

**Avizul Autorității Europene pentru Protecția Datelor cu privire la Comunicarea Comisiei privind o abordare globală referitoare la transferul de date din registrul cu numele pasagerilor (PNR) către țări terțe**

(2010/C 357/02)

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 articolul 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 <sup>(1)</sup>,

având în vedere solicitarea unui aviz formulată în conformitate cu 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 <sup>(2)</sup>,

ADOPTĂ PREZENTUL AVIZ:

## I. INTRODUCERE

### 1. Consultarea AEPD

1. La 21 septembrie 2010, Comisia a adoptat o comunicare privind o abordare globală referitoare la transferul de date din registrul cu numele pasagerilor (PNR) către țări terțe <sup>(3)</sup>. Comunicarea a fost transmisă AEPD spre consultare în aceeași zi.
2. AEPD salută faptul că a fost consultată de către Comisie. AEPD a avut ocazia de a formula observații neoficiale chiar înainte de adoptarea comunicării. Unele dintre aceste observații au fost luate în considerare în versiunea finală a documentului, în schimb alte puncte generează în continuare îngrijorări în ceea ce privește protecția datelor.

### 2. Propunerea și contextul acesteia

3. Abordarea globală a aspectelor în materie de PNR prezentată de Comisie în comunicarea sa vizează furnizarea unui cadru coerent pentru transmiterea datelor PNR către

țări terțe. În afară de necesitatea asigurării securității juridice, prezentată pe larg în cadrul comunicării, această abordare armonizată a fost susținută puternic de către Parlamentul European, căruia i s-a încredințat, în noul cadru instituțional, competența de a ratifica acorduri PNR cu țările terțe <sup>(4)</sup>.

4. Comunicarea este completată de recomandări cu privire la negocierile acordurilor PNR cu anumite țări terțe. Aceste recomandări sunt de ordin restrâns și nu sunt analizate în prezentul aviz. Cu toate acestea, relația dintre comunicarea generală și recomandări este comentată în capitolul II.
5. În plus față de abordarea globală referitoare la transferul de date PNR către țări terțe, Comisia pregătește și o abordare revizuită referitoare la PNR, pentru UE. Anterior, o propunere privind un astfel de cadru UE a fost discutată intens în Consiliu, în cadrul fostului pilon al treilea, înainte de intrarea în vigoare a Tratatului de la Lisabona <sup>(5)</sup>. Aceste discuții nu s-au soldat cu un consens în legătură cu o serie de elemente esențiale ale sistemului PNR, cum ar fi, de exemplu, utilizarea bazei de date create în cadrul unui astfel de sistem. Ulterior, Programul de la Stockholm a impulsionat Comisia să facă o nouă propunere, dar aceasta nu a rezolvat elementele esențiale ale acestei propuneri. Un proiect de directivă pentru un sistem UE de utilizare a registrului cu numele pasagerilor (UE PNR) este așteptat la începutul anului 2011.
6. Prezentul aviz se concentrează asupra comunicării Comisiei. Prima parte a acestuia analizează comunicarea în contextul actualelor evoluții în domeniul protecției datelor, a doua parte abordează legitimitatea sistemului PNR, iar a treia parte se concentrează asupra unor aspecte mai specifice privind protecția datelor abordate în comunicare.

<sup>(4)</sup> Au fost semnate acorduri cu:

- Statele Unite: 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 (DHS) (Acordul PNR 2007) (JO L 204, 4.8.2007, p. 18);
- Canada: Acord între Comunitatea Europeană și Guvernul Canadei privind prelucrarea informațiilor prealabile referitoare la pasageri și a datelor din registrul cu numele pasagerilor (JO L 82, 21.3.2006, p. 15);
- Australia: Acord între Uniunea Europeană și Australia privind prelucrarea și transferul de către transportatorii aerieni către Serviciul vamal australian a datelor din registrul de nume al pasagerilor (PNR) provenind din Uniunea Europeană (JO L 213, 8.8.2008, p. 49-57).

<sup>(5)</sup> La 6 noiembrie 2007, Comisia a adoptat o propunere de decizie-cadru a Consiliului privind utilizarea datelor din registrul cu numele pasagerilor (PNR) în scopul aplicării legii [COM(2007) 654 final]. AEPD și-a prezentat avizul referitor la această propunere la 20 decembrie 2007 (JO C 110, 1.5.2008, p. 1).

<sup>(1)</sup> JO L 281, 23.11.1995, p. 31.

<sup>(2)</sup> JO L 8, 12.1.2001, p. 1.

<sup>(3)</sup> COM(2010) 492 final.

## II. ANALIZA PROPUNERII

### 1. Observații generale

7. AEPD salută abordarea orizontală a comunicării, în concordanță cu cerințele recente ale Parlamentului European referitoare la o analiză amănunțită și o perspectivă coerentă asupra sistemelor PNR existente și preconizate. Atingerea unui nivel ridicat și armonizat de protecție aplicabil tuturor acestor sisteme reprezintă un obiectiv care ar trebui să fie puternic susținut.
8. AEPD pune totuși sub semnul întrebării sincronizarea generală a diferitelor inițiative legate în mod direct sau indirect de prelucrarea datelor PNR.
9. Deși comunicarea menționează acordurile internaționale privind sistemele PNR și inițiativa privind un sistem UE PNR, standardele propuse în comunicare se referă doar la acordurile internaționale. Cadrul UE va fi discutat și elaborat într-o etapă ulterioară.
10. O agendă mai logică și mai oportună ar fi inclus, din punctul de vedere al AEPD, o reflecție aprofundată asupra unui eventual sistem UE care să includă garanții privind protecția datelor conforme cu cadrul juridic al UE și, pe această bază, conceperea unei abordări pentru acordurile cu țări terțe.
11. De asemenea, AEPD subliniază activitatea aflată în curs de desfășurare în legătură cu un acord general UE-SUA privind punerea în comun a datelor în scopul aplicării legii <sup>(1)</sup>, al cărui obiectiv este de a stabili un set de principii care să garanteze un nivel înalt de protecție a datelor cu caracter personal ca o condiție a schimbului de astfel de date cu Statele Unite. Rezultatul negocierilor dintre UE și SUA ar trebui să constituie un punct de referință pentru acordurile bilaterale ulterioare încheiate de UE și statele membre, inclusiv acordul PNR dintre UE și SUA.
12. Un alt element care trebuie luat în considerare în acest context este reflecția generală asupra cadrului UE de protecție a datelor, activitate desfășurată în prezent de către Comisie, în vederea adoptării unei comunicări înainte de sfârșitul anului 2010, care să fie urmată de o propunere pentru un nou cadru de reglementare în cursul anului 2011 <sup>(2)</sup>. Acest proces de revizuire are loc în cadrul
- „post-Lisabona”, ceea ce are un impact direct asupra aplicării orizontale a principiilor de protecție a datelor pentru foștii piloni ai UE, incluzând cooperarea polițienească și judiciară în materie penală.
13. Pentru a asigura coerența, UE ar trebui să convină asupra instrumentelor sale interne și pe baza acestor instrumente interne să negocieze acorduri cu țările terțe. Prin urmare, agenda globală ar trebui să se concentreze mai întâi asupra cadrului general UE de protecție a datelor, apoi asupra eventualei necesități a unui sistem UE PNR, iar în final asupra condițiilor privind schimburile cu țări terțe, pe baza cadrului UE actualizat. În această etapă, la stabilirea condițiilor pentru transferul de date PNR către țări terțe ar trebui avute în vedere și garanțiile preconizate într-un viitor acord UE-SUA.
14. AEPD este conștientă de faptul că, din diferite motive de natură procedurală sau politică, această ordine ideală nu este urmată în practică. AEPD consideră, totuși, că logica ce stă la baza acestor etape diferite ar trebui avută în vedere de către diverșii actori implicați din cadrul Comisiei, Consiliului și Parlamentului. Întrucât evoluțiile, în special în legătură cu cadrul UE și negocierile UE-SUA, au loc în paralel, trebuie luată în considerare în mod corespunzător necesitatea coerenței și a unei perspective armonizate asupra garanțiilor privind protecția datelor în cadrul UE și în contextul transferurilor. Mai concret, aceasta ar implica în special:
- luarea în considerare a rezultatelor evaluării impactului asupra UE PNR înainte de finalizarea oricăror negocieri cu țări terțe privind PNR;
  - asigurarea însușirii unor învățăminte în urma analizei actualelor mecanisme privind PNR;
  - și, în ceea ce privește negocierile cu Statele Unite, corelarea negocierilor privind PNR cu negocierile referitoare la acordul general privind punerea în comun a datelor în scopul aplicării legii. Aceasta este singura modalitate de a asigura existența unor garanții coerente în ambele acorduri.
15. În cele din urmă, AEPD ridică problema legăturii dintre comunicare și orientările redactate de către Comisie. Această chestiune se referă la măsura în care ar trebui specificate garanții și condiții precise în standardele elaborate în comunicare sau în orientările stabilite pentru fiecare țară: dacă obiectivul general este acela al armonizării condițiilor pentru prelucrarea și schimbul de date privind PNR, AEPD consideră că spațiul de manevră pentru fiecare acord internațional ar trebui să fie cât mai limitat cu putință, iar standardele ar trebui să stabilească un cadru precis. Standardele trebuie să aibă un impact efectiv asupra conținutului acordurilor. Câteva dintre observațiile formulate în cele ce urmează pun în discuție necesitatea unei precizii sporite în acest sens.

<sup>(1)</sup> A se vedea în special consultarea demarată de Comisie în ianuarie 2010 referitoare la viitorul acord internațional dintre Uniunea Europeană (UE) și Statele Unite ale Americii (SUA) privind protecția datelor cu caracter personal și punerea în comun a informațiilor în scopul aplicării legii, precum și contribuțiile Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal și ale AEPD, disponibile la: [http://ec.europa.eu/justice/news/consulting\\_public/news\\_consulting\\_0005\\_en.htm](http://ec.europa.eu/justice/news/consulting_public/news_consulting_0005_en.htm)

<sup>(2)</sup> Comisia a demarat un proces de revizuire a cadrului juridic actual, care a început cu o conferință la nivel înalt în luna mai 2009. Aceasta a fost urmată de o consultare publică până la sfârșitul anului 2009 și de mai multe reuniuni de consultare ale părților interesate în luna iulie 2010. Contribuția Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, în cadrul căruia AEPD a participat activ, este disponibilă la: [http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index\\_en.htm#general\\_issues](http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm#general_issues)

## 2. Legitimitatea sistemului

16. AEPD, precum și Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal au insistat deja într-o serie de avize<sup>(1)</sup> asupra necesității unei justificări clare pentru elaborarea de sisteme PNR, fie acestea în cadrul UE, fie destinate schimbului de date cu țările terțe. Necesitatea măsurilor trebuie stabilită și susținută cu dovezi concrete, iar apoi ar trebui evaluată și pusă în balanță cu gradul de intruziune în viața privată a persoanelor, pentru a asigura obținerea unui rezultat proporțional și cât mai puțin invaziv. Faptul că evoluțiile tehnologice recente fac posibile în prezent accesul pe scară largă și analiza, după cum se afirmă la sfârșitul punctului 2.2 al comunicării, nu reprezintă o justificare în sine pentru crearea unui sistem menit să realizeze un control de securitate al tuturor călătorilor. Cu alte cuvinte: disponibilitatea mijloacelor nu trebuie să justifice scopul.
17. După cum se explică în cele ce urmează, AEPD consideră că transferarea în bloc a datelor referitoare la persoane inocente în scopul evaluării riscului ridică probleme serioase de proporționalitate. AEPD contestă în special utilizarea proactivă a datelor PNR. Deși utilizarea „re-activă” a datelor nu dă naștere unor îngrijorări majore, atâta timp cât ea face parte dintr-o investigație a unei infracțiuni comise deja, utilizarea proactivă și în timp real este evaluată mai critic.
