

I

(Rezoluții, recomandări și avize)

AVIZE

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR

Avizul Autorității Europene pentru Protecția Datelor referitor la propunerea de decizie a Consiliului privind încheierea unui acord între Uniunea Europeană și Australia privind prelucrarea și transferul datelor din registrul cu numele pasagerilor (PNR) de către transportatorii aerieni către Serviciul vamal și de protecție a frontierelor din Australia

(2011/C 322/01)

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR,

către Serviciul vamal și de protecție a frontierelor din Australia ⁽³⁾. Propunerea a fost transmisă AEPD la data de 23 mai.

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 16,

2. AEPD a fost consultată neoficial în cursul lunii mai 2011, în contextul unei proceduri rapide, referitor la propunerea privind încheierea unui acord între Uniunea Europeană și Australia privind prelucrarea și transferul datelor PNR.

având în vedere Carta drepturilor fundamentale a Uniunii Europene, în special articolele 7 și 8,

3. Considerând că observațiile sale privind fondul propunerii adoptate de către Comisie și prezentate Consiliului și Parlamentului rămân valabile, AEPD a hotărât să realizeze o difuzare mai amplă a comentariilor sale sub forma unui aviz public. În acest mod, observațiile sale pot fi preluate în cadrul dezbaterilor ulterioare privind propunerea.

având în vedere 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 ⁽¹⁾,

4. AEPD folosește această ocazie pentru a ridica și alte probleme și încurajează Consiliul și Parlamentul să ia în considerare părerile sale în momentul luării unei decizii privind propunerea, în conformitate cu articolul 218 din Tratatul privind funcționarea Uniunii Europene.

având în vedere articolul 41 din 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 ⁽²⁾,

ADOPTĂ PREZENTUL AVIZ:

1.2. Contextul propunerii

1. INTRODUCERE

1.1. Consultarea AEPD

1. La 19 mai 2011, Comisia a adoptat o propunere privind încheierea unui acord între Uniunea Europeană și Australia privind prelucrarea și transferul datelor din registrul cu numele pasagerilor (PNR) de către transportatorii aerieni

5. Acordul între Uniunea Europeană și Australia privind datele PNR reprezintă un pas înainte pe agenda Uniunii Europene, care cuprinde orientările globale privind PNR, realizarea unui sistem PNR al UE și negocierea unor acorduri cu țările terțe ⁽⁴⁾.

⁽¹⁾ JO L 281, 23.11.1995, p. 31.

⁽²⁾ JO L 8, 12.1.2001, p. 1.

⁽³⁾ COM(2011) 281 final.

⁽⁴⁾ A se vedea în special Comunicarea Comisiei din 21 septembrie 2010 privind o abordare globală referitoare la transferul de date din registrul cu numele pasagerilor (PNR) către țări terțe [COM(2010) 492 final].

6. AEPD a urmărit îndeaproape evoluțiile privind PNR și a adoptat recent două avize privind „pachetul PNR” al Comisiei și propunerea de directivă privind PNR al UE ⁽¹⁾. Opiniile exprimate de către AEPD referitor la sistemele PNR completează și concordă în mare măsură cu cele ale Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal ⁽²⁾, dar și cu alte documente recente printre care avizul Comitetului Economic și Social ⁽³⁾ și avizul Agenției pentru Drepturi Fundamentale ⁽⁴⁾.
7. După cum se detaliază în cele ce urmează, abordarea consecventă a AEPD a constat întotdeauna în confruntarea scopului sistemelor PNR cu cerințele fundamentale referitoare la necesitate și proporționalitate, iar într-o etapă ulterioară în analiza detaliilor prevederilor în vederea sugerării unor îmbunătățiri acolo unde este cazul.

1.3. Observație preliminară

8. AEPD salută abordarea generală prin care se urmărește armonizarea garanțiilor privind protecția datelor în diversele acorduri PNR cu țările terțe. Cu toate acestea, mai trebuie formulate câteva observații.
9. Una dintre remarcile exprimate repetat în avizele AEPD și în avizele Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal se aplică în mod egal și propunerii privind registrul australian cu numele pasagerilor: trebuie demonstrată necesitatea și proporționalitatea sistemelor PNR.
10. Aceste două cerințe fundamentale reprezintă aspecte esențiale ale legislației în materie de protecție a datelor, în conformitate cu articolele 7 și 8 din Carta drepturilor

fundamentale și cu articolul 16 din Tratatul privind funcționarea Uniunii Europene. Uniunea Europeană trebuie să asigure respectarea cerințelor din legislația UE în materie de protecție a datelor și în cazurile în care datele cu caracter personal ale cetățenilor europeni sunt prelucrate și transferate din teritoriul UE către o țară terță. În astfel de cazuri, înainte de semnarea oricărui acord trebuie evaluate și stabilite necesitatea și proporționalitatea demersului. În plus față de elementele care susțin necesitatea sistemului PNR, proporționalitatea presupune și existența unui echilibru corespunzător între scopul urmărit și prelucrarea unor cantități masive de date, care ar avea drept rezultat o imixtiune gravă în viața privată a persoanelor.

11. În ceea ce privește sistemele PNR, scopul acestora este combaterea terorismului și a infraționiilor (transnaționale) grave prin intermediul culegerii unei cantități masive de date referitoare la toți pasagerii, în vederea efectuării unei evaluări a riscurilor prezentate de acești pasageri. Până în prezent AEPD nu a găsit niciun element convingător în cadrul justificărilor prezentate în favoarea sistemelor PNR existente sau preconizate, precum sistemul PNR al UE pe care l-a analizat în detaliu în avizul din martie 2011 ⁽⁵⁾.

12. În plus, chiar și în cazul în care se va stabili necesitatea sistemului, AEPD subliniază că acesta trebuie să treacă și testul proporționalității. Agenția pune sub semnul întrebării echilibrul dintre prelucrarea datelor cu caracter personal pe scară largă și scopul urmărit, cu precădere având în vedere numărul mare de infrațiuni cuprinse în domeniul de aplicare al proiectului de acord. AEPD ia în considerare disponibilitatea altor instrumente eficiente de combatere a terorismului și a infraționiilor grave.

13. Comentariile specifice expuse în continuare nu aduc atingere acestei observații preliminare fundamentale. AEPD salută dispozițiile care prevăd garanții specifice precum cele privind securitatea datelor, aplicarea și supravegherea, precum și pe cele referitoare la transferurile ulterioare. În același timp, AEPD își exprimă îngrijorarea privind domeniul de definiție și condițiile de păstrare a datelor, în plus față de necesitatea și proporționalitatea sistemului.

2. ANALIZA PROPUNERII

2.1. Temeiul juridic

14. AEPD observă că acordul se întemeiază pe articolul 82 alineatul (1) litera (d), pe articolul 87 alineatul (2) litera (a) și pe articolul 218 alineatul (6) litera (a) din Tratatul privind funcționarea Uniunii Europene. AEDP reamintește că printre factorii obiectivi care trebuie luați în considerare pentru alegerea temeiului juridic se numără în special

⁽¹⁾ — Avizul AEPD din 25 martie 2011 referitor la propunerea de directivă a Parlamentului European și a Consiliului privind utilizarea datelor din registrul cu numele pasagerilor pentru prevenirea, depistarea, cercetarea și urmărirea penală a infraționiilor de terorism și a infraționiilor grave;

— Avizul AEPD din 19 octombrie 2010 privind o abordare globală referitoare la transferul de date din registrul cu numele pasagerilor (PNR) către țări terțe.

Ambele avize sunt disponibile la adresa <http://www.edps.europa.eu/EDPSWEB/edps/cache/off/Consultation>

⁽²⁾ Avizul nr. 10/2011 al Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal din 5 aprilie 2011 referitor la propunerea de directivă a Parlamentului European și a Consiliului privind utilizarea datelor din registrul cu numele pasagerilor pentru prevenirea, depistarea, cercetarea și urmărirea penală a infraționiilor de terorism și a infraționiilor grave: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2011_en.htm

⁽³⁾ Avizul Comitetului Economic și Social European din 5 mai 2011 referitor la propunerea de directivă a Parlamentului European și a Consiliului privind utilizarea datelor din registrul cu numele pasagerilor pentru prevenirea, depistarea, cercetarea și urmărirea penală a infraționiilor de terorism și a infraționiilor grave [COM(2011) 32 final].

⁽⁴⁾ Avizul Agenției pentru Drepturi Fundamentale a Uniunii Europene din 14 iunie 2011 referitor la propunerea de directivă a Parlamentului European și a Consiliului privind utilizarea datelor din registrul cu numele pasagerilor pentru prevenirea, depistarea, cercetarea și urmărirea penală a infraționiilor de terorism și a infraționiilor grave [COM(2011) 32 final].

⁽⁵⁾ Avizul AEPD din 25 martie 2011 referitor la propunerea de directivă a Parlamentului European și a Consiliului privind utilizarea datelor din registrul cu numele pasagerilor pentru prevenirea, depistarea, cercetarea și urmărirea penală în cazul infraționiilor de terorism și a infraționiilor grave; a se vedea, de asemenea, avizul Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, menționat mai sus.

- scopul și conținutul actului⁽¹⁾. Dacă prin analizarea unui act al Uniunii Europene se dovedește că acesta urmărește o dublă finalitate sau că are două componente și dacă una dintre aceste finalități sau componente poate fi identificată ca fiind principală sau preponderentă, iar cealaltă nu este decât accesorie, actul trebuie să aibă un temei juridic unic, și anume temeiul impus de finalitatea sau de componenta principală ori preponderentă⁽²⁾. Cu titlu excepțional, dacă se stabilește că actul urmărește simultan mai multe finalități care sunt legate în mod indisolubil, fără ca vreuna să fie accesorie și indirectă în raport cu alta, actul normativ poate fi adoptat pe baza diferitelor temeiuri juridice corespunzătoare⁽³⁾.
15. În contextul jurisprudenței constante rezumate mai sus, cu excepția articolului 218 alineatul (6) litera (a), AEPD consideră că acordul nu ar trebui să se întemeieze pe articolul 82 alineatul (1) litera (d) și pe articolul 87 alineatul (2) litera (a), ci pe articolul 16 din Tratatul privind funcționarea Uniunii Europene.
16. În ceea ce privește scopul, trebuie reamintit faptul că toate acordurile PNR negociate de UE au fost determinate de necesitatea de a reconcilia obligația transportatorilor aerieni de a furniza date PNR autorităților din țări terțe, cu dreptul fundamental la protecția datelor⁽⁴⁾. În plus, textul propunerii se referă în numeroase rânduri la scopul protecției datelor cu caracter personal⁽⁵⁾.
17. În ceea ce privește conținutul acordului, este evidentă preponderența dispozițiilor referitoare la protecția datelor. Cu excepția articolelor 3, 4 și 6, preocuparea privind protecția datelor pare să se găsească aproape în totalitatea dispozițiilor acordului. Acest lucru este evident în
- (1) Cauza C-491/01, British American Tobacco, în special punctele 92 și 93.
- (2) Cauza C-42/97, Parlamentul European/Consiliul, punctele 39 și 40.
- (3) A se vedea în acest scop cauza C-491/01, British American Tobacco, punctele 92 și 93 și cauza C-42/97, Parlamentul European/Consiliul, punctul 38.
- (4) Curtea recunoaște acest lucru în partea factuală a hotărârilor privind PNR, cauzele conexe C-317/04 și C-318/04, punctul 33.
- (5) — În expunerea de motive se recunoaște faptul că legislația UE în materie de protecție a datelor nu permite transportatorilor să transmită date PNR către țările care nu asigură un nivel adecvat de protecție. Prin urmare, „este necesar să se găsească o soluție care să ofere temeiul juridic pentru transfer [...] pentru a asigura [...] respectarea dreptului persoanei la protecția datelor cu caracter personal”.
- Obiectivul de asigurare a respectării dreptului de protecție a datelor cu caracter personal reiese foarte clar și din preambul, respectiv din considerentul în care se citează articolul 6 din Tratatul privind Uniunea Europeană, articolul 16 din Tratatul privind funcționarea Uniunii Europene, articolul 8 din Convenția europeană a drepturilor omului, Convenția 108 etc.
- În preambul se menționează și dispozițiile relevante privind protecția datelor din legislația australiană, admițându-se faptul că acestea cuprind dispoziții cu privire la protecția datelor, drepturile de acces și despăgubire, rectificarea și adnotare, precum și căile de atac și sancțiunile pentru utilizarea frauduloasă a datelor personale.
- În articolul 1 din acord – intitulat „Obiectivul acordului” – se afirmă că acesta cuprinde dispoziții privind transferul de date PNR. În continuare se menționează că acordul „prevede condițiile în care astfel de date pot fi transferate și utilizate, precum și modul în care datele respective sunt protejate” (sublinierea noastră).
- articolul 1 (obiectiv), articolul 2 (definiții), articolul 5 (adecvare) și articolele 7-19 (garanții aplicabile prelucrării datelor PNR).
18. În ceea ce privește dispozițiile referitoare la garanții (articolele 7-19), trebuie remarcat că acestea cuprind prevederi caracteristice legislației privind protecția datelor⁽⁶⁾. Faptul că un act cuprinde prevederi care aparțin de obicei unui domeniu legislativ specific a fost considerat de către Curte ca element de justificare a unui singur temei juridic specific⁽⁷⁾.
19. Pe scurt, AEPD consideră că obiectivul acestui acord nu este îmbunătățirea cooperării polițienești, ci mai degrabă împunerea și autorizarea operatorilor privați să efectueze transferul de date cu caracter personal în cazul primirii unei solicitări de la o țară terță. Deși în principiu un astfel de transfer către o țară terță nu ar fi posibil în conformitate cu reglementările Uniunii Europene, acordul PNR are ca scop să permită transferul de date cu caracter personal conform cerințelor UE privind protecția datelor, prin adoptarea unor garanții specifice.
20. Din aceste motive, AEPD consideră că acordul ar trebui să se întemeieze – în mod prioritar în orice caz – pe articolul 16 din Tratatul privind funcționarea Uniunii Europene⁽⁸⁾.

2.2. Scop și definiții

21. AEPD remarcă faptul că scopurile pentru care datele PNR pot fi prelucrate sunt precis definite în articolul 3 al propunerii. Cu toate acestea, agenția deplânge faptul că definițiile curente sunt mai cuprinzătoare decât definițiile din propunerea de directivă privind sistemul PNR al UE, care la rândul lor ar fi trebuit restrânse, mai ales în ceea ce privește infracțiunile minore.
22. În timp ce definițiile din propunerea referitoare la PNR UE iau în considerare consecințele activităților definite ca „teroriste”, precum prejudiciile concrete aduse persoanelor sau guvernelor (moartea, atacuri asupra integrității fizice, distrugeri asupra unui sistem de transport, a unei infrastructuri etc.), propunerea de față este mai puțin specifică și în mai mare măsură orientată spre scop atunci când se referă la intimidarea persoanelor sau a guvernelor, ori la destabilizarea gravă a structurilor politice sau economice fundamentale.

⁽⁶⁾ De exemplu dispozițiile privind datele sensibile, securitatea datelor, răspunderea, transparența, dreptul de acces, de rectificare și de ștergere, dreptul de a recurge la căi de atac, prelucrarea automată etc.

⁽⁷⁾ Avizul nr. 2/2000, Protocolul de la Cartagena, punctul 33.

⁽⁸⁾ În acest context ar trebui să se facă referire și la Declarația 21 „privind protecția datelor cu caracter personal în domeniul cooperării judiciare în materie penală și al cooperării polițienești”, anexată la Tratatul de la Lisabona. Formularea clară a Declarației 21 confirmă că, chiar și în cazul existenței unor elemente de cooperare polițienească, instrumentele de protecție a datelor din acest domeniu trebuie să se întemeieze în continuare pe dispozițiile articolului 16 din Tratatul privind funcționarea Uniunii Europene (acolo unde se potrivesc cu alte dispoziții). Această analiză nu poate aduce atingere repartizării responsabilităților în cadrul Comisiei Europene.

23. AEPD consideră că se impune mai multă precizie în ceea ce privește noțiunile de „intimidare, obligare sau constrângere”, precum și „structurile fundamentale politice, constituționale, economice sau (mai ales) sociale ale unei țări sau ale unei organizații internaționale”. Aceasta ar împiedica aplicarea sistemului PNR în situațiile pe care acesta nu ar trebui să le vizeze în niciun caz, precum activitățile legitime într-un context social, cultural sau politic (de exemplu demonstrațiile pașnice) ⁽¹⁾.
24. Posibilitatea prelucrării datelor în alte cazuri cu caracter excepțional ridică întrebări suplimentare, în special deoarece se extinde asupra „amenințării la adresa sănătății”. AEPD consideră că o astfel de extindere a scopului este disproporționată, în special luând în considerare faptul că, acolo unde este necesar, de la caz la caz, pot fi găsite proceduri alternative, cu caracter specific, de înlăturare a amenințărilor grave la adresa sănătății. În plus, datele PNR nu reprezintă instrumentul cel mai adecvat de identificare a pasagerilor: există date mai precise, în special datele API.
25. AEPD observă, de asemenea, că lista datelor PNR anexată la propunere depășește ceea ce autoritățile de protecție a datelor au considerat ca fiind proporțional în avizele Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal ⁽²⁾. Această listă ar trebui diminuată. În mod special, nu se justifică includerea categoriei „Observații generale”, care poate cuprinde date irelevante – și potențial sensibile – și care ar trebui șterse.

2.3. Date sensibile

26. AEPD salută excluderea prelucrării datelor sensibile din domeniul de aplicare, după cum se menționează în articolul 8 din propunere. Cu toate acestea, felul în care este formulată această dispoziție sugerează în continuare că datele sensibile pot fi „prelucrate”. Dispoziția permite trimiterea acestor date de către companiile aeriene într-o primă etapă, urmată de ștergerea lor de către autoritățile publice în a doua etapă. Trimiterea efectuată de companiile aeriene reprezintă un act de prelucrare. AEPD consideră că societățile aeriene ar trebui obligate să filtreze datele sensibile la sursa procesului de prelucrare.

2.4. Securitatea datelor

27. Propunerea cuprinde în articolul 9 o prevedere cuprinzătoare referitoare la securitatea și integritatea datelor, care este binevenită. AEPD susține în special obligația raportării cazurilor de încălcare a securității la Biroul comisarului australian pentru informații. În ceea ce privește trimiterea ulterioară a informațiilor către Comisia Europeană, sunt necesare explicații suplimentare privind procedura care trebuie urmată. În plus, AEPD consideră

că și autoritățile de protecție a datelor reprezintă destinatari relevanți pentru acest tip de informații și că ar trebui menționate explicit în propunere.

2.5. Supraveghere și aplicare

28. Sistemul de supraveghere, care include măsuri de control și responsabilizare și care insistă asupra nediscriminării în baza cetățeniei sau a locului de reședință, este binevenit. De asemenea, AEPD susține cu tărie dreptul fundamental al fiecărei persoane la despăgubiri administrative și la protecție jurisdicțională eficientă. Agenția consideră că rolul Biroului comisarului australian pentru informații reprezintă o garanție importantă în ceea ce privește posibilitățile de despăgubire și exercitarea drepturilor persoanelor vizate.

2.6. Deciziile individuale automatizate

29. În conformitate cu articolul 15, interpretat *a contrario*, pe baza prelucrării automate a datelor PNR se pot lua decizii automatizate în cazurile în care acestea nu „afectează semnificativ și nici nu au un efect juridic negativ asupra unui călător”. Garanțiile se aplică numai în cazul în care decizia ar afecta semnificativ călătorul. Luând în considerare domeniul amplu de aplicare a prelucrării automate a datelor cu caracter personal prevăzut de sistemul PNR, în opinia AEPD această restricție este discutabilă. Pentru a evita interpretarea flexibilă a acestei dispoziții, agenția recomandă să se elimine termenul „semnificativ” și să nu se permită luarea niciunei decizii automatizate care ar avea un efect negativ asupra unei persoane.

2.7. Păstrarea datelor

30. AEPD consideră că lungimea perioadei de păstrare a datelor prevăzută la articolul 16 reprezintă una din principalele dificultăți ale propunerii. Perioada de păstrare de cinci ani și jumătate, dintre care trei ani fără nicio mascare a datelor, este în mod clar disproporționată, în special în comparație cu sistemul PNR australian anterior, care nu prevedea stocarea datelor decât de la caz la caz ⁽³⁾. Sunt necesare justificări cuprinzătoare care să explice de ce se prevede o perioadă de păstrare atât de lungă, care nu a fost considerată necesară în primul sistem PNR australian.
31. În conformitate cu poziția pe care a susținut-o în avizul privind propunerea de directivă privind sistemul PNR al UE, AEPD consideră că după cel mult 30 de zile, dacă nu imediat după analiză, ar trebui să aibă loc anonimizarea completă (respectiv ireversibilă) a tuturor datelor.

⁽¹⁾ În acest sens, spre exemplu dreptul fundamental la libertatea de întrunire (articolul 12 din Carta drepturilor fundamentale) nu ar trebui să fie știrbit de o formulare excesiv de cuprinzătoare.

⁽²⁾ Avizul din 23 iunie 2003 privind nivelul de protecție asigurat în Statele Unite pentru transferul datelor pasagerilor, Grupul de lucru 78.

⁽³⁾ A se vedea în acest scop avizul pozitiv al Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal: Avizul nr. 1/2004 din 16 ianuarie 2004 privind nivelul de protecție asigurat în Australia pentru transmiterea datelor din registrul cu numele pasagerilor de către transportatorii aerieni, Grupul de lucru 85. Avizul ia în considerare faptul că „vămile aplică o politică generală de nepăstrare a acestor date. Pentru cei 0,05 %-0,1 % dintre pasageri care sunt semnalati autorităților vamale în vederea unei evaluări mai amănunțite, datele PNR transmise de către transportatorul aerian sunt păstrate temporar până la finalizarea evaluării vamale, însă nu sunt stocate. După finalizarea evaluării, datele PNR ale pasagerilor respectivi sunt șterse din calculatorul ofițerului unității de analiză a pasagerilor (PAU) din cadrul autorității vamale și nu sunt introduse în bazele de date australiene”.

2.8. Transferurile ulterioare

32. Garanțiile prevăzute la articolele 18 și 19 sunt binevenite, în special deoarece cuprind dispoziții cu privire la lista destinatarilor datelor transferate pe teritoriul Australiei, la transferul datelor de la caz la caz și la evaluarea necesității transferului în fiecare situație. Cu toate acestea, AEPD observă că această dispoziție poate fi eludată prin excepția prevăzută la articolul 18.1 litera (c), care permite schimburile de date depersonalizate chiar dacă acestea nu se realizează conform principiului „de la caz la caz”. Cu toate acestea, depersonalizarea nu implică ștergerea elementelor care permit identificarea, ci numai mascarea acestora, accesul deplin la date rămânând posibil. Din acest motiv, AEPD recomandă să nu se permită nicio excepție de la principiul transferării datelor „de la caz la caz”. Ca garanție suplimentară, AEPD sugerează limitarea transferurilor la autoritățile „a căror sarcină este combaterea terorismului sau a infracțiunilor transnaționale”, fără a include autoritățile ale căror funcții sunt „direct legate de prevenirea (acestor) infracțiuni”.

33. Agenția susține condiționarea transferurilor către țări terțe de oferirea „acelorași” garanții ca și în acordul original. Cu toate acestea, luând în considerare faptul că transferurile ulterioare implică totuși pierderea într-o anumită măsură a controlului asupra modului în care se pot prelucra datele și în lipsa unui acord internațional care să garanteze aplicarea efectivă a garanțiilor de către noii destinatari, AEPD sugerează în plus ca aceste transferuri să necesite în prealabil autorizare judiciară.

34. Propunerea prevede că, atunci când datele unui rezident al unui stat membru UE sunt transferate către o țară terță, statul membru în cauză trebuie informat dacă Serviciul vamal și de protecție a frontierelor din Australia a luat cunoștință de această situație [articolul 19.1 litera (f)]. AEPD consideră că trebuie menționate detalii suplimentare care să explice scopul acestei transmiteri către statul membru. În cazul în care această transmitere de informații afectează persoana vizată, ar trebui prevăzute justificări și garanții suplimentare.

35. În sfârșit, în ceea ce privește transferurile pe teritoriul Australiei și cele către țările terțe, atât articolul 18, cât și articolul 19 prevăd o dispoziție generală conform căreia nimic nu ar trebui să împiedice divulgarea datelor PNR în cazul în care acest lucru este necesar în sensul articolului 3 alineatul (4) ⁽¹⁾, cu alte cuvinte în cazul unor circumstanțe excepționale care impun protecția intereselor vitale ale oricărei persoane, inclusiv în caz de amenințare la adresa sănătății. AEPD a pus deja sub semnul întrebării riscul ca această excepție să fie interpretată într-un sens prea larg. În plus, agenția nu înțelege motivul pentru care orice transfer în circumstanțe excepționale nu s-ar supune garanțiilor

prevăzute la articolul 18 și articolul 19, în special în ceea ce privește limitarea scopului sau reducerea la minimum a datelor, precum și în ceea ce privește protecția identității destinatarilor și nivelul de protecție acordat datelor cu caracter personal.

2.9. Transferurile efectuate de companiile aeriene

36. În conformitate cu articolul 21.3, se pot efectua mai mult de cinci transferuri de date PNR către autorități pentru fiecare zbor, în circumstanțe excepționale, în cazul unei amenințări specifice. Pentru consolidarea securității juridice, condițiile în care au loc astfel de transferuri suplimentare ar trebui să fie mai detaliate și să cuprindă în special cerința suplimentară referitoare la existența unei amenințări imediate.

2.10. Revizuirea acordului

37. În opinia AEPD, condițiile revizuirii ar trebui să fie mai detaliate în ceea ce privește câteva aspecte. Ar trebui specificată frecvența revizuirilor ulterioare celei inițiale. În plus, autoritățile de protecție a datelor ar trebui incluse în echipa de revizuire în mod explicit și nu doar condiționat.

38. AEPD sugerează ca revizuirea să se concentreze și asupra evaluării necesității și proporționalității măsurilor, prin culegerea de date statistice privind numărul persoanelor afectate și efectiv condamnate pe baza datelor PNR, precum și privind exercitarea efectivă a drepturilor persoanelor vizate: evaluarea ar trebui să includă verificarea modului în care solicitările persoanelor vizate sunt prelucrate în practică, mai ales în cazurile în care nu s-a permis accesul direct.

3. CONCLUZIE

39. AEPD salută garanțiile prevăzute în propuneri, în special cele referitoare la punerea concretă în aplicare a acordului. În special aspectele privind securitatea datelor, supravegherea și dispozițiile referitoare la punerea în aplicare au fost elaborate în mod satisfăcător. AEPD subliniază faptul că orice persoană are acces la Autoritatea Australiană de Protecție a Datelor, precum și la autoritățile judiciare australiene. Acestea fac parte dintre garanțiile esențiale prevăzute în propuneri.

40. Cu toate acestea, AEPD a identificat și o marjă semnificativă de îmbunătățire, mai ales în ceea ce privește domeniul de aplicare al acordului, definiția terorismului și includerea unor scopuri excepționale, precum și perioada de păstrare a datelor PNR. În comparație cu sistemul PNR australian anterior, dar și cu propunerea referitoare la PNR al UE, această perioadă de păstrare este disproporționată.

⁽¹⁾ Precum și în sensul articolului 10 atunci când datele sunt transferate pe teritoriul Australiei.

41. Temeiul juridic al acordului ar trebui reexaminat. În contextul jurisprudenței constante, cu excepția articolului 218 alineatul (6) litera (a), AEPD consideră că acordul ar trebui să se întemeieze – în mod prioritar în orice caz – pe articolul 16 din Tratatul privind funcționarea Uniunii Europene și nu pe articolul 82 alineatul (1) litera (d) și pe articolul 87 alineatul (2) litera (a) din Tratatul privind funcționarea Uniunii Europene. Acest lucru este în totalitate conform cu Declarația 21 anexată la Tratatul de la Lisabona.
42. Aceste observații ar trebui interpretate în contextul mai larg al legitimității oricărui sistem PNR, privit ca o culegere sistematică de date privind pasagerii, în vederea evaluării riscurilor. Propunerea poate să îndeplinească celelalte cerințe menționate în privința protecției datelor numai dacă sistemul respectă cerințele fundamentale privind necesitatea și proporționalitatea prevăzute la articolele 7 și 8 din Carta drepturilor fundamentale și la articolul 16 din Tratatul privind funcționarea Uniunii Europene.
43. Prin urmare, AEPD conchide, de asemenea, că acestor cerințe fundamentale ar trebui să li se acorde atenție sporită în cadrul evaluărilor finale care vor preceda încheierea acordului.

Adoptat la Bruxelles, 15 iulie 2011.

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor
