



UNIUNEA EUROPEANĂ

PARLAMENTUL EUROPEAN

CONSILIUL

Bruxelles, 15 aprilie 2016
(OR. en)

2011/0023 (COD)

PE-CONS 71/15

GENVAL 81
AVIATION 164
DATAPROTECT 233
ENFOPOL 417
CODEC 1698

ACTE LEGISLATIVE ȘI ALTE INSTRUMENTE

Subiect: DIRECTIVĂ A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI privind
utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru
prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de
terorism și a infracțiunilor grave

DIRECTIVA (UE) 2016/...
A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI

din ...

**privind utilizarea datelor din registrul cu numele pasagerilor (PNR)
pentru prevenirea, depistarea, investigarea și urmărirea penală
a infracțiunilor de terorism și a infracțiunilor grave**

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 82 alineatul (1) litera (d) și articolul 87 alineatul (2) litera (a),

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Comitetului Economic și Social European¹,

după consultarea Comitetului Regiunilor,

hotărând în conformitate cu procedura legislativă ordinară²,

¹ JO C 218, 23.7.2011, p. 107.

² Poziția Parlamentului European din 14 aprilie 2016 (nepublicată încă în Jurnalul Oficial) și Decizia Consiliului din

întrucât:

- (1) La 6 noiembrie 2007, Comisia a adoptat o propunere de decizie-cadru a Consiliului privind utilizarea registrului cu numele pasagerilor (PNR) în scopul aplicării legii. Cu toate acestea, în urma intrării în vigoare a Tratatului de la Lisabona la 1 decembrie 2009, propunerea Comisiei, care nu a fost adoptată de Consiliu până la data respectivă, a devenit caducă.
- (2) „Programul de la Stockholm – O Europă deschisă și sigură în serviciul cetățenilor și pentru protecția acestora”¹ invită Comisia să prezinte o propunere privind utilizarea datelor din PNR în vederea prevenirii, depistării, investigării și urmării penale a infracțiunilor de terorism și a infracțiunilor grave.
- (3) În comunicarea sa din 21 septembrie 2010 privind o abordare globală referitoare la transferul de date din registrul cu numele pasagerilor (PNR) către țări terțe, Comisia a prezentat o serie de elemente principale ale unei politici a Uniunii în acest domeniu.
- (4) Directiva 2004/82/CE a Consiliului² reglementează transferul datelor privind informațiile prealabile referitoare la pasageri (API) de către operatorii de transport aerian către autoritățile naționale competente, în scopul îmbunătățirii controalelor la frontieră și al combaterii imigrației ilegale.
- (5) Obiectivele prezentei directive sunt, printre altele, asigurarea securității, protejarea vieții și siguranței persoanelor și crearea unui cadru juridic pentru protecția datelor din PNR în ceea ce privește prelucrarea acestora de către autoritățile competente.

¹ JO C 115, 4.5.2010, p. 1.

² Directiva 2004/82/CE a Consiliului din 29 aprilie 2004 privind obligația operatorilor de transport de a comunica datele privind pasagerii (JO L 261, 6.8.2004, p. 24).

- (6) Utilizarea eficace a datelor din PNR, cum ar fi compararea datelor din PNR cu diferite baze de date privind persoane și obiecte căutate, este necesară pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave, consolidând astfel securitatea internă, pentru strângerea probelor și, acolo unde este cazul, pentru identificarea complicilor infractorilor și destructurarea rețelelor infracționale.
- (7) Evaluarea datelor din PNR permite identificarea persoanelor care nu erau suspectate de implicare în infracțiuni de terorism sau în infracțiuni grave înainte de o astfel de evaluare, și care ar trebui să facă obiectul unor cercetări suplimentare desfășurate de către autoritățile competente. Prin utilizarea datelor din PNR se poate contracara amenințarea reprezentată de infracțiunile de terorism și de infracțiunile grave dintr-o altă perspectivă decât prin prelucrarea altor categorii de date cu caracter personal. Cu toate acestea, pentru a asigura faptul că prelucrarea datelor din PNR rămâne limitată la ceea ce este necesar, definirea și aplicarea de criterii de evaluare ar trebui să fie limitate la infracțiuni de terorism și infracțiuni grave pentru care este relevantă utilizarea unor astfel de criterii. Mai mult decât atât, criteriile de evaluare ar trebui definite într-un mod care să reducă la minimum numărul persoanelor nevinovate identificate greșit prin intermediul acestui sistem.
- (8) Transportatorii aerieni colectează și prelucrează deja datele din PNR ale pasagerilor lor în scopuri comerciale proprii. Prezenta directivă nu ar trebui să impună transportatorilor aerieni nicio obligație de a colecta sau păstra date suplimentare de la pasageri sau să impună vreo obligație pasagerilor de a furniza date în plus față de cele furnizate deja transportatorilor aerieni.

