferate unei autorități competente și sunt utilizate în contextul unor cazuri specifice în scopul prevenirii, depistării, investigării sau urmării penale a infracțiunilor de terorism sau a infracțiunilor grave, când păstrarea acestor date de către autoritatea competentă este reglementată de dreptul intern.</p>	<p>Art.30 - Perioada de păstrare a datelor PNR și depersonalizarea</p> <p>.....</p> <p>(3) La împlinirea termenului prevăzut la alin.(1), datele PNR din sistemul de evidență a datelor PNR se șterg în mod automat, printr-o procedură ireversibilă.</p> <p>(4) Dispozițiile alin.(3) nu afectează stocarea, de către autoritățile competente, a datelor PNR transferate la acestea de către UNIP și prelucrate în cazuri concrete în scopurile prevăzute la art.18. Păstrarea datelor PNR de către autoritățile competente respectă regimul juridic aplicabil cazului concret în care au fost prelucrate.</p> <p>.....</p>	
<p>(5) Rezultatul prelucrării menționate la articolul 6 alineatul (2) litera (a) este păstrat de UIP numai pentru perioada necesară pentru informarea autorităților competente și, în conformitate cu articolul 9 alineatul (1), informarea UIP ale altor state membre cu privire la un rezultat pozitiv. În cazul în care rezultatul unei prelucrări automatizate s-a dovedit negativ, după o reexaminare individuală prin mijloace neautomatizate astfel cum se</p>	<p>Art.30 - Perioada de păstrare a datelor PNR și depersonalizarea</p> <p>.....</p> <p>(5) Rezultatele prelucrării efectuate potrivit art.20 alin.(1) lit.a) se păstrează de către UNIP numai pentru perioada necesară transferului acestora către autoritățile competente potrivit art.22 alin.(2) sau către UIP ale celorlalte state membre potrivit art.24</p>	



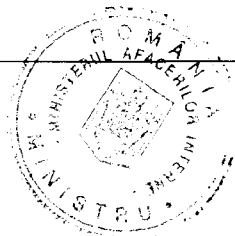
<p>menționează la articolul 6 alineatul (5), acesta poate fi, totuși, stocat pentru a se evita viitoare răspunsuri pozitive „false” pe durata în care datele de bază nu sunt șterse în temeiul alineatului (4) din prezentul articol.</p>	<p>alin.(2). (6) În cazul în care, urmare reexaminării individuale prin mijloace neautomatizate potrivit art.22 alin.(1) se stabilește că rezultatul prelucrării efectuate potrivit art.20 alin.(1) lit.a) nu este necesar a fi transferat autorităților competente pentru efectuarea unei examinări suplimentare, acesta poate fi stocat până la împlinirea termenului prevăzut la alin.(1) pentru datele PNR în cauză, pentru a fi folosit la identificarea facilă a viitoarelor rezultate care nu necesită o examinare suplimentară din partea autorităților competente. </p>	
<p>Articolul 13 - Protecția datelor cu caracter personal (1) Fiecare stat membru se asigură că, în ceea ce privește toate prelucrările de date cu caracter personal în temeiul prezentei directive, fiecare pasager are același drept la protecția datelor sale cu caracter personal, drepturi la acces, rectificare, ștergere sau restricționare și drepturile de a fi despăgubit și de a exercita o cale de atac, în conformitate cu dreptul Uniunii și cu dreptul intern și în aplicarea articolelor 17, 18, 19 și 20 din Decizia-cadru 2008/977/JAI. Articolele respective sunt, prin urmare, aplicabile.</p>	<p>Art.33 - Exercițarea drepturilor persoanei vizate în contextul prelucrării datelor cu caracter personal în cadrul Sistemului de evidență a datelor PNR (1) Drepturile persoanei vizate în contextul prelucrării datelor cu caracter personal în cadrul Sistemului de evidență a datelor PNR se exercită potrivit Legii nr.677/2001, cu modificările și completările ulterioare, cu aplicarea art.24-28 din Legea nr.238/2009, republicată și a alin.(2)-(6). (2) Cererile formulate în exercitarea drepturilor persoanelor vizate se adresează numai UNIP. O cerere este validă numai în situația în care persoana vizată face dovada identității în condițiile legii. (3) Pentru a comunica solicitantului informații cu privire la datele cu caracter personal prelucrate în cadrul Sistemului de evidență a datelor PNR, în situația prelucrărilor prevăzute la art.24-29, UNIP solicită, după caz, acordul autorităților competente către care au fost transferate datele, acordul EUROPOL sau acordul entităților similare din străinătate care a furnizat datele. (4) Autoritățile competente comunică opțiunea în termen de 20 de zile de la data primirii solicitării din partea UNIP. (5) În situația în care entitatea similară din străinătate consultată potrivit alin.(3) nu comunică un răspuns în considerarea termenelor de răspuns la cererile persoanelor vizate, UNIP</p>	