18. Potrivit formulării comunicării, chiar și în „contextul timpului real”, datele PNR vor fi „utilizate pentru prevenirea unei infracțiuni, supravegherea sau arestarea unor persoane înainte de săvârșirea unei infracțiuni”, pe baza unor „indicatori de risc factuali prestabiliți”<sup>(2)</sup>. Ideea principală a luării unor măsuri față de persoane înainte de săvârșirea unei infracțiuni pe baza unor indicatori de risc reprezintă, din punctul de vedere al AEPD, o măsură proactivă, a cărei utilizare într-un context de aplicare a legii este în mod tradițional definită în mod strict și limitată.
19. În plus, nici noțiunea de indicatori de risc, nici cea de „evaluare a riscului” nu sunt elaborate suficient, iar cea din urmă ar putea fi confundată ușor cu noțiunea de „elaborare de profile”. Similitudinea este întărită și mai mult de obiectivul presupus, acela al stabilirii unor „modele factuale de deplasare și de comportament”. AEPD pune sub semnul întrebării legătura dintre faptele inițiale și modelele deduse din aceste fapte. Procesul are ca scop supunerea unei persoane la o evaluare de risc – și eventual la unele măsuri de coerciție – pe baza unor fapte care nu au legătură cu persoana respectivă. După cum s-a afirmat deja în avizul anterior referitor la o propunere de PNR al UE, principala preocupare a AEPD este legată de faptul că „se vor lua decizii în privința persoanelor pe baza modelelor și criteriilor stabilite

folosind datele despre pasageri în general. Astfel, s-ar putea lua o decizie cu privire la o persoană utilizându-se ca referință (cel puțin parțial) modele extrase din datele despre alte persoane. Se vor lua, astfel, decizii în legătură cu un context teoretic, fapt ce poate afecta în mare măsură persoanele vizate. Pentru persoane, este foarte dificil să se apere în fața unor astfel de decizii”<sup>(3)</sup>.

20. Utilizarea pe scară largă a unor astfel de tehnici care presupun controlul de securitate al tuturor pasagerilor ridică, prin urmare, întrebări serioase referitoare la respectarea principiilor fundamentale de protecție a vieții private și a datelor, inclusiv a celor prevăzute la articolul 8 din CEDO, la articolele 7 și 8 din Cartă și la articolul 16 din Tratatul privind funcționarea Uniunii Europene.
21. Orice decizie definitivă cu privire la legitimitatea sistemelor PNR ar trebui să țină seama de aceste elemente, care ar trebui analizate și dezvoltate în evaluarea de impact aflată în curs de realizare în cadrul proiectului UE PNR. Ar trebui stabilită o agendă pentru a permite considerarea atentă a rezultatelor acestei evaluări de impact în redactarea cerințelor globale pentru sistemele PNR.

## 3. Conținutul standardelor propuse

22. Fără a aduce atingere observațiilor fundamentale precedente referitoare la legitimitatea sistemelor PNR, AEPD salută existența unei liste lungi de standarde, inspirate în mod vizibil de principiile UE de protecție a datelor, care ar trebui să întărească în mai multe privințe protecția preconizată în anumite acorduri specifice. În cele ce urmează sunt discutate valoarea adăugată și deficiențele identificate în aceste standarde.