- (9) Unii transportatori aerieni păstrează, ca parte a datelor din PNR, datele API, pe care le colectează, iar alții nu. Utilizarea datelor din PNR împreună cu datele API conferă valoare adăugată asistenței oferite statelor membre pentru verificarea identității unei persoane, consolidând, prin aceasta, valoarea rezultatului respectiv în ceea ce privește aplicarea legii și reducând la minimum riscul de a efectua verificări și cercetări cu privire la persoane nevinovate. Este așadar importantă asigurarea faptului că, atunci când transportatorii aerieni colectează date API, aceștia le transferă indiferent dacă păstrează datele API prin alte mijloace tehnice decât pentru alte date din PNR.
- (10) Pentru a preveni, depista, investiga și urmări penal infracțiunile de terorism și infracțiunile grave, este esențial ca toate statele membre să introducă dispoziții care să stabilească obligații pentru transportatorii aerieni care operează zboruri extra-UE de a transfera datele din PNR colectate, inclusiv datele API. De asemenea, statele membre ar trebui să aibă posibilitatea să extindă această obligație la transportatorii aerieni care operează zboruri intra-UE. Aceste dispoziții nu ar trebui să aducă atingere Directivei 2004/82/CE.
- (11) Prelucrarea datelor cu caracter personal ar trebui să fie proporțională cu obiectivele specifice de securitate urmărite prin prezenta directivă.
- (12) Definiția infracțiunilor de terorism aplicată în prezenta directivă ar trebui să fie aceeași ca cea din Decizia-cadru 2002/475/JAI a Consiliului¹. Definiția infracțiunilor grave ar trebui să cuprindă categoriile de infracțiuni enumerate în anexa II la prezenta directivă.

¹ Decizia-cadru 2002/475/JAI a Consiliului din 13 iunie 2002 privind combaterea terorismului (JO L 164, 22.6.2002, p. 3).

- (13) Datele din PNR ar trebui să fie transferate unei singure unități de informații despre pasageri (UIP) desemnate din statul membru în cauză, astfel încât să se asigure claritatea și să se reducă costurile pentru transportatorii aerieni. UIP poate avea diferite filiale într-un stat membru și totodată statele membre pot institui o UIP în comun. Statele membre ar trebui să facă schimb de informații prin intermediul rețelelor relevante de schimb de informații în scopul de a facilita partajarea de informații și a asigura interoperabilitatea.
- (14) Statele membre ar trebui să suporte costurile aferente utilizării, păstrării și schimbului de date din PNR.
- (15) O listă a datelor din PNR solicitate care urmează să fie obținute de o UIP ar trebui să fie elaborată cu scopul de a reflecta cerințele legitime ale autorităților publice de prevenire, depistare, investigare și urmărire penală a infracțiunilor de terorism și a infracțiunilor grave, îmbunătățind prin aceasta securitatea internă în cadrul Uniunii și protejând totodată drepturile fundamentale, în special dreptul la viață privată și dreptul la protecția datelor cu caracter personal. În acest scop, ar trebui să se aplice standarde ridicate în conformitate cu Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „Carta”), cu Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (denumită în continuare „Convenția nr. 108”) și cu Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale (denumită în continuare „CEDO”). O astfel de listă nu ar trebui să se bazeze pe rasa sau originea etnică, religia sau convingerile, opiniile politice sau de orice altă natură, apartenența la un sindicat, starea de sănătate, viața sexuală sau orientarea sexuală a unei persoane. Datele din PNR ar trebui să conțină exclusiv detalii privind rezervările pasagerilor și itinerariile călătoriilor, care permit autorităților competente să-i identifice pe acei pasageri ai curselor aeriene care reprezintă o amenințare pentru securitatea internă.

- (16) În prezent sunt disponibile două metode de transfer de date: metoda de tip „pull”, prin care autoritățile competente din statul membru care solicită datele din PNR pot accesa sistemul de rezervări al transportatorului aerian și extrage („pull”) o copie a datelor din PNR solicitate, și metoda de tip „push”, prin care transportatorii aerieni transferă („push”) datele PNR solicitate către autoritatea care le solicită, permițându-le astfel transportatorilor aerieni să păstreze controlul asupra datelor pe care le furnizează. Se consideră că metoda de tip „push” oferă un grad mai mare de protecție a datelor și ar trebui să fie obligatorie pentru toți transportatorii aerieni.
- (17) Comisia susține orientările Organizației Aviației Civile Internaționale (OACI) privind PNR. Respectivele orientări ar trebui să reprezinte, prin urmare, baza adoptării formatelor de date compatibile pentru transferurile de date din PNR de către transportatorii aerieni către statele membre. În vederea asigurării unor condiții uniforme pentru punerea în aplicare a formatelor de date compatibile și a protocoalelor relevante aplicabile transferurilor de date de la transportatorii aerieni ar trebui conferite competențe de executare Comisiei. Respectivele competențe ar trebui exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului¹.
- (18) Statele membre ar trebui să ia toate măsurile necesare pentru a le permite transportatorilor aerieni să își îndeplinească obligațiile ce le revin în temeiul prezentei directive. Statele membre ar trebui să prevadă sancțiuni eficace, proporționale și disuasive, inclusiv sancțiuni financiare, împotriva transportatorilor aerieni care nu își respectă obligațiile privind transferul de date din PNR.
- (19) Fiecare stat membru ar trebui să fie responsabil de evaluarea amenințărilor potențiale legate de infracțiuni de terorism și de infracțiuni grave.

¹ Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului din 16 februarie 2011 de stabilire a normelor și principiilor generale privind mecanismele de control de către statele membre al exercitării competențelor de executare de către Comisie (JO L 55, 28.2.2011, p. 13).

- (20) Ținându-se cont pe deplin de dreptul la protecția datelor cu caracter personal și de dreptul la nediscriminare, nu ar trebui să fie luată nicio decizie care produce efecte juridice adverse asupra unei persoane sau care o afectează în mod semnificativ exclusiv ca urmare a prelucrării automatizate a datelor din PNR. Mai mult, conform articolelor 8 și 21 din Cartă, nicio astfel de decizie nu ar trebui să discrimineze o persoană pe motive precum sexul, rasa, culoarea, originea etnică sau socială, caracteristicile genetice, limba, religia sau convingerile, opiniile politice sau de orice altă natură, apartenența la o minoritate națională, averea, nașterea, un handicap, vârsta sau orientarea sexuală. Cu ocazia revizuirii aplicării prezentei directive, Comisia ar trebui, de asemenea, să ia în considerare respectivele principii.
- (21) Rezultatul prelucrării datelor din PNR nu ar trebui să fie utilizat în niciun caz de statele membre ca motiv pentru eludarea obligațiilor lor internaționale în temeiul Convenției de la Geneva din 28 iulie 1951 privind statutul refugiaților astfel cum a fost modificată de Protocolul din 31 ianuarie 1967, și nici nu ar trebui să fie utilizat pentru a refuza solicitanților de azil utilizarea unor căi legale sigure și eficiente către teritoriul Uniunii pentru a-și exercita dreptul lor la protecție internațională.
- (22) Ținând pe deplin seama de principiile evidențiate în jurisprudența relevantă recentă a Curții de Justiție a Uniunii Europene, aplicarea prezentei directive ar trebui să asigure respectarea deplină a drepturilor fundamentale, a dreptului la viață privată și a principiului proporționalității. De asemenea, ar trebui să respecte cu adevărat obiectivele vizând necesitatea și proporționalitatea pentru a îndeplini interesele generale recunoscute de Uniune și nevoia de a proteja drepturile și libertățile celorlalți în combaterea infracțiunilor de terorism și a infracțiunilor grave. Aplicarea prezentei directive ar trebui justificată în mod corespunzător și ar trebui să existe garanțiile necesare pentru a se asigura legalitatea oricărei acțiuni de stocare, analiză, transfer sau utilizare a datelor din PNR.