	<p>răspunde solicitantului fără a indica proveniența datelor.</p> <p>(6) În situația în care o entitate similară din străinătate solicită UNIP, în urma transmiterii unor date PNR, acordul pentru comunicarea unor informații solicitate de persoana vizată, UNIP comunică acordul în termen de 30 de zile de la primirea solicitării sau, după caz, în termenul indicat de entitatea solicitantă. Dacă datele au fost transferate unei autorități competente, înainte de a transmite răspunsul către entitatea similară din străinătate, UNIP consultă respectiva autoritate competentă indicând și eventualul termen precizat de entitatea solicitantă.</p>	
<p>(2) Fiecare stat membru se asigură că dispozițiile adoptate în temeiul dreptului intern în aplicarea articolelor 21 și 22 din Decizia-cadru 2008/977/JAI privind confidențialitatea prelucrării și securitatea datelor se aplică, de asemenea, tuturor prelucrărilor de date cu caracter personal în temeiul prezentei directive.</p>	<p>Art.34 - Confidențialitatea și securitatea prelucrărilor</p> <p>(1) Asigurarea confidențialității și securității prelucrării datelor cu caracter personal în cadrul Sistemului de evidență a datelor PNR se realizează potrivit art.19 și 20 din Legea nr.677/2001, cu modificările și completările ulterioare.</p> <p>(2) Este interzisă prelucrarea datelor PNR prin intermediul persoanelor împuternicite de către operator, în sensul art.3 lit.f) din Legea nr.677/2001, cu modificările și completările ulterioare.</p> <p>(3) Operatorul prevăzut la art.32 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 de evidență a datelor PNR, ținând seama de riscurile asociate prelucrării datelor PNR și de natura respectivelor date.</p>	
<p>(3) Prezenta directivă nu aduce atingere aplicabilității Directivei 95/46/CE a Parlamentului European și a Consiliului în ceea ce privește prelucrarea datelor cu caracter personal de către transportatorii aerieni, în special obligația acestora de a lua măsuri tehnice și organizatorice adecvate pentru a proteja securitatea și confidențialitatea datelor cu caracter personal.</p>	<p>Art.40 - Obligațiile transportatorilor aerieni privind protecția datelor cu caracter personal</p> <p>(1) Prezenta lege nu poate fi interpretată în sensul modificării în orice fel a obligațiilor ce revin transportatorilor aerieni potrivit dispozițiilor legale din domeniul protecției datelor cu caracter personal aplicabile acestora.</p> <p>(2) În cadrul activităților necesare pentru transmiterea datelor PNR către UNIP, transportatorii aerieni rămân responsabili, în temeiul</p>	



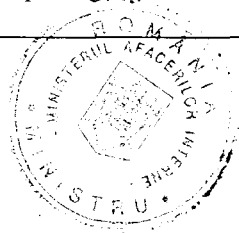
	<p>dispozițiilor legale din domeniul protecției datelor cu caracter personal aplicabile acestora, în ceea ce privește:</p> <p>a) adoptarea măsurilor tehnice și organizatorice necesare pentru asigurarea protecției datelor PNR împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, precum și împotriva oricărei alte forme de prelucrare ilegală;</p> <p>b) prelucrarea datelor PNR în mod legal, echitabil și transparent față de persoana vizată, inclusiv informarea pasagerilor, prealabilă colectării datelor PNR, cu privire la faptul că acestea sunt transmise către UNIP;</p> <p>c) colectarea datelor PNR în scopuri determinate, explicite și legitime și abținerea de la prelucrarea ulterioară într-un mod incompatibil cu aceste scopuri;</p> <p>d) colectarea de date PNR adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate;</p> <p>e) prelucrarea de date PNR exacte și actualizate;</p> <p>f) păstrarea datelor PNR într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate.</p>	
<p>(4) Statele membre interzic prelucrarea datelor din PNR care dezvăluie rasa sau originea etnică, opiniile politice, religia sau convingerile filozofice, apartenența la un sindicat, sănătatea, viața sexuală sau orientarea sexuală a unei persoane. În situația în care UIP primește date din PNR care dezvăluie astfel de informații, acestea sunt șterse imediat.</p>	<p>Art.35 - Interzicerea prelucrării categoriilor speciale de date cu caracter personal</p> <p>(1) Prelucrarea datelor PNR care dezvăluie originea rasială sau etnică, opiniile politice, religia sau convingerile filozofice, apartenența la un sindicat, sănătatea, viața sexuală sau orientarea sexuală este interzisă.</p> <p>(2) În cazul în care datele PNR transmise de transportatorii aerieni cuprind informații din categoriile prevăzute la alin.(1), personalul UNIP șterge în mod ireversibil respectivele informații imediat după identificarea acestora în Sistemul de evidență a datelor PNR.</p> <p>(3) Prelucrarea datelor PNR după criteriile legate de categoriile de informații prevăzute la alin.(1) este interzisă.</p>	