### *Gradul de adecvare și caracterul obligatoriu al oricărui acord*

23. Din felul în care este formulată comunicarea, AEPD înțelege că evaluarea adecvării se poate baza pe cadrul general al protecției datelor din țara destinatară sau poate fi contextuală, depinzând de angajamentele obligatorii din punct de vedere juridic dintr-un acord internațional care reglementează prelucrarea datelor cu caracter personal. Având în vedere rolul decisiv al acordurilor internaționale în legătură cu evaluarea adecvării, AEPD subliniază necesitatea stabilirii clare a caracterului obligatoriu al acordurilor pentru toate părțile vizate și consideră că acest aspect ar trebui completat printr-o mențiune explicită conform căreia acordurile să asigure drepturi aplicabile în mod direct persoanelor vizate. AEPD consideră că aceste elemente constituie un aspect esențial al evaluării gradului de adecvare.

### *Domeniul de aplicare și scopul*

24. Primele două puncte din lista de principii se referă la limitarea scopului. Sub subtitlul „utilizarea datelor”, primul

<sup>(1)</sup> Avizul AEPD din 20 decembrie 2007 referitor la propunerea de decizie-cadru a Consiliului privind utilizarea datelor din registrul cu numele pasagerilor (PNR) în scopul aplicării legii, JO C 110, 1.5.2008, p. 1. Avizele Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal sunt disponibile la: [http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index\\_en.htm#data\\_transfers](http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm#data_transfers)

<sup>(2)</sup> Pagina 4 din comunicare, capitolul 2.1.

<sup>(3)</sup> Avizul din 20 decembrie 2007 referitor la propunerea de decizie-cadru a Consiliului privind utilizarea datelor din registrul cu numele pasagerilor (PNR) în scopul aplicării legii, JO C 110, 1.5.2008, p. 4.

punct menționează aplicarea legii și asigurarea securității, iar apoi se referă la terorism și la alte infracțiuni transnaționale grave, pe baza „abordării” definițiilor prevăzute în diverse instrumente UE. AEPD pune la îndoială această formulare, care ar putea conduce la interpretarea conform căreia acordurile viitoare nu s-ar baza exact pe aceste definiții, ci ar fi inspirate de ele. Este esențial din punct de vedere al securității juridice ca terorismul și celelalte infracțiuni transnaționale grave să fie definite precis și ca instrumentele UE menționate în comunicare să fie identificate. În plus, AEPD amintește că, înainte ca diferitele tipuri de infracțiuni să fie incluse în sistemul PNR, acestea trebuie să fie supuse unui test de necesitate și proporționalitate, ca o condiție prealabilă.

25. Cel de al doilea punct pare să se refere mai mult la domeniul de aplicare (natura datelor culese) decât la principiul scopului. AEPD remarcă faptul că în comunicare nu este inclusă o listă a datelor care ar putea face obiectul transferurilor, deoarece aceasta lasă la latitudinea fiecărui acord specific în parte stabilirea categoriilor de date care vor fi transferate. Pentru a evita divergențele și includerea unor categorii disproporționate de date în unele acorduri cu țări terțe, AEPD consideră că la aceste standarde ar trebui adăugată o listă comună și exhaustivă a categoriilor de date, în conformitate cu scopul schimbului de date. AEPD se referă în această privință la avizele Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, care prevăd categoriile de date care ar fi admisibile și pe cele considerate excesive în raport cu drepturile fundamentale ale persoanelor vizate <sup>(1)</sup>. Categoriile de date ce trebuie excluse sunt în special cele care pot fi interpretate drept date sensibile – și care sunt protejate de articolul 8 din Directiva 95/46/CE, date SSR/SSI (Special Service Request/Information), date OSI (Other Service-Related Information), câmpuri deschise sau care permit introducerea unui text liber (precum „Observații generale”, unde pot apărea date cu caracter sensibil) și informații privind călătorii frecvenți și „datele comportamentale”.

#### *Datele sensibile*

26. Comunicarea arată că datele sensibile nu vor fi folosite decât în împrejurări excepționale. AEPD regretă această exceptare. AEPD consideră condițiile de exceptare prea vaste și crede că acestea nu furnizează nicio garanție: utilizarea datelor de la caz la caz este prezentată doar ca exemplu; în plus, limitarea scopului ar trebui să constituie un principiu general aplicabil oricărei prelucrări de date PNR, nu doar o garanție care se aplică datelor sensibile. AEPD consideră că a permite prelucrarea datelor sensibile, chiar și în cazuri limitate, ar duce la alinierea nivelului de protecție al tuturor sistemelor PNR la sistemul mai puțin conform de protecție a datelor, mai degrabă decât la

sistemul cu un grad de conformitate mai mare. Prin urmare, AEPD solicită o excludere completă a prelucrării datelor sensibile, ca principiu.

#### *Securitatea datelor*

27. Obligația generală privind securitatea, prevăzută în comunicare, este considerată satisfăcătoare. Cu toate acestea, AEPD consideră că aceasta ar fi putut fi completată cu o obligație de informare reciprocă în cazul unei încălcări a securității: beneficiarii ar avea responsabilitatea de a-și informa omologii în cazul în care datele pe care le-au primit au făcut obiectul unei dezvăluiri ilegale. Aceasta va contribui la o responsabilizare sporită în prelucrarea datelor în condiții de siguranță.

#### *Punerea în aplicare*

28. AEPD susține sistemul de supraveghere prevăzut în comunicare, inclusiv măsurile de control și răspundere. Dreptul fiecărei persoane de a avea acces la căi de atac administrative și judiciare este, de asemenea, susținut cu tărie. În ceea ce privește drepturile de acces, AEPD înțelege că nu poate fi preconizată nicio limitare, ceea ce este un lucru binevenit. În cazul în care, în situații excepționale, ar fi necesară o limitare, domeniul precis de aplicare al acestora și garanțiile necesare, incluzând în special un drept indirect de acces, ar trebui menționate clar în cadrul standardelor.

#### *Transferurile ulterioare*

29. AEPD este mulțumită de restricționarea transferurilor ulterioare de la caz la caz, fie că este vorba de transferuri către autorități guvernamentale, fie către țări terțe. AEPD consideră că, în plus față de acest principiu, limitarea scopului aplicabilă transferurilor către țări terțe ar trebui să se aplice și transferurilor din cadrul țării terțe către alte autorități guvernamentale. Acest lucru ar preveni orice utilizare ulterioară sau verificarea încrucișată a datelor PNR cu informații prelucrate în alte scopuri. AEPD este preocupată în special de riscul verificării încrucișate a informațiilor provenite din alte baze de date, precum ESTA, în ceea ce privește Statele Unite. AEPD remarcă faptul că decizia recentă a SUA de a percepe o taxă pentru ESTA are ca rezultat colectarea de informații privind cărțile de credit ale călătorilor. AEPD dorește o limitare clară pentru a preveni compararea necorespunzătoare a informațiilor care ar depăși domeniul de aplicare al acordului PNR.

#### *Păstrarea datelor*

30. Perioada de păstrare a datelor nu face obiectul unei armonizări eficiente. AEPD consideră că, de principiu, datele PNR ar trebui șterse atunci când controalele efectuate cu ocazia transmiterii datelor nu au condus la o măsură executorie. Dacă în contextul național este justificată necesitatea unei perioade limitate de păstrare, AEPD consideră că în cadrul standardelor ar trebui stabilită o perioadă maximă de păstrare. În plus, ar trebui întărit principiu

<sup>(1)</sup> Avizul din 23 iunie 2003 privind nivelul de protecție asigurat de Statele Unite pentru transferul datelor pasagerilor, GL78. Acest aviz și avizele subsecvente ale Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, referitoare la această chestiune, sunt disponibile la: [http://ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/wpdocs/index\\_en.htm#data\\_transfers](http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/index_en.htm#data_transfers)



limitării în timp a drepturilor de acces ale funcționarilor, iar anonimizarea treptată a datelor ar trebui considerată o obligație, nu un exemplu.

#### Modalități de transmitere

31. AEPD susține utilizarea exclusivă a sistemului „push” pentru transmiterea datelor PNR. AEPD solicită garanții concrete care să asigure că sistemul „push” este în mod efectiv singurul sistem folosit în practică. Experiența și inspecțiile efectuate de către autoritățile de protecție a datelor au arătat, într-adevăr, că în ciuda obligațiilor prevăzute de acordurile aflate deja în vigoare, în special cu privire la „PNR SUA”, mai acționează și un sistem rezidual „pull”, iar în paralel cu „push”, autoritățile SUA au un acces mai larg la datele PNR prin sisteme computerizate de rezervare. Ar trebui adoptate măsuri juridice și tehnice de prevenire a oricărei eludări a sistemului „push”.
32. Ar trebui definită frecvența transmițerilor de date de către companiile aeriene („rezonabilă”) și ar trebui stabilit un număr maxim de transmițeri. Pentru un astfel de exercițiu ar trebui luate ca reper sistemele existente care conțin prevederile cele mai sigure de respectare a vieții private.

#### Concepte-cheie

33. AEPD solicită de asemenea mai multă precizie cu privire la elementele esențiale ale punerii în aplicare a acordurilor PNR. Duratele acordurilor („fixă”, „adekvată”) și revizuirea acestora („periodică”) ar trebui definite mai bine într-o perspectivă orizontală. Ar putea fi precizată în special periodicitatea revizuirilor comune, ca și obligația de a se efectua o primă revizuire în cadrul unui anumit interval de la intrarea în vigoare a acordurilor: s-ar putea menționa un termen maxim de trei ani.

### III. CONCLUZIE

34. AEPD salută abordarea orizontală prezentată de Comisie în comunicarea sa. Aceasta reprezintă un pas esențial în direcția realizării unui cadru cuprinzător pentru schimbul de date PNR. Această apreciere cu caracter general este însă într-o oarecare măsură atenuată de unele îngrijorări majore.
35. Sistemele PNR prezentate în comunicare nu îndeplinesc în sine cerințele testelor de necesitate și proporționalitate

descrise în prezentul aviz și în avizele anterioare ale AEPD și ale Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal. Pentru a fi admisibile, condițiile pentru colectarea și prelucrarea datelor cu caracter personal ar trebui să fie restricționate considerabil. AEPD este preocupată în special în legătură cu utilizarea sistemelor PNR pentru evaluarea riscului sau elaborarea de profile.

36. Elaborarea de standarde PNR ar trebui să țină seama de cadrul general de protecție a datelor și de evoluțiile juridice conexe din cadrul UE, precum și de negocierea unor acorduri de schimb de date la un nivel mai general, în special cu Statele Unite. Ar trebui să se asigure respectarea de către un acord PNR viitor cu Statele Unite a acordului general cu SUA privind protecția datelor. Acordurile privind PNR cu țările terțe ar trebui să fie, de asemenea, consecvente cu această abordare.
37. Este esențial ca orice acord cu țări terțe să țină seama de noile cerințe în materie de protecție a datelor care sunt în prezent în curs de elaborare în cadrul instituțional post-Lisabona.
38. De asemenea, AEPD solicită o mai mare precizie în abordarea globală în ceea ce privește garanțiile minime aplicabile tuturor acordurilor: ar trebui să se aplice condiții mai stricte, în special cu privire la prelucrarea datelor sensibile, principiul limitării scopului, condițiile pentru transferurile ulterioare și păstrarea datelor.
39. În final, AEPD insistă asupra faptului că orice acord ar trebui să prevadă drepturi aplicabile în mod direct pentru persoanele vizate. Eficacitatea procedurilor de executare de către persoanele vizate, precum și de către autoritățile de supraveghere, este o condiție esențială pentru evaluarea gradului de adecvare al oricărui acord.

Adoptat la Bruxelles, 19 octombrie 2010.

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor