

Avizul Autorității Europene pentru Protecția Datelor referitor la propunerea de decizie a Consiliului privind încheierea Acordului dintre Statele Unite ale Americii și Uniunea Europeană privind utilizarea și transferul de date din registrele cu numele pasagerilor (PNR) către Departamentul pentru Securitate Internă al Statelor Unite

(2012/C 35/03)

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR,

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

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

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⁾,

având în vedere 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, în special articolul 41 ⁽²⁾,

ADOPTĂ PREZENTUL AVIZ:

1. INTRODUCERE

1.1. Consultarea AEPD și scopul avizului

1. La 28 noiembrie 2011, Comisia a adoptat o propunere de decizie a Consiliului privind încheierea Acordului dintre Statele Unite ale Americii și Uniunea Europeană privind utilizarea și transferul de date din registrele cu numele pasagerilor (PNR) către Departamentul pentru Securitate Internă al Statelor Unite ⁽³⁾ (denumit în continuare „acordul”).
2. La 9 noiembrie 2011, Autoritatea Europeană pentru Protecția Datelor a fost consultată neoficial cu privire la proiectul de propunere, în contextul unei proceduri accelerate. La 11 noiembrie 2011, AEPD a emis mai multe observații de ordin restrâns. Scopul prezentului aviz este să completeze aceste observații prin prisma acestei propuneri și să pună la dispoziția publicului punctul său de vedere. De asemenea, prezentul aviz are la bază mai multe intervenții privind PNR, emise anterior de către AEPD și Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal.

1.2. Contextul propunerii

3. Acordul își propune să ofere un temei juridic solid pentru transferul de date PNR din UE către Statele Unite. În prezent, aceste transferuri se efectuează în baza acordului din 2007 ⁽⁴⁾, deoarece Parlamentul a hotărât să amâne votul privind aprobarea până la soluționarea motivelor sale de îngrijorare privind protecția datelor. Mai precis, în rezoluția sa din 5 mai 2010 ⁽⁵⁾, Parlamentul a făcut referire la următoarele cerințe:

⁽¹⁾ JO L 281, 23.11.1995, p. 31.

⁽²⁾ JO L 8, 12.1.2001, p. 1.

⁽³⁾ COM(2011) 807 final.

⁽⁴⁾ Acord între Uniunea Europeană și Statele Unite ale Americii privind prelucrarea și transferul datelor din registrul cu numele pasagerilor (PNR), de către transportatorii aerieni, către Departamentul pentru Securitate Internă al Statelor Unite (DHS) (Acordul PNR 2007) (JO L 204, 4.8.2007, p. 18).

⁽⁵⁾ Rezoluția Parlamentului European din 5 mai 2010 referitoare la lansarea negocierilor pentru acordurile privind Registrul cu numele pasagerilor (PNR) cu Statele Unite ale Americii, Australia și Canada (JO C 81 E, 15.3.2011, p. 70). A se vedea și rezoluția Parlamentului European din 13 martie 2003 privind transferul datelor cu caracter personal de către companiile aeriene în cazul zborurilor transatlantice (JO C 61 E, 10.3.2004, p. 381), rezoluția sa din 9 octombrie 2003 privind transferul datelor personale de către companiile aeriene în cazul zborurilor transatlantice: stadiul negocierilor cu SUA (JO C 81 E, 31.3.2004, p. 105), rezoluția sa din 31 martie 2004 referitoare la proiectul de decizie a Comisiei stabilind nivelul corespunzător de protecție prevăzut pentru datele personale conținute de registrele cu numele pasagerilor (PNR) transferate către Biroul Vămilelor și Protecției Frontierelor al Statelor Unite (JO C 103 E, 29.4.2004, p. 665), recomandarea sa din 7 septembrie 2006 adresată Consiliului referitoare la negocierile în vederea unui acord cu SUA cu privire la utilizarea datelor din registrele cu numele pasagerilor (PNR) pentru prevenirea și combaterea terorismului și a criminalității transnaționale, inclusiv a criminalității organizate (JO C 305 E, 14.12.2006, p. 250), rezoluția sa din 14 februarie 2007 privind SWIFT, acordul PNR și dialogul transatlantic pe aceste teme (JO C 287 E, 29.11.2007, p. 349) și rezoluția sa din 12 iulie 2007 referitoare la acordul privind registrul pentru evidența călătorilor (PNR) cu Statele Unite ale Americii [texte adoptate, P6_TA(2007)0347]. Toate sunt disponibile la <http://www.europarl.europa.eu>

- conformitatea cu legislația privind protecția datelor, la nivel național și european;
 - o evaluare de impact asupra vieții private înainte de adoptarea oricărui instrument legislativ;
 - un test de proporționalitate care să demonstreze că instrumentele juridice existente nu sunt suficiente;
 - limitarea strictă a scopului ⁽⁶⁾ și limitarea utilizării datelor PNR la infracțiuni sau amenințări specifice, de la caz la caz;
 - limitarea volumului de date care urmează a fi colectate;
 - perioade limitate de păstrare;
 - interzicerea extragerii de date și a realizării de profiluri psihologice;
 - interzicerea deciziilor automatizate care afectează cetățenii în mod semnificativ ⁽⁷⁾;
 - mecanisme adecvate de revizuire independentă, supraveghere judiciară și control democratic;
 - toate transferurile internaționale trebuie să fie în conformitate cu standardele UE în materie de protecție a datelor și să facă obiectul unei constatări a adecvării.
4. Prezentul acord trebuie să fie interpretat în contextul unei abordări globale a PNR, care include negocieri cu alte țări terțe (respectiv Australia ⁽⁸⁾ și Canada ⁽⁹⁾), precum și al propunerii de sistem PNR la nivelul Uniunii Europene ⁽¹⁰⁾. De asemenea, acesta intră în sfera negocierilor privind un acord între UE și SUA referitor la schimbul de date cu caracter personal în cadrul cooperării polițienești și judiciare în materie penală ⁽¹¹⁾. Într-un context mai larg, acordul a fost parafat cu câteva săptămâni înainte de data preconizată pentru adoptarea propunerilor de revizuire a cadrului general de protecție a datelor ⁽¹²⁾.
5. AEPD salută această abordare globală menită să ofere un cadru juridic coerent pentru acordurile PNR, în concordanță cu cerințele juridice ale Uniunii Europene. Cu toate acestea, AEPD regretă că, în practică, calendarul stabilit nu permite asigurarea consecvenței acordurilor cu noile norme ale UE privind protecția datelor. De asemenea, dorește să amintească faptul că acordului UE-SUA privind PNR ar trebui să i se aplice prevederile acordului general dintre UE și SUA referitor la schimburile de date.
-
- ⁽⁶⁾ Limitat la motive de aplicare a legii și de securitate în cazurile grave de criminalitate organizată sau transnațională sau de terorism cu caracter transfrontalier, în temeiul definițiilor prevăzute de Decizia-cadru 2002/475/JAI a Consiliului din 13 iunie 2002 privind combaterea terorismului (JO L 164, 22.6.2002, p. 3) și de Decizia-cadru 2002/584/JAI a Consiliului din 13 iunie 2002 privind mandatul european de arestare (JO L 190, 18.7.2002, p. 1).
- ⁽⁷⁾ „Nicio decizie de interdicție de zbor și nicio decizie de investigare sau punere sub urmărire nu poate fi luată exclusiv pe baza unor astfel de căutări automatizate sau de consultări ale bazelor de date.”
- ⁽⁸⁾ 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, semnat la 29 septembrie 2011.
- ⁽⁹⁾ Acord între Comunitatea Europeană și Guvernul Canadei privind prelucrarea informațiilor prelabile referitoare la pasagerii și la dosarele pasagerilor (JO L 82, 21.3.2006, p. 15).
- ⁽¹⁰⁾ Propunere de directivă a Parlamentului European și a Consiliului privind utilizarea datelor din registrul cu numele pasagerilor pentru prevenirea, depistarea, cercetarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave (COM/2011/0032 final).
- ⁽¹¹⁾ La 3 decembrie 2010, Consiliul a autorizat inițierea negocierilor în scopul încheierii unui acord între UE și SUA privind protecția datelor cu caracter personal în momentul transferării și prelucrării în scopul prevenirii, anchetării, detectării sau urmăririi penale a infracțiunilor, inclusiv a actelor de terorism, în cadrul cooperării polițienești și judiciare în materie penală. A se vedea comunicatul de presă al Comisiei la <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1661>
- ⁽¹²⁾ A se vedea Comunicarea Comisiei „O abordare globală a protecției datelor cu caracter personal în Uniunea Europeană”, 4 noiembrie 2010, COM(2010) 609 final, precum și continuarea acesteia.

2. OBSERVAȚII GENERALE

6. În conformitate cu Carta drepturilor fundamentale a Uniunii Europene, orice limitare a drepturilor și libertăților fundamentale trebuie să fie necesară, proporțională și stabilită prin lege. După cum au declarat în mod repetat AEPD⁽¹³⁾ și Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal⁽¹⁴⁾, necesitatea și proporționalitatea sistemelor PNR, precum și a transferurilor în bloc de date PNR către țările terțe, nu au fost încă demonstrate. Această părere este împărtășită și de Comitetul Economic și Social European, precum și de Agenția pentru Drepturi Fundamentale⁽¹⁵⁾. Observațiile specifice expuse în continuare nu aduc atingere acestei observații preliminare fundamentale.
7. Cu toate că prezentul acord prezintă unele îmbunătățiri în comparație cu acordul din 2007 și include garanții corespunzătoare privind controlul și securitatea datelor, acesta nu pare să soluționeze niciunul dintre principalele motive de îngrijorare exprimate în avizele menționate și nici nu pare să îndeplinească condițiile impuse de Parlamentul European pentru obținerea aprobării sale⁽¹⁶⁾.

3. OBSERVAȚII SPECIFICE

3.1. Scopul trebuie clarificat

8. Articolul 4 alineatul (1) din acord prevede că Statele Unite prelucrează date PNR în scopul prevenirii, depistării, cercetării și urmăririi penale a: (a) infracțiunilor teroriste și a infracțiunilor asociate terorismului; și (b) infracțiunilor care pot fi sancționate cu pedepse cu închisoarea pentru trei ani sau mai mult și care au caracter transnațional. Unele dintre aceste concepte sunt definite suplimentar.
9. Cu toate că aceste definiții sunt mai precise decât în acordul din 2007, există încă excepții și concepte vagi care ar putea să prevaleze asupra limitării scopului și să submineze securitatea juridică. În mod special:
- la articolul 4 alineatul (1) litera (a) punctul (i), formularea „comportamentul care [...] pare să aibă ca scop intimidarea sau constrângerea” [sau] „influențarea politicii unui guvern” s-ar putea referi și la activități care nu pot fi considerate infracțiuni teroriste în conformitate cu Decizia-cadru 2002/475/JAI a Consiliului⁽¹⁷⁾. Pentru a exclude această posibilitate, ar trebui ca noțiunile „a părea să”, „intimidare” și „influențare” să fie clarificate;
 - articolul 4 alineatul (1) litera (b) ar trebui să cuprindă o listă de infracțiuni specifice. Referirea la „alte infracțiuni care pot fi sancționate cu pedepse cu închisoarea pentru trei ani sau mai mult” nu este suficientă, întrucât acest prag presupune infracțiuni diferite în Uniunea Europeană și Statele Unite ale Americii, respectiv în diversele state membre ale UE și statele membre ale SUA;

⁽¹³⁾ 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 infracțiunilor de terorism și a infracțiunilor grave; Avizul AEPD din 15 iulie 2011 referitor la propunerea de decizie a Consiliului privind încheierea unui acord între Uniunea Europeană și Australia privind prelucrarea și transferul datelor PNR de către transportatorii aerieni către Serviciul vamal și de protecție a frontierelor din Australia; Avizul AEPD din 19 octombrie 2010 cu privire la abordarea globală referitoare la transferul de date PNR către țări terțe, precum și Avizul AEPD din 20 decembrie 2007 referitor la propunerea de decizie-cadru a Consiliului privind utilizarea datelor PNR în scopul aplicării legii. Toate sunt disponibile la <http://www.edps.europa.eu>

⁽¹⁴⁾ Avizul nr. 10/2011 al Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal 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 infracțiunilor de terorism și a infracțiunilor grave; Avizul nr. 7/2010 cu privire la Comunicarea Comisiei Europene privind o abordare globală referitoare la transferul de date din registrul cu numele pasagerilor (PNR) către țări terțe; Avizul nr. 5/2007 cu privire la noul acord între Uniunea Europeană și Statele Unite ale Americii privind prelucrarea și transferul de date din registrul cu numele pasagerilor (PNR), de către transportatorii aerieni, către Departamentul pentru Securitate Internă al Statelor Unite, încheiat în iulie 2007, precum și Avizul nr. 4/2003 privind nivelul de protecție asigurat în SUA pentru transferul datelor pasagerilor. Toate sunt disponibile la http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2011_en.htm

⁽¹⁵⁾ Avizul FRA din 14 iunie 2011 privind propunerea de directivă privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, cercetarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave (disponibil la <http://fra.europa.eu/fraWebsite/attachments/FRA-PNR-Opinion-June2011.pdf>) și Avizul CESE din 5 mai 2011 privind 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 infracțiunilor de terorism și a infracțiunilor grave (disponibil la <http://www.eesc.europa.eu/?i=portal.en.soc-opinions.15579>).

⁽¹⁶⁾ A se vedea nota de subsol nr. 5.

⁽¹⁷⁾ Decizia-cadru 2002/475/JAI a Consiliului din 13 iunie 2002 privind combaterea terorismului (JO L 164, 22.6.2002, p. 3).

- infracțiunile minore ar trebui să fie excluse în mod explicit din scopul acestui acord;
- la articolul 4 alineatul (2) ar trebui definit conceptul de „amenințare gravă”, iar utilizarea datelor PNR dacă „s-a emis un ordin judecătoresc” ar trebui să se limiteze la cazurile menționate la articolul 4 alineatul (1);
- în mod similar, pentru a se evita aplicarea articolului 4 alineatul (3) în scopuri precum controlul la frontieră, ar trebui să se specifice că doar persoanele suspectate de a fi luat parte la oricare dintre infracțiunile enumerate la articolul 4 alineatul (1) pot să fie „supuse unui interogatoriu sau unei examinări mai riguroase”.

3.2. Lista datelor PNR care urmează să fie transferate ar trebui restrânsă

10. Anexa I la acord menționează 19 tipuri de date care urmează să fie transmise către Statele Unite. Majoritatea acestora cuprind și categorii diferite de date și sunt identice câmpurilor de date menționate în acordul din 2007, pe care AEPD și Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal le considerau deja disproporționate ⁽¹⁸⁾.
11. Este vorba în mod special despre câmpul „Observații generale, inclusiv informații OSI ⁽¹⁹⁾, SSI ⁽²⁰⁾ și SSR ⁽²¹⁾”, care poate divulga date privind convingerile religioase (de exemplu, preferințele alimentare) sau sănătatea (de exemplu, solicitarea unui scaun rulant). Astfel de date sensibile ar trebui să fie excluse din listă în mod explicit.
12. La evaluarea proporționalității listei ar trebui să se ia în considerare și faptul că, datorită transmiterii prealabile [articolul 15 alineatul (3) din acord], aceste categorii nu se referă doar la pasagerii efectivi, ci și la persoanele care nu mai zboară în cele din urmă (de exemplu, din cauza anulărilor).
13. În plus, prezența unor câmpuri de date deschise ar putea să submineze securitatea juridică. Categoriile de tipul „toate informațiile de contact disponibile”, „toate informațiile cu privire la bagaje” și „observații generale” ar trebui să fie mai bine definite.
14. Prin urmare, lista ar trebui să fie restrânsă. În conformitate cu avizul Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal ⁽²²⁾, considerăm că datele ar trebui să se limiteze la următoarele informații: codul de localizare a dosarului PNR, data rezervării, data (datele) prevăzută (prevăzute) a(le) călătoriei, numele pasagerului, alte nume care figurează în PNR, itinerariul complet, elementele de identificare ale biletelor gratuite, biletele dus, informații privind locul emiterii biletului, date privind costurile biletelor prelucrate automat (*Automatic Ticket Fare Quote*, ATFQ), numărul biletului, data emiterii biletului, date referitoare la neprezentarea la îmbarcare, numărul de bagaje, numerele etichetelor de bagaje, pasagerii de ultim moment fără rezervare, numărul de bagaje pe fiecare segment, transferurile voluntare/involuntare la o clasă superioară, istoricul modificărilor datelor PNR cu privire la elementele enumerate mai sus.

3.3. DHS nu ar trebui să prelucreze date sensibile

15. Articolul 6 din acord prevede că DHS filtrează și „maschează” datele sensibile în mod automat. Cu toate acestea, datele sensibile sunt stocate timp de minimum 30 de zile și pot fi utilizate în cazuri specifice [articolul 6 alineatul (4)]. AEPD dorește să sublinieze că aceste date rămân „sensibile” chiar și după „mascare” și se referă la persoane fizice identificabile.
16. După cum s-a menționat deja de către AEPD, DHS nu ar trebui să prelucreze date sensibile referitoare la cetățenii Uniunii Europene, chiar dacă aceste date sunt „mascate” în momentul primirii. AEPD recomandă ca textul acordului să specifice că transportatorii aerieni nu trebuie să transfere date sensibile către DHS.

⁽¹⁸⁾ A se vedea avizele AEPD și avizul Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal citate mai sus.

⁽¹⁹⁾ Alte informații privind serviciile.

⁽²⁰⁾ Informații privind serviciile speciale.

⁽²¹⁾ Cereri de servicii speciale.

⁽²²⁾ A se vedea Avizul nr. 4/2003 al Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, citat mai sus.

3.4. Perioada de păstrare este excesivă

17. Articolul 8 prevede că datele PNR se păstrează într-o bază de date activă pentru o perioadă de până la cinci ani, după care sunt transferate într-o bază de date pasivă, în care sunt păstrate timp de cel mult zece ani. Această perioadă maximă de păstrare de 15 ani este în mod clar disproporționată, indiferent dacă datele se păstrează în baze de date „active” sau „pasive”, după cum au subliniat deja AEPD și Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal.
18. Articolul 8 alineatul (1) specifică faptul că datele sunt „depersonalizate și mascate” după șase luni de la primirea de către DHS. Cu toate acestea, atât datele „mascate”, cât și cele stocate într-o „bază de date pasivă” sunt date cu caracter personal atât timp cât nu sunt anonimizate. Prin urmare, datele ar trebui să fie anonimizate (irreversibil) sau șterse imediat după analiză ori după cel mult 6 luni.

3.5. Utilizarea metodei „push” și frecvența transferurilor

19. AEPD salută prevederile articolului 15 alineatul (1), conform cărora datele se transferă prin intermediul metodei „push”. Cu toate acestea, articolul 15 alineatul (1) impune transportatorilor să „permită accesul” la datele PNR în circumstanțe excepționale. Pentru a face definitiv imposibilă utilizarea sistemului de tip „pull” și din perspectiva motivelor de îngrijorare subliniate recent încă o dată de către Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal⁽²³⁾, recomandăm insistent ca acordul să interzică în mod explicit posibilitatea ca funcționarii SUA să acceseze datele în mod separat prin intermediul unui sistem de tip „pull”.
20. Acordul ar trebui să definească numărul și periodicitatea transferurilor efectuate de transportatorii aerieni către DHS. De asemenea, pentru consolidarea securității juridice, ar trebui să se detalieze condițiile în care s-ar permite efectuarea unor transferuri suplimentare.

3.6. Securitatea datelor

21. AEPD salută articolul 5 din acord, referitor la securitatea și integritatea datelor, în special obligația de a notifica persoanele afectate în cazul unui incident de încălcare a vieții private. Cu toate acestea, ar trebui ca următoarele elemente ale notificării privind încălcarea securității datelor să fie clarificate:
- destinarii notificării: ar trebui să se specifice care sunt „autoritățile europene competente” ce trebuie să fie informate. În orice caz, autoritățile naționale de protecție a datelor ar trebui să se numere printre acestea. De asemenea, ar trebui să fie înștiințată și o autoritate competentă din Statele Unite;
 - pragul notificării transmise acestor autorități: ar trebui să se definească ce constituie „incident semnificativ de încălcare a vieții private”;
 - conținutul notificării transmise persoanelor fizice și autorităților ar trebui să fie specificat.
22. AEPD susține obligația de a înregistra sau documenta toate sesiunile de acces și prelucrare a datelor PNR, întrucât în acest mod se poate verifica dacă DHS a utilizat datele PNR în mod corespunzător și dacă au fost cazuri de acces neautorizat la sistem.

3.7. Supraveghere și punere în aplicare

23. AEPD salută faptul că respectarea garanțiilor privind protejarea vieții private menționate în prezentul acord face obiectul supravegherii și controlului independent al unor inspecțiuni pentru protecția confidențialității, precum inspectorul-șef pentru protecția confidențialității (*Chief Privacy Officer*) al

⁽²³⁾ A se vedea scrisoarea din 19 ianuarie 2011 a Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, adresată comisarului Malmström și având ca obiect acordurile privind PNR încheiate de Uniunea Europeană cu SUA, Canada și Australia.

DHS, după cum se prevede la articolul 14 alineatul (1). Cu toate acestea, pentru a asigura exercitarea eficientă a drepturilor persoanelor vizate, AEPD și autoritățile naționale de protecție a datelor ar trebui să colaboreze cu DHS în privința procedurilor și modalităților de exercitare a acestor drepturi⁽²⁴⁾. AEPD ar aprecia dacă acordul ar conține o referire la această cooperare.

24. AEPD susține cu tărie dreptul de a formula căi de atac „indiferent de naționalitate, țară de origine sau reședință”, prevăzut la cel de al doilea paragraf din articolul 14 alineatul (1). Cu toate acestea, regretă că articolul 21 prevede în mod explicit că acordul „nu creează și nu conferă, în temeiul legislației Statelor Unite, drepturi sau beneficii niciunei persoane”. Chiar dacă acordul garantează dreptul la „revizuire judiciară” în SUA, acesta poate să nu fie echivalent cu dreptul la un control jurisdicțional efectiv în Uniunea Europeană, în special prin prisma restricției prevăzute la articolul 21.

3.8. Transferuri naționale și internaționale ulterioare

25. Articolul 16 din acord interzice transferul de date către autoritățile naționale care nu aplică în cazul datelor PNR garanții „echivalente sau comparabile” cu cele prevăzute în prezentul acord. AEPD salută această dispoziție. Cu toate acestea, ar trebui ca lista autorităților care ar putea să primească date PNR să fie specificată în mai mare detaliu. În ceea ce privește transferurile internaționale, acordul prevede că acestea ar trebui să aibă loc numai dacă destinatarul intenționează să utilizeze datele în conformitate cu prezentul acord și dacă se prezintă garanții privind protejarea vieții private „comparabile” cu cele prevăzute în acord, cu excepția situațiilor de urgență.
26. În ceea ce privește termenii „comparabile” sau „echivalente” utilizați în acord, AEPD dorește să sublinieze că DHS nu ar trebui să efectueze niciun fel de transferuri naționale sau internaționale ulterioare dacă destinatarul nu prezintă garanții cel puțin la fel de stricte ca cele stabilite în prezentul acord. De asemenea, ar trebui ca acordul să specifice că transferul de date PNR se realizează de la caz la caz, asigurându-se faptul că se transferă către destinatarul relevanți doar datele necesare, fără să se permită excepții. În plus, AEPD recomandă ca transferurile de date către țări terțe să facă în prealabil obiectul unei autorizări judiciare.
27. Articolul 17 alineatul (4) prevede că, atunci când datele unui rezident al unui stat membru al UE sunt transferate către o țară terță, autoritățile competente din statul membru în cauză trebuie să fie informate în cazul în care DHS are cunoștință de această situație. Această condiție ar trebui eliminată, întrucât DHS ar trebui să fie informat în permanență cu privire la transferurile ulterioare către țări terțe.

3.9. Forma și examinarea acordului

28. Nu este clar ce formă juridică au ales Statele Unite pentru încheierea prezentului acord și nici în ce mod va căpăta acest acord caracter juridic obligatoriu în SUA. Aceste aspecte ar trebui să fie clarificate.
29. Articolul 20 alineatul (2) abordează aspectul coerenței cu eventualul sistem PNR al UE. AEPD constată că în cadrul consultărilor privind modificarea prezentului acord trebuie să se stabilească în special „dacă orice viitor sistem PNR al UE ar aplica standarde de protecție a datelor mai puțin stricte decât cele prevăzute de prezentul acord”. În vederea asigurării coerenței, eventualele modificări ar trebui să ia în considerare și (mai ales) prevederea unor garanții mai puternice în orice viitor sistem PNR.
30. De asemenea, acordul ar trebui să fie examinat în contextul noului cadru de protecție a datelor, precum și în contextul eventualei încheieri de către Uniunea Europeană și Statele Unite a unui acord general cu privire la schimbul de date cu caracter personal în cadrul cooperării polițienești și judiciare în materie penală. Se poate adăuga o nouă prevedere, similară articolului 20 alineatul (2), care să menționeze următoarele: „în cazul în care și atunci când se adoptă un nou cadru juridic de protecție a datelor în

⁽²⁴⁾ De exemplu, Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal a oferit deja orientări privind furnizarea de informații către pasagerii (a se vedea Avizul nr. 2/2007 al Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal cu privire la informațiile furnizate pasagerilor referitoare la transferul de date PNR către autoritățile SUA, disponibil la http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp151_en.pdf).

Uniunea Europeană sau se încheie un nou acord privind schimbul de date între UE și Statele Unite, părțile se consultă pentru a stabili dacă prezentul acord trebuie să fie modificat în consecință. Aceste consultări trebuie să analizeze, în special, dacă eventuala modificare ulterioară a cadrului juridic de protecție a datelor în Uniunea Europeană sau eventualul acord UE-SUA privind protecția datelor ar aplica garanții de protecție a datelor mai stricte decât cele prevăzute de prezentul acord”.

31. În ceea ce privește examinarea acordului (articolul 23), AEPD consideră că autoritățile naționale de protecție a datelor trebuie să fie incluse în mod explicit în echipa însărcinată cu examinarea. De asemenea, examinarea ar trebui să se concentreze și pe evaluarea necesității și proporționalității măsurilor, precum și pe exercitarea efectivă a drepturilor persoanelor vizate, și să includă verificarea modului în care se prelucrează în practică solicitările persoanelor vizate, în mod special în cazul în care nu se permite accesul direct. Ar trebui să se specifice frecvența examinărilor.

4. CONCLUZIE

32. AEPD salută garanțiile privind controlul și securitatea datelor prevăzute în acord, precum și îmbunătățirile acestuia în comparație cu acordul din 2007. Cu toate acestea, rămân numeroase motive de îngrijorare, în mod special în ceea ce privește coerența abordării globale a PNR, limitarea scopului, categoriile de date care urmează să fie transferate către DHS, prelucrarea datelor sensibile, perioada de păstrare, excepțiile de la metoda „push”, drepturile persoanelor vizate și transferurile ulterioare.
33. Aceste observații nu aduc atingere cerințelor privind necesitatea și proporționalitatea oricărui acord și sistem PNR legitim care prevede transferul în bloc de date PNR din Uniunea Europeană spre țări terțe. După cum a reiterat Parlamentul European în rezoluția sa din 5 mai, „necesitatea și proporționalitatea reprezintă principii esențiale, fără de care lupta împotriva terorismului nu va fi niciodată eficientă”.

Adoptat la Bruxelles, 9 decembrie 2011.

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor