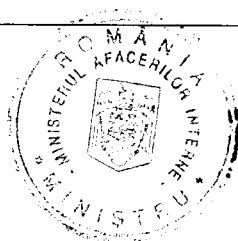
<p>(5) Statele membre se asigură că UIP păstrează documentația referitoare la toate sistemele și procedurile de prelucrare aflate în responsabilitatea sa. Această documentație conține cel puțin:</p> <p>(a) numele și datele de contact ale organizației și ale personalului UIP care are sarcina de a prelucra datele din PNR și diferitele niveluri de autorizare a accesului;</p> <p>(b) cererile depuse de autoritățile competente și UIP ale altor state membre;</p> <p>(c) toate cererile de date din PNR și transferurile de aceste date către o țară terță.</p> <p>La cerere, UIP pune toată documentația la dispoziția autorității naționale de supraveghere.</p>	<p>Art.36 - Evidența activităților de prelucrare</p> <p>(1) UNIP păstrează o evidență a tuturor categoriilor de activități de prelucrare a datelor PNR aflate în responsabilitatea sa. Această evidență cuprinde următoarele informații:</p> <p>a) numele și datele de contact ale instituției și ale personalului care are sarcina de a prelucra datele PNR și diferitele niveluri de autorizare a accesului;</p> <p>b) cererile depuse de autoritățile competente și UIP ale altor state membre;</p> <p>c) cererile de date PNR și transferurile de asemenea date către o țară terță.</p> <p>(2) Evidența prevăzută la alin.(1) se pune la dispoziția Autorității naționale de supraveghere, la cererea acesteia.</p>	
<p>(6) Statele membre se asigură că UIP păstrează înregistrări cel puțin pentru următoarele operațiuni de prelucrare: colectarea, consultarea, dezvăluirea și ștergerea. Înregistrările operațiunilor de consultare și de dezvăluire indică, în special, scopul, data și ora acestor operațiuni și, în măsura în care este posibil, identitatea persoanei care a consultat sau a dezvăluit datele din PNR și identitatea destinatarilor acestor date. Înregistrările sunt utilizate exclusiv în scopul verificării și al automonitorizării, pentru asigurarea integrității și securității datelor sau pentru audit. La cerere, UIP pune înregistrările la dispoziția autorității naționale de supraveghere.</p> <p>Înregistrările respective sunt păstrate pentru o perioadă de cinci ani.</p>	<p>Art.37 - Trasabilitatea prelucrărilor</p> <p>(1) Sistemul de evidență a datelor PNR asigură trasabilitatea prelucrărilor efectuate la nivelul UNIP, 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 UNIP.</p> <p>(2) Sistemul de evidență a datelor PNR asigură cel puțin trasabilitatea operațiunilor de colectare, consultare, dezvăluire și ștergere.</p> <p>(3) Fișierul de trasabilitate generat de Sistemul de evidență a datelor PNR trebuie să conțină cel puțin următoarele informații:</p> <p>a) scopul prelucrării;</p> <p>b) data și ora operațiunilor de prelucrare;</p> <p>c) utilizatorul;</p> <p>d) destinatarul datelor PNR, atunci când este cazul;</p> <p>e) datele accesate și categoria de operațiune efectuată asupra datelor, potrivit art.3 lit.b) din Legea nr.677/2001, cu modificările și completările ulterioare.</p> <p>(4) Fișierele de trasabilitate generate de Sistemul de evidență a datelor PNR pot fi accesate doar pentru următoarele scopuri:</p>	



	<p>a) verificarea și monitorizarea legalității efectuării prelucrărilor;</p> <p>b) asigurarea funcționării tehnice corespunzătoare a Sistemului de evidență a datelor PNR;</p> <p>c) asigurarea integrității și securității datelor PNR.</p> <p>(5) Utilizarea fișierelor de trasabilitate generate de către Sistemul de evidență a datelor PNR în alte scopuri decât cele prevăzute la alin.(4) este interzisă.</p> <p>(6) Fișierele de trasabilitate generate de către Sistemul de evidență a datelor PNR se păstrează pentru o perioadă de cinci ani și se pun la dispoziția Autorității naționale de supraveghere, la cererea acestora.</p>	
<p>(7) Statele membre se asigură că UIP pune în aplicare măsurile și procedurile tehnice și organizatorice adecvate pentru a garanta un nivel ridicat de securitate, adaptat la riscurile reprezentate de prelucrare și de natura datelor din PNR.</p>	<p>Art.34 - Confidențialitatea și securitatea prelucrărilor</p> <p>(1) Asigurarea confidențialității și securității prelucrării datelor cu caracter personal în cadrul Sistemului de evidență a datelor PNR se realizează potrivit art.19 și 20 din Legea nr.677/2001, cu modificările și completările ulterioare.</p> <p>(2) Este interzisă prelucrarea datelor PNR prin intermediul persoanelor împuternicite de către operator, în sensul art.3 lit.f) din Legea nr.677/2001, cu modificările și completările ulterioare.</p> <p>(3) Operatorul prevăzut la art.32 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 de evidență a datelor PNR, ținând seama de riscurile asociate prelucrării datelor PNR și de natura respectivelor date.</p>	
<p>(8) Statele membre se asigură că, atunci când o încălcare a securității datelor cu caracter personal ar putea prezenta un risc ridicat pentru protecția datelor cu caracter personal sau ar afecta viața privată a persoanei vizate, UIP comunică fără întârzieri nejustificate această încălcare persoanei vizate și autorității naționale de supraveghere.</p>	<p>Art.39 - Notificarea autorității naționale de supraveghere în cazul încălcării securității datelor</p> <p>(1) UNIP notifică Autoritatea națională de supraveghere de îndată, dar nu mai târziu de 24 de ore, de la constatare, încălcarea securității datelor cu caracter personal din cadrul Sistemului de evidență a datelor PNR, cu excepția cazului în care încălcarea securității datelor nu este susceptibilă să genereze un risc la adresa</p>	



	<p>drepturilor și libertăților persoanelor fizice.</p> <p>(2) În situația în care nu este posibilă notificarea în termenul prevăzut la alin.(1), notificarea se transmite în termen de 72 de ore de la constatarea încălcării securității datelor, însoțită de o justificare a întârzierii.</p> <p>(3) Notificarea prevăzută la alin.(1) trebuie să conțină cel puțin:</p> <ul style="list-style-type: none">a) o descriere a caracterului încălcării securității datelor cu caracter personal prelucrate în cadrul Sistemului de evidență a datelor PNR, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ de persoane vizate 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 UNIP sau un 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. <p>(4) UNIP 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.</p> <p>(5) În cazul în care încălcarea securității datelor implică date cu caracter personal care au fost transmise de un operator dintr-un alt stat membru sau către un astfel de operator, informațiile prevăzute la alin.(3) se comunică de îndată operatorului respectiv.</p> <p>(6) 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, de îndată, persoana vizată cu privire la încălcarea securității datelor cu</p>	
--	---	--



	<p>caracter personal.</p> <p>(7) Informarea persoanei vizate, prevăzută la alin.(6), nu este necesară în cazul în care este îndeplinită oricare dintre următoarele condiții:</p> <p>a) operatorul a pus în aplicare măsuri tehnologice și organizatorice adecvate de protecție, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securității datelor cu caracter personal, 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;</p> <p>b) operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat la adresa drepturilor și libertăților persoanelor vizate nu mai este susceptibil să se materializeze;</p> <p>c) notificarea ar necesita un efort disproporționat;</p> <p>d) contactarea persoanei vizate nu este posibilă.</p> <p>(8) În cazul prevăzut la alin.(7) lit.c) informarea persoanei vizate se înlocuiește cu o informare publică sau o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficace.</p>	
<p>Articolul 14 - Sancțiuni</p> <p>Statele membre stabilesc norme privind sancțiunile care se aplică în cazul nerespectării dispozițiilor naționale adoptate în temeiul prezentei directive și iau toate măsurile necesare pentru a asigura aplicarea acestora.</p> <p>În special, statele membre stabilesc norme privind sancțiuni, inclusiv sancțiuni financiare, împotriva transportatorilor aerieni care nu transmit datele astfel cum este prevăzut la articolul 8 sau nu fac acest lucru în formatul cerut.</p> <p>Sancțiunile prevăzute trebuie să fie eficace, proporționale și cu efect de descurajare.</p>	<p>CAP. V – Regimul sancționator</p> <p>Art.42 - Contravenții și sancțiuni</p> <p>(1) Constituie contravenții, dacă nu sunt săvârșite în astfel de condiții încât să constituie infracțiuni, următoarele fapte:</p> <p>a) neîndeplinirea de către transportatorii aerieni a obligațiilor ce le revin potrivit art.13;</p> <p>b) nerespectarea de către transportatorii aerieni a termenelor prevăzute la art.15;</p> <p>c) neîndeplinirea de către transportatorii aerieni a obligațiilor ce le revin potrivit art.16.</p> <p>(2) Contravențiile prevăzute la alin. (1) se sancționează după cum urmează:</p> <p>a) cu amendă de la 25.000 la 50.000 lei, contravențiile prevăzute la lit.a) și c).</p> <p>b) cu amendă de la 10.000 la 25.000 lei, contravenția prevăzută la</p>	



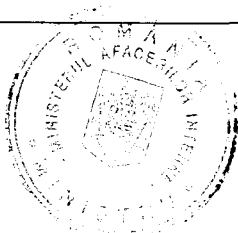
	<p>lit.b);</p> <p>(3) Dacă, în decurs de un an de la data constatării și aplicării sancțiunii pentru una dintre faptele prevăzute la alin.(1), transportatorul aerian săvârșește o nouă contravenție prevăzută de prezenta lege, limitele amenzilor prevăzute la alin.(2) se dublează.</p> <p>(4) Constatarea contravențiilor și aplicarea sancțiunilor se realizează după cum urmează:</p> <p>a) de către personalul din cadrul UNIP cu atribuții în acest scop, pentru contravențiile prevăzute la alin.(1) lit.a) și b);</p> <p>b) de către personalul Autorității naționale de supraveghere cu atribuții în acest scop, pentru contravenția prevăzută la alin.(1) lit.c).</p> <p>(5) Contravențiilor prevăzute de prezenta lege le sunt aplicabile prevederile Ordonanței Guvernului nr.2/2001 privind regimul juridic al contravențiilor, aprobată cu modificări și completări prin Legea nr. 180/2002, cu modificările și completările ulterioare.</p>	
<p>Articolul 15 - Autoritatea națională de supraveghere</p> <p>(1) Fiecare stat membru prevede că autoritatea națională de supraveghere menționată la articolului 25 din Decizia-cadru 2008/977/JAI este responsabilă de <u>consilierea</u> privind aplicarea pe teritoriul său a dispozițiilor adoptate de statele membre în temeiul prezentei directive, precum și de monitorizarea respectivei aplicări. Se aplică articolul 25 din Decizia-cadru 2008/977/JAI.</p> <p>(2) Respectivele autorități naționale de supraveghere își desfășoară activitățile de la alineatul (1) urmărind protejarea drepturilor fundamentale legate de prelucrarea datelor cu caracter personal.</p>	<p>Art.41 - Monitorizarea aplicării actului normativ</p> <p>(1) Prelucrarea datelor cu caracter personal în cadrul Sistemului de evidență a datelor PNR, inclusiv transferul acestor date în străinătate, sunt monitorizate și se supun controlului Autorității naționale de supraveghere.</p> <p>.....</p> <p>(3) Autoritatea națională de supraveghere auditează sistematic operațiunile de prelucrare a datelor cu caracter personal efectuate la nivelul UNIP.</p> <p>(4) Autoritatea națională de supraveghere oferă consiliere oricărei persoane vizate, la cererea acesteia, cu privire la exercitarea drepturilor sale în contextul prelucrării datelor cu caracter personal în cadrul Sistemului de evidență a datelor PNR.</p>	
<p>(3) Fiecare autoritate națională de supraveghere are următoarele îndatoriri:</p> <p>(a) tratează plângerile depuse de orice persoană vizată,</p>	<p>Art.41 - Monitorizarea aplicării actului normativ</p> <p>.....</p> <p>(2) Pentru realizarea monitorizării și controlului prevăzut la</p>	



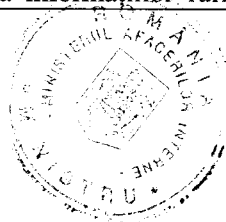
<p>investighează chestiunea și informează persoanele vizate cu privire la evoluția și la soluționarea plângerilor lor într-o perioadă de timp rezonabilă;</p> <p>(b) verifică legalitatea prelucrării datelor, desfășoară investigații, inspecții și audituri în conformitate cu dreptul intern, fie din proprie inițiativă, fie pe baza unei plângeri menționate la litera (a).</p>	<p>alin.(1), Autoritatea națională de supraveghere îndeplinește următoarele atribuții:</p> <p>a) primește plângerile depuse de orice persoană vizată, investighează aspectele semnalate și informează persoanele vizate cu privire la evoluția și la soluționarea plângerilor lor;</p> <p>b) verifică legalitatea prelucrării datelor cu caracter personal în cadrul Sistemului de evidență a datelor PNR și desfășoară investigații în conformitate cu Legea nr.677/2001, cu modificările și completările ulterioare, fie din oficiu, fie pe baza unei plângeri;</p> <p>c) verifică respectarea modului de punere în aplicare a prevederilor art.8 alin.(5).</p>	
<p>(4) La cerere, fiecare autoritate națională de supraveghere oferă consiliere oricărei persoane vizate cu privire la exercitarea drepturilor prevăzute în dispozițiile adoptate în temeiul prezentei directive.</p>	<p>Art.41 - Monitorizarea aplicării actului normativ</p> <p>(4) Autoritatea națională de supraveghere oferă consiliere oricărei persoane vizate, la cererea acesteia, cu privire la exercitarea drepturilor sale în contextul prelucrării datelor cu caracter personal în cadrul Sistemului de evidență a datelor PNR.</p>	
<p>CAPITOLUL III - Măsuri de punere în aplicare Articolul 16 - Protocoale comune și formate de date compatibile</p> <p>(1) Toate transferurile de date din PNR efectuate de către transportatorii aerieni către UIP în sensul prezentei directive sunt efectuate prin mijloace electronice care oferă garanții suficiente în ceea ce privește măsurile tehnice de securitate și măsurile organizatorice care reglementează prelucrarea ce urmează a fi efectuată. În cazul unei defecțiuni tehnice, datele din PNR pot fi transferate prin orice alte mijloace adecvate, cu condiția ca același nivel de securitate să fie menținut și ca dreptul Uniunii privind protecția datelor să fie respectat pe deplin.</p>	<p>Art.16 - Măsuri tehnice privind transmiterea datelor PNR</p> <p>(1) Transportatorii aerieni transmit datele PNR către UNIP, exclusiv prin metoda de tip push, prin mijloace electronice de comunicație capabile să asigure protecția datelor PNR prin măsurile tehnice de securitate și prin măsurile organizatorice aplicate transmiterii datelor PNR, sau, în caz de defecțiune tehnică, prin orice alte mijloace de comunicației care asigură același nivel de protecție a datelor PNR, precum și respectarea dispozițiilor legale privind protecția datelor cu caracter personal aplicabile.</p>	
<p>(2) La un an de la data la care Comisia adoptă pentru prima dată, în conformitate cu alineatul (3), protocoalele comune și formatele de date compatibile, toate transferurile de date din PNR efectuate de către transportatorii aerieni către UIP în sensul prezentei</p>	<p>Art.16 - Măsuri tehnice privind transmiterea datelor PNR</p> <p>(3) După împlinirea termenului de un an de la data la care Comisia Europeană adoptă pentru prima dată lista protocoalelor comune și</p>	



<p>directive sunt efectuate electronic, prin utilizarea de metode securizate conform protocoalelor comune respective. Aceste protocoale sunt comune tuturor transferurilor, pentru a asigura securitatea datelor din PNR în timpul transferului. Datele din PNR sunt transferate într-un format de date compatibil, pentru a asigura posibilitatea citirii datelor de către toate părțile implicate. Toți transportatorii aerieni sunt obligați să selecționeze și să îi precizeze UIP protocolul comun și formatul de date pe care intenționează să le utilizeze pentru transferurile lor.</p>	<p>a formatelor de date compatibile potrivit art.8 alin.(3) din Directiva (UE) 2016/681 a Parlamentului European și a Consiliului din 27 aprilie 2016, transportatorii aerieni sunt obligați:</p> <p>a) să notifice UNIP protocolul comun și formatul de date compatibil, dintre cele cuprinse în lista adoptată de Comisia Europeană, pe care urmează să le utilizeze pentru transmiterea datelor PNR;</p> <p>b) să utilizeze metode securizate, conforme cu protocolul comun notificat potrivit lit.a), pentru transmiterea datelor PNR către UNIP prin mijloace electronice de comunicație;</p> <p>c) să utilizeze formatul de date compatibil notificat potrivit lit.a) pentru transmiterea datelor PNR către UNIP.</p> <p>.....</p>	
<p>(3) Lista protocoalelor comune și a formatelor de date compatibile este stabilită și, dacă este necesar, este adaptată de către Comisie prin intermediul actelor de punere în aplicare. Actele de punere în aplicare respective sunt adoptate în conformitate cu procedura de examinare menționată la articolul 17 alineatul (2).</p>		
<p>(4) Alineatul (1) se aplică atât timp cât protocoalele comune și formatele de date compatibile menționate la alineatele (2) și (3) nu sunt disponibile.</p>	<p>Art.16 - Măsuri tehnice privind transmiterea datelor PNR (2) Până la aplicarea dispozițiilor alin.(3), datele PNR se transmit către UNIP în formatul/formatele de date stabilit/stabilite prin dispoziția inspectorului general al IGPF. </p>	
<p>(5) În termen de un an de la data adoptării protocoalelor comune și a formatelor de date compatibile menționate la alineatul (2), fiecare stat membru asigură adoptarea măsurilor tehnice necesare pentru a putea utiliza protocoalele comune și formatele de date.</p>	<p>Art.16 - Măsuri tehnice privind transmiterea datelor PNR (4) În termen de un an de la data la care Comisia Europeană adoptă pentru prima dată lista protocoalelor comune și a formatelor de date compatibile, IGPF asigură implementarea măsurilor tehnice necesare pentru ca Sistemul de evidență a</p>	



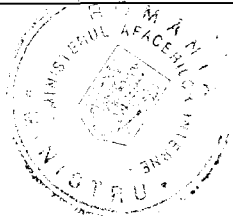
	<p>datelor PNR să utilizeze toate protocoalele comune și formatele de date compatibile cuprinse în lista adoptată de Comisia Europeană.</p> <p>(5) Resursele financiare necesare pentru implementarea măsurilor tehnice prevăzute la alin.(4) se asigură de la bugetul de stat, prin bugetul Ministerului Afacerilor Interne, pentru IGPF sau din fonduri externe nerambursabile.</p>	
<p>Articolul 17 - Procedura comitetului</p> <p>(1) Comisia este asistată de un comitet. Respectivul comitet este un comitet în înțelesul Regulamentului (UE) nr. 182/2011.</p>		
<p>(2) Atunci când se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.</p> <p>În cazul în care comitetul nu emite un aviz, Comisia nu adoptă proiectul de act de punere în aplicare și se aplică articolul 5 alineatul (4) al treilea paragraf din Regulamentul (UE) nr. 182/2011.</p>		
<p>CAPITOLUL IV - Dispoziții finale</p> <p>Articolul 18 - Transpunere</p> <p>(1) Statele membre asigură intrarea în vigoare a actelor cu putere de lege și a actelor administrative necesare pentru a se conforma prezentei directive până la 25 mai 2018. Statele membre informează de îndată Comisia cu privire la aceasta.</p> <p>Atunci când statele membre adoptă aceste acte, ele conțin o trimitere la prezenta directivă sau sunt însoțite de o asemenea trimitere la data publicării lor oficiale. Statele membre stabilesc modalitatea de efectuare a acestei trimiteri.</p> <p>(2) Statele membre transmit Comisiei textul principalelor dispoziții de drept intern pe care le adoptă în domeniul reglementat de prezenta directivă.</p>	<p><i>* Prezenta lege transpune Directiva 2016/681/UE 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, publicată în Jurnalul Oficial al Uniunii Europene, seria L, nr.119 din 4 mai 2016.</i></p>	
<p>Articolul 19 - Revizuirea</p> <p>(1) Pe baza informațiilor furnizate de statele membre, inclusiv</p>		<p>Nu sunt stabilite obligații de</p>



<p>informațiile statistice menționate la articolul 20 alineatul (2), Comisia revizuieste toate elementele prezentei directive și transmite și prezintă un raport Parlamentului European și Consiliului până la 25 mai 2020.</p> <p>(2) În realizarea acestei revizuii, Comisia acordă o atenție deosebită următoarelor:</p> <p>(a) respectării standardelor aplicabile de protecție a datelor cu caracter personal;</p> <p>(b) necesității și proporționalității colectării și prelucrării datelor din PNR pentru fiecare dintre scopurile prevăzute în prezenta directivă;</p> <p>(c) duratei perioadei de păstrare a datelor;</p> <p>(d) eficacității schimbului de date între statele membre; și</p> <p>(e) calității evaluărilor, inclusiv în ceea ce privește informațiile statistice colectate în conformitate cu articolul 20.</p> <p>(3) Raportul menționat la alineatul (1) include, de asemenea, o evaluare cu privire la necesitatea, proporționalitatea și eficiența includerii în domeniul de aplicare a prezentei directive a colectării și a transferului datelor din PNR cu caracter obligatoriu, referitoare la toate sau la anumite zboruri intra-UE. Comisia ține seama de experiența acumulată de statele membre, îndeosebi acele state membre care aplică prezenta directivă în ceea ce privește zborurile intra-UE în conformitate cu articolul 2. Raportul analizează, de asemenea, necesitatea includerii operatorilor economici care nu sunt transportatori, cum ar fi agențiile de voiaj și operatorii de turism care oferă servicii legate de călătorii, inclusiv rezervarea de zboruri, în cadrul domeniului de aplicare al prezentei directive.</p> <p>(4) Dacă este cazul, ținând seama de revizuirea efectuată în temeiul prezentului articol, Comisia face o propunere legislativă Parlamentului European și Consiliului în vederea modificării prezentei directive.</p>		transpunere
Articolul 20 - Date statistice	CAP.VI - Evaluarea eficienței utilizării datelor PNR	



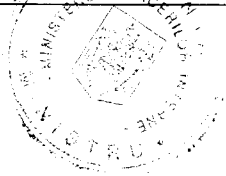
<p>(1) Statele membre pun anual la dispoziția Comisiei un set de informații statistice privind datele din PNR furnizate UIP. Aceste statistici nu trebuie să conțină nicio informație cu caracter personal.</p>	<p>Art.43 - Date statistice (1) UNIP transmite anual Comisiei Europene un set de informații statistice privind utilizarea datelor PNR. Este interzis ca datele transmise Comisiei Europene să conțină date cu caracter personal. </p>	
<p>(2) Statisticile includ cel puțin: (a) numărul total de pasageri ale căror date din PNR au fost colectate și partajate; (b) numărul de pasageri identificați pentru examinări suplimentare.</p>	<p>Art.43 - Date statistice (2) Informațiile statistice includ cel puțin: a) numărul total de pasageri ale căror date din PNR au fost colectate și transferate; b) numărul de pasageri identificați pentru examinări suplimentare.</p>	
<p>Articolul 21 - Relația cu alte instrumente (1) Statele membre pot continua să aplice acordurile sau înțelegerile bilaterale sau multilaterale dintre acestea privind schimbul de informații dintre autoritățile competente, aflate în vigoare la 24 mai 2016, în măsura în care aceste acorduri sau înțelegeri sunt compatibile cu prezenta directivă. (2) Prezenta directivă nu aduce atingere aplicabilității Directivei 95/46/CE în ceea ce privește prelucrarea datelor cu caracter personal de către transportatorii aerieni. (3) Prezenta directivă nu aduce atingere altor obligații și angajamente ale statelor membre sau ale Uniunii în temeiul unor acorduri bilaterale sau multilaterale cu țări terțe.</p>	<p>CAP. VII – Dispoziții tranzitorii și finale Art.44 - Dispoziții tranzitorii (1) Prezenta lege nu aduce atingere obligațiilor asumate, până la intrarea sa în vigoare, prin tratate încheiate cu țări terțe. (2) Tratatelor încheiate cu alte state membre ale Uniunii Europene privind schimbul de informații dintre autoritățile competente, aflate în vigoare la data de 24 mai 2016, se aplică după intrarea în vigoare a prezentei legi, numai în măsura în care sunt compatibile cu dispozițiile acesteia. (3) Prezenta lege nu aduce atingere dispozițiilor care stabilesc obligațiile transportatorilor aerieni cu privire la protecția datelor cu caracter personal. (4) Documentele de cooperare încheiate în temeiul art.9 alin.(6) din Ordonanța Guvernului nr.13/2015 se aplică și după intrarea în vigoare a prezentei legi, numai în măsura în care sunt compatibile cu dispozițiile acesteia.</p>	
<p>Articolul 22 - Intrarea în vigoare Prezenta directivă intră în vigoare în a douăzecea zi de la data publicării în Jurnalul Oficial al Uniunii Europene. Prezenta directivă se adresează statelor membre în conformitate cu tratatele.</p>		



<p>ANEXA I</p> <p>Datele din registrul cu numele pasagerilor în măsura în care au fost colectate de transportatorii aerieni</p> <ol style="list-style-type: none"> 1. Cod de reper al dosarului pasagerului 2. Data rezervării/emiterii biletului 3. Data (datele) prevăzută (prevăzute) a(le) călătoriei 4. Nume 5. Adresă și informații de contact (număr de telefon, adresă de e-mail) 6. Toate informațiile privind forma de plată, inclusiv adresa de facturare 7. Itinerarul complet de călătorie pentru anumite PNR 8. Informațiile din profilul „client fidel” („frequent flyer”) 9. Agenția/agentul de turism 10. 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 11. Informații scindate/divizate din registrul cu numele pasagerilor 12. Mențiuni 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) 13. Informații despre bilet, inclusiv numărul biletului, data emiterii biletului și bilete dus simplu, câmpurile aferente furnizării automate a prețului unui bilet de călătorie 14. Numărul locului și alte informații privind locul 15. Informații cu privire la codurile partajate 16. Toate informațiile cu privire la bagaje 	<p>Art.14 - Datele PNR</p> <p>(1) Transportatorii aerieni transmit către UNIP, în condițiile prevăzute la art.15 și art.16, următoarele date PNR:</p> <ol style="list-style-type: none"> a) codul de rezervare; b) data rezervării sau a emiterii biletului; c) data (datele) programată (programate) a (ale) călătoriei; d) numele și prenumele asociate rezervării; e) adresa și informațiile de contact (număr de telefon, adresă de e-mail) asociate rezervării; f) toate informațiile privind forma de plată, inclusiv adresa de facturare; g) itinerarul complet de călătorie; h) informațiile din profilul „client fidel”; i) agenția sau agentul de turism prin care a fost făcută rezervarea sau a fost cumpărat biletul; j) 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; k) informațiile scindate sau divizate din registrul cu numele pasagerilor; l) mențiunile cu caracter general, inclusiv toate informațiile disponibile despre minorii neînsoțiți cu vârsta sub 18 ani, precum numele 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; m) informațiile despre bilet, inclusiv numărul biletului, data emiterii biletului și bilete dus simplu și câmpurile aferente furnizării automate a prețului unui bilet de călătorie; n) numărul locului și alte informații privind locul; o) informațiile cu privire la codurile partajate; 	<p>Sintagma „<i>pentru anumite date PNR</i>” de la pct.7 (variantele de text din limbile română, engleză sau germană) nu asigură un grad adecvat de previzibilitate normei respective. Sensul corect al sintagmei este cel rezultat din variantele de text din limbile franceză, spaniolă și portugheză, adică „<i>pentru respectivele PNR</i>”.</p> <p>Formularea utilizată la art.14 alin.(1) lit.g) din proiectul de lege, corelată cu textul propus la art.13 alin.(1) din același proiect, stabilește obligația de transmitere a datelor referitoare la itinerarul complet de călătorie pentru toate datele PNR</p>
---	--	--



<p>17. Numărul pasagerilor înregistrați în PNR și alte nume ale acestora</p> <p>18. Orice date API colectate (inclusiv tipul, numărul, țara de emisie și data expirării oricărui document de identitate, cetățenia, numele de familie, prenumele, sexul, data nașterii, compania aeriană, numărul zborului, data plecării, data sosirii, aeroportul de plecare, aeroportul de sosire, ora plecării și ora sosirii)</p> <p>19. Un istoric al tuturor modificărilor datelor din PNR enumerate la punctele 1-18.</p>	<p>p) toate informațiile cu privire la bagaje;</p> <p>q) numărul pasagerilor înregistrați în PNR și alte nume ale acestora;</p> <p>r) orice date API colectate, inclusiv tipul, numărul, țara de emisie și data expirării oricărui document de identitate, cetățenia, numele de familie, prenumele, sexul, data nașterii, compania aeriană, numărul zborului, data plecării, data sosirii, aeroportul de plecare, aeroportul de sosire, ora plecării și ora sosirii;</p> <p>s) un istoric al tuturor modificărilor datelor PNR prevăzute la lit.a) – r).</p>	<p><u>pentru care asemenea informații au fost colectate de către transportator.</u></p>
<p>ANEXA II</p> <p>Lista de infracțiuni menționată la articolul 3 punctul 9</p> <ol style="list-style-type: none"> 1. participarea la un grup infracțional organizat, 2. traficul de ființe umane, 3. exploatarea sexuală a copiilor și pornografia infantilă, 4. traficul ilicit de stupefiante și substanțe psihotrope, 5. traficul ilegal de arme, muniții și materiale explozibile, 6. corupția, 7. fraudă, inclusiv fraudă care aduce atingere intereselor financiare ale Uniunii, 8. spălarea 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 ostateci, 15. furtul organizat și tâlhăria prin folosirea unei arme, 16. traficul ilicit de bunuri culturale, inclusiv antichități și opere de artă, 	<p>Art.3 - Definirea unor termeni și expresii</p> <p>În sensul prezentei legi, termenii și expresiile de mai jos au următoarele semnificații:</p> <p>i) infracțiuni grave – infracțiunile pentru care pedeapsa prevăzută de lege este detențiunea pe viață sau închisoarea al cărei maxim special este de cel puțin trei ani, corespunzătoare formelor de criminalitate prevăzute în Anexa la prezenta lege;</p> <p>ANEXA</p> <p>Formele de criminalitate la care se referă art.3 lit.i)</p> <p>.....</p> <ol style="list-style-type: none"> 2. Participarea la un grup infracțional organizat; 3. Traficul de ființe umane; 4. Exploatarea sexuală a copiilor și pornografia infantilă; 5. Traficul ilicit de stupefiante și substanțe psihotrope; 6. Traficul ilegal de arme, muniții și materiale explozibile; 7. Corupția; 8. Fraudă, inclusiv fraudă care aduce atingere intereselor financiare ale Uniunii Europene; 9. Spălarea banilor sau a produselor infracțiunii și falsificarea de monedă, inclusiv falsificarea monedei euro; 10. Infracțiunile informatice și criminalitatea cibernetică; 11. Infracțiunile împotriva mediului, inclusiv traficul ilicit de 	<p>La pct.1 al anexei sunt menționate „Infracțiunile <i>contra securității naționale</i>”, având în vedere faptul că obiectul de reglementare al proiectului de lege este extins și la utilizarea datelor PNR pentru apărarea securității naționale, domeniu aflat în competența exclusivă a statelor membre.</p>



<p>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.</p>	<p>specii de animale pe cale de dispariție și traficul ilicit de specii și soiuri de plante pe cale de dispariție; 12. Facilitarea intrării și șederii neautorizate; 13. Omorul și vătămarea corporală gravă; 14. Traficul ilicit de organe și țesuturi umane; 15. Răpirea, lipsirea de libertate în mod ilegal și luarea de ostateci; 16. Furtul organizat și tâlhăria prin folosirea unei arme; 17. Traficul ilicit de bunuri culturale, inclusiv antichități și opere de artă; 18. Contrafacerea și pirateria produselor; 19. Falsificarea de documente administrative și uzul de fals; 20. Traficul ilicit de substanțe hormonale și alți factori de creștere; 21. Traficul ilicit de materiale nucleare sau radioactive; 22. Violul și agresiunea sexuală; 23. Infracțiunile de competența Curții Penale Internaționale; 24. Sechestrarea ilicită a aeronavelor/navelor; 25. Sabotajul; 26. Traficul de autovehicule furate; 27. Spionajul industrial;</p>	
---	---	--