- (23) Statele membre ar trebui să facă schimb de date din PNR pe care le primesc, între ele și cu Europol, atunci când acest lucru este considerat necesar pentru prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor de terorism sau a infracțiunilor grave. UIP ar trebui să transmită, după caz, rezultatul prelucrării datelor din PNR fără întârziere către UIP ale altor state membre pentru investigații suplimentare. Dispozițiile prezentei directive nu ar trebui să aducă atingere altor instrumente ale Uniunii privind schimbul de informații între poliție și alte autorități de aplicare a legii și autoritățile judiciare, inclusiv Deciziei 2009/371/JAI a Consiliului¹ și Deciziei-cadru 2006/960/JAI a Consiliului². Acest schimb de date din PNR ar trebui să fie reglementat de normele privind cooperarea polițienească și judiciară și nu ar trebui să aducă atingere nivelului ridicat de protecție a vieții private și a datelor cu caracter personal impus de Cartă, de Convenția nr. 108 și de CEDO.
- (24) Ar trebui să fie asigurat un schimb securizat de informații privind datele PNR între statele membre prin intermediul oricărui canal de cooperare existent între autoritățile competente ale statelor membre, precum și, în special, cu Europol, prin intermediul aplicației de rețea pentru schimbul securizat de informații (SIENA) a Europol.

¹ Decizia 2009/371/JAI a Consiliului din 6 aprilie 2009 privind înființarea Oficiului European de Poliție (Europol) (JO L 121, 15.5.2009, p. 37).

² Decizia-cadru 2006/960/JAI a Consiliului din 18 decembrie 2006 privind simplificarea schimbului de informații și date operative între autoritățile de aplicare a legii ale statelor membre ale Uniunii Europene (JO L 386, 29.12.2006, p. 89).

- (25) Datele din PNR ar trebui să fie păstrate atât timp cât este necesar în scopul prevenirii, depistării, investigării și urmării penale a infracțiunilor de terorism și a infracțiunilor grave și proporțională cu acest scop. Din cauza naturii datelor și scopurilor pentru care acestea sunt utilizate, este necesar ca datele din PNR să fie păstrate o perioadă suficient de îndelungată pentru efectuarea de analize și pentru utilizarea în investigații. În vederea evitării utilizării disproporționate, după perioada inițială de păstrare datele ar trebui să fie depersonalizate prin mascarea elementelor de date. Pentru a asigura cel mai înalt nivel de protecție a datelor, accesul la datele complete din PNR care permit identificarea directă a persoanei vizate, ar trebui acordat numai în condiții foarte stricte și limitate după perioada inițială respectivă.
- (26) În cazul în care date specifice din PNR au fost transferate unei autorități competente și sunt utilizate în contextul unor anchete penale sau urmăriri penale specifice, păstrarea acestor date de către autoritatea competentă ar trebui să fie reglementată prin dreptul intern, indiferent de perioadele de păstrare a datelor prevăzute în prezenta directivă.
- (27) Prelucrarea datelor PNR în fiecare stat membru, de către UIP și autoritățile competente, ar trebui să facă obiectul unui standard de protecție a datelor cu caracter personal în temeiul dreptului intern în concordanță cu Decizia-cadru 2008/977/JAI a Consiliului¹ și cu cerințele specifice în materie de protecție a datelor prevăzute în prezenta directivă. Trimiterile la Decizia-cadru 2008/977/JAI ar trebui înțelese ca trimiteri la legislația aflată în vigoare, precum și la legislația viitoare care ar putea să o înlocuiască.

¹ Decizia-cadru 2008/977/JAI a Consiliului din 27 noiembrie 2008 privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală (JO L 350, 30.12.2008, p. 60).

- (28) Ținând seama de dreptul la protecția datelor cu caracter personal, drepturile persoanelor vizate cu privire la prelucrarea datelor acestora din PNR, cum ar fi drepturile de acces, rectificare, ștergere și restricționare și drepturile de a fi despăgubit și de a exercita o cale de atac, ar trebui să fie în concordanță atât cu Decizia-cadru 2008/977/JAI cât și cu nivelul ridicat de protecție prevăzut de Cartă și de CEDO.
- (29) Ținând cont de dreptul pasagerilor de a fi informați cu privire la prelucrarea datelor lor cu caracter personal, statele membre ar trebui să asigure faptul că pasagerilor li se furnizează informații corecte, ușor accesibile și ușor de înțeles privind colectarea datelor în PNR, transferul acestora către UIP, și drepturile lor ca persoane vizate.
- (30) Prezenta directivă nu aduce atingere dreptului Uniunii sau dreptului intern privind principiul accesului public la documente oficiale.
- (31) Transferurile de date din PNR de către statele membre către țări terțe ar trebui să fie permise doar de la caz la caz și cu respectarea deplină a dispozițiilor prevăzute de statele membre în temeiul Deciziei-cadru 2008/977/JAI. În vederea asigurării protecției datelor cu caracter personal, astfel de transferuri ar trebui să îndeplinească cerințe suplimentare referitoare la scopul transferului. Acestea ar trebui, de asemenea, să facă obiectul principiilor necesității și proporționalității și la nivelul ridicat de protecție prevăzut de Cartă și de CEDO.
- (32) Autoritatea națională de supraveghere înființată în contextul punerii în aplicare a Deciziei-cadru 2008/977/JAI ar trebui să fie, de asemenea, responsabilă de consilierea privind dispozițiile adoptate de statele membre în temeiul prezentei directive și de monitorizarea aplicării acestora.

- (33) Prezenta directivă nu aduce atingere posibilității statelor membre de a prevedea, în dreptul intern, un sistem pentru colectarea și prelucrarea datelor din PNR de la operatorii economici care nu sunt transportatori aerieni, cum ar fi agențiile de voiaj și operatorii de turism care oferă servicii legate de călătorii – inclusiv rezervarea de zboruri – pentru care colectează și prelucrează date din PNR, sau de la alți transportatori decât cei menționați în prezenta directivă, cu condiția ca aceste dispoziții ale dreptului intern să respecte dreptul Uniunii.
- (34) Prezenta directivă nu aduce atingere normelor actuale ale Uniunii privind modalitățile în care se realizează controalele la frontieră și nici normelor Uniunii care reglementează intrarea și ieșirea de pe teritoriul Uniunii.
- (35) Ca o consecință a diferențelor juridice și tehnice dintre dispozițiile naționale privind prelucrarea datelor cu caracter personal, inclusiv datele din PNR, transportatorii aerieni se confruntă și se vor confrunta cu cerințe diferite referitoare la tipurile de informații care urmează să fie transmise și la condițiile în care acestea sunt furnizate autorităților naționale competente. Respectivele diferențe pot aduce atingere cooperării eficiente între autoritățile naționale competente în scopul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de terorism și a infracțiunilor grave. Prin urmare, este necesar să se stabilească la nivelul Uniunii un cadrul legal comun pentru transferul și prelucrarea datelor din PNR.
- (36) Prezenta directivă respectă drepturile fundamentale și principiile Cartei, în special dreptul la protecția datelor cu caracter personal, dreptul la viață privată și dreptul la nediscriminare, astfel cum sunt protejate prin articolele 8, 7 și 21 din Cartă, și, prin urmare, ar trebui să fie pusă în aplicare în consecință. Prezenta directivă este compatibilă cu principiile protecției datelor, iar dispozițiile sale sunt conforme cu Decizia-cadru 2008/977/JAI. În plus, în vederea respectării principiului proporționalității, în domeniul specific prezenta directivă prevede norme mai stricte privind protecția datelor decât Decizia-cadru 2008/977/JAI.

- (37) Domeniul de aplicare al prezentei directive este cât se poate de limitat, întrucât: prevede păstrarea datelor din PNR în UIP pentru o perioadă care nu depășește cinci ani, după care datele ar trebui șterse; permite ca datele să fie depersonalizate prin mascarea elementelor de date după o perioadă inițială de șase luni; și interzice colectarea și utilizarea datelor sensibile. Pentru a asigura eficiența și un nivel ridicat de protecție a datelor, statele membre sunt obligate să asigure că o autoritate de supraveghere națională independentă și, în special, un responsabil cu protecția datelor, sunt responsabili de consilierea și de monitorizarea privind modul de prelucrare a datelor din PNR. Fiecare prelucrare de date din PNR ar trebui să fie luată într-o evidență sau documentată în scopul verificării legalității sale, al automonitorizării și în scopul garantării integrității și securității adecvate a prelucrării datelor. De asemenea, statele membre ar trebui să se asigure că pasagerilor le sunt oferite informații clare și precise cu privire la colectarea datelor în PNR și cu privire la drepturile lor.
- (38) Deoarece obiectivele prezentei directive, și anume transferul datelor din PNR de către transportatorii aerieni și prelucrarea acestor date în scopul prevenirii, depistării, investigării și urmării penale a infracțiunilor de terorism și a infracțiunilor grave, nu pot fi realizate în mod satisfăcător de către statele membre, dar pot fi realizate mai bine la nivelul Uniunii, aceasta poate adopta măsuri în conformitate cu principiul subsidiarității astfel cum este definit la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum este definit la articolul menționat, prezenta directivă nu depășește ceea ce este necesar pentru realizarea obiectivelor menționate.

- (39) În conformitate cu articolul 3 din Protocolul nr. 21 privind poziția Regatului Unit și a Irlandei cu privire la spațiul de libertate, securitate și justiție, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, aceste state membre au notificat intenția lor de a participa la adoptarea și la aplicarea prezentei directive.
- (40) În conformitate cu articolele 1 și 2 din Protocolul nr. 22 privind poziția Danemarcei, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, Danemarca nu participă la adoptarea prezentei directive, nu are obligații în temeiul acesteia și aceasta nu i se aplică.
- (41) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului¹ și a emis un aviz la 25 martie 2011,

ADOPTĂ PREZENTA DIRECTIVĂ:

¹ Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date (JO L 8, 12.1.2001, p. 1).

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.
- (2) Datele din PNR colectate în conformitate cu prezenta directivă pot fi prelucrate doar în scopul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de terorism și a infracțiunilor grave, astfel cum este prevăzut la articolul 6 alineatul (2) literele (a), (b) și (c).

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 moment. Comisia publică respectiva notificare și orice revocare în *Jurnalul Oficial al Uniunii Europene*.

- (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.
- (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.

Articolul 3

Definiții

În sensul prezentei directive, se aplică următoarele definiții:

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;
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;
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 multor state membre, 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;
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;
6. „sistem de rezervare” înseamnă sistemul intern al transportatorului aerian, în care datele din 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;
8. „infrațiuni de terorism” înseamnă infrațiunile prevăzute de dreptul intern menționate la articolele 1 - 4 din Decizia-cadru 2002/475/JAI;
9. „infrațiuni grave” înseamnă infrațiunile 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;
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.

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).
- (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 rezultate ale prelucrării acestora cu UIP din alte state membre și cu Europol, în conformitate cu articolele 9 și 10.
- (3) Membrii personalului UIP pot fi detașați de la autoritățile competente. Statele membre furnizează UIP resurse adecvate pentru ca acestea să-și îndeplinească sarcinile.

- (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.
- (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*.

Articolul 5

Responsabilul cu protecția datelor în cadrul UIP

- (1) UIP numește un responsabil cu protecția datelor pentru monitorizarea prelucrării datelor din PNR și punerea în aplicare a garanțiilor relevante.
- (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.
- (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.

Articolul 6
Prelucrearea 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 incluse în anexa I, UIP șterge aceste date imediat și definitiv la primirea lor.
- (2) UIP prelucrează datele din PNR doar în următoarele scopuri:
 - (a) efectuarea unei evaluări a pasagerilor înainte de sosirea în 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 prelucrearea datelor din PNR în cazuri specifice în scopul prevenirii, depistării, investigării și urmăririi 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 definerii de noi criterii ce urmează a fi utilizate pentru evaluările efectuate în temeiul alineatului (3) litera (b) cu scopul identificării oricăror persoane care pot fi implicate într-o infracțiune de terorism sau într-o infracțiune gravă.

- (3) În momentul efectuării evaluării menționate la alineatul (2) litera (a), UIP poate:
- (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 bazele de date; sau
 - (b) să prelucreze date din PNR în conformitate cu anumite criterii prestabilite.
- (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. Respectivetele 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.
- (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.

- (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.
- (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 autoritatea națională de supraveghere în acest sens.
- (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.

- (9) Consecințele evaluărilor pasagerilor menționate la alineatul (2) litera (a) din prezentul articol nu periclitează dreptul 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 Consiliului¹. 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 Consiliului², consecințele acestor evaluări respectă regulamentul menționat.

Articolul 7

Autorități competente

- (1) Fiecare stat membru adoptă o listă a autorităților competente îndreptățite să solicite sau să primească date din PNR sau rezultatul prelucrării acestor datelor de la UIP în vederea examinării suplimentare a acestor informații sau a adoptării măsurilor necesare în vederea prevenirii, depistării, investigării și urmării penale a infracțiunilor de terorism sau a infracțiunilor grave.

¹ Directiva 2004/38/CE a Parlamentului European și a Consiliului din 29 aprilie 2004 privind dreptul la liberă circulație și ședere pe teritoriul statelor membre pentru cetățenii Uniunii și membrii familiilor acestora, de modificare a Regulamentului (CEE) nr. 1612/68 și de abrogare a Directivelor 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE și 93/96/CEE (JO L 158, 30.4.2004, p. 77).

² Regulamentul (CE) nr. 562/2006 al Parlamentului European și al Consiliului din 15 martie 2006 de instituire a unui Cod comunitar privind regimul de trecere a frontierelor de către persoane (Codul Frontierelor Schengen) (JO L 105, 13.4.2006, p. 1).

- (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.
- (3) În sensul articolului 9 alineatul (3), fiecare stat membru notifică Comisiei lista autorităților sale competente până la ... [doisprezece luni de la data intrării în vigoare a prezentei directive], și poate modifica notificarea sa în orice moment. Comisia publică această notificare și eventualele modificări ale acesteia în *Jurnalul Oficial al Uniunii Europene*.
- (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.
- (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.
- (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.

Articolul 8

Obligațiile transportatorilor aerieni privind transferurile de date

- (1) Statele membre adoptă măsurile necesare pentru a se asigura că transportatorii aerieni transferă, prin „metoda push”, datele din PNR enumerate 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. 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. 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 referitoare la zboruri intra-UE.

- (2) În cazul în care transportatorii aerieni au colectat date privind informații prealabile 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.

- (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:
- (a) cu 24 până la 48 de ore înainte de ora programată pentru 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.
- (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.
- (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).

Articolul 9

Schimbul de informații dintre statele membre

- (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 destinate să transmit informațiile primite către autoritățile lor competente, în conformitate cu articolul 6 alineatul (6).

- (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 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).
- (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.
- (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.

- (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.

Articolul 10

Condițiile de acces al Europol la datele din PNR

- (1) Europol are competența de a solicita date din PNR sau rezultatul prelucrării respectivelor date de la UIP din statele membre, în limitele competențelor sale și în vederea îndeplinirii atribuțiilor sale.
- (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.

- (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.
- (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 informații este cea aplicabilă SIENA.

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).

- (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 permis în circumstanțe excepționale și numai dacă:
- (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
 - (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.

- (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.
- (4) Responsabilul cu protecția datelor din UIP al statului membru care a transferat datele din PNR este informat de fiecare dată când statul membru transferă datele din PNR în temeiul prezentului articol.

Articolul 12

Perioada de păstrare a datelor și depersonalizarea

- (1) Statele membre se asigură că datele din PNR furnizate de 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.

- (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:
- (a) numele, inclusiv numele altor pasageri din PNR precum și numărul pasagerilor care călătoresc împreună și care figurează în PNR;
 - (b) adresa și informațiile de contact;
 - (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;
 - (d) informațiile din profilul „client fidel” („frequent flyer”);
 - (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
 - (f) orice date API care au fost colectate.
- (3) După expirarea perioadei de șase luni menționată la alineatul (2), dezvăluirea datelor complete din PNR este permisă numai dacă:
- (a) se consideră în mod rezonabil că este necesară în scopul menționat la articolul 6 alineatul (2) litera (b) și

- (b) este aprobată de către:
- (i) o autoritate judiciară; sau
 - (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.
- (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 urmăririi penale a infracțiunilor de terorism sau a infracțiunilor grave, când păstrarea acestor date de către autoritatea competentă este reglementată de dreptul intern.
- (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 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.

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.
- (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.
- (3) Prezenta directivă nu aduce atingere aplicabilității Directivei 95/46/CE a Parlamentului European și a Consiliului¹ 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.
- (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.

¹ Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (JO L 281, 23.11.1995, p. 31).

- (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:
- (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;
 - (b) cererile depuse de autoritățile competente și UIP ale altor state membre;
 - (c) toate cererile de date din PNR și transferurile de aceste date către o țară terță.

La cerere, UIP pune toată documentația la dispoziția autorității naționale de supraveghere.

- (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.

Înregistrările respective sunt păstrate pentru o perioadă de cinci ani.

- (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.

- (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.

Articolul 14

Sanțiuni

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.

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.

Sanțiunile prevăzute trebuie să fie eficiente, proporționale și cu efect de descurajare.

Articolul 15

Autoritatea națională de supraveghere

- (1) Fiecare stat membru prevede că autoritatea națională de supraveghere menționată la articolului 25 din Decizia-cadru 2008/977/JAI este responsabilă de consilierea 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.

- (2) Respectivele autorități naționale de supraveghere își desfășoară activitățile de la alineatul (1) urmărind protejarea drepturilor fundamentale legate de prelucrarea datelor cu caracter personal.
- (3) Fiecare autoritate națională de supraveghere are următoarele îndatoriri:
- (a) tratează plângerile depuse de orice persoană vizată, investighează chestiunea și informează persoanele vizate cu privire la evoluția și la soluționarea plângerilor lor într-o perioadă de timp rezonabilă;
 - (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).
- (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.

CAPITOLUL III

MĂSURI DE PUNERE ÎN APLICARE

Articolul 16

Protocoale comune și formate de date compatibile

- (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.

- (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 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.

- (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).
- (4) Alineatul (1) se aplică atât timp cât protocoalele comune și formatele de date compatibile menționate la alineatele (2) și (3) nu sunt disponibile.
- (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.

Articolul 17

Procedura comitetului

- (1) Comisia este asistată de un comitet. Respectivul comitet este un comitet în înțelesul Regulamentului (UE) nr. 182/2011.
- (2) Atunci când se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.

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.

CAPITOLUL IV

DISPOZIȚII FINALE

Articolul 18

Transpunere

- (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 ... [doi ani de la intrarea în vigoare a prezentei directive]. Statele membre informează de îndată Comisia cu privire la aceasta.

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.

- (2) Statele membre transmit Comisiei textul principalelor dispoziții de drept intern pe care le adoptă în domeniul reglementat de prezenta directivă.

Articolul 19

Revizuirea

- (1) Pe baza informațiilor furnizate de statele membre, inclusiv informațiile statistice menționate la articolul 20 alineatul (2), Comisia revizuieste toate elementele prezentei directive și transmite și prezintă un raport Parlamentului European și Consiliului în până la ... [patru ani de la data intrării în vigoare a prezentei directive].

- (2) În realizarea acestei revizuii, Comisia acordă o atenție deosebită următoarelor:
- (a) respectării standardelor aplicabile de protecție a datelor cu caracter personal,
 - (b) necesității și proporționalității colectării și prelucrării datelor din PNR pentru fiecare dintre scopurile prevăzute în prezenta directivă,
 - (c) duratei perioadei de păstrare a datelor,
 - (d) eficacității schimbului de date între statele membre, și
 - (e) calității evaluărilor, inclusiv în ceea ce privește informațiile statistice colectate în conformitate cu articolul 20.
- (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.
- (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.

Articolul 20

Date statistice

- (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.
- (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.

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 ... [data intrării în vigoare a prezentei directive], 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.

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.

Adoptată la ...,

Pentru Parlamentul European
Președintele

Pentru Consiliu
Președintele

ANEXA I

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

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
 17. Numărul pasagerilor înregistrați în PNR și alte nume ale acestora
 18. 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)
 19. Un istoric al tuturor modificărilor datelor din PNR enumerate la punctele 1 - 18.
-

ANEXA II

Lista de infracțiuni menționată la articolul 3 punctul 9

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,
 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.
-