

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 poziția Uniunii în cadrul Comitetului mixt de cooperare vamală UE-SUA cu privire la recunoașterea reciprocă a Programului Uniunii Europene referitor la operatorii economici autorizați și a Programului Statelor Unite privind parteneriatul vămi-comerț împotriva terorismului

(2012/C 160/01)

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:

I. INTRODUCERE

I.1. Consultarea AEPD și scopul avizului

1. La 5 ianuarie 2011, Comisia a adoptat o propunere de Decizie a Consiliului privind poziția Uniunii în cadrul Comitetului mixt de cooperare vamală UE-SUA cu privire la recunoașterea reciprocă a Programului Uniunii Europene referitor la operatorii economici autorizați și a Programului Statelor Unite privind parteneriatul vămi-comerț împotriva terorismului ⁽³⁾ (denumită în continuare „propunerea”). Propunerea a fost transmisă AEPD în aceeași zi.
2. AEPD a fost consultată informal anterior și a transmis Comisiei un număr de observații, de asemenea informale. Scopul prezentului aviz este completarea acestor observații având în vedere actuala propunere și prezentarea publică a punctului său de vedere.
3. AEPD recunoaște că prelucrarea datelor cu caracter personal nu reprezintă cel mai important aspect al propunerii. Majoritatea informațiilor prelucrate nu vor conține date cu caracter personal, astfel cum sunt definite în legislația privind protecția datelor ⁽⁴⁾. Cu toate acestea, legea privind protecția datelor trebuie să fie respectată și în aceste situații, astfel cum se va explica mai jos.

⁽¹⁾ JO L 281, 23.11.1995, p. 31.

⁽²⁾ JO L 8, 12.1.2001, p. 1.

⁽³⁾ COM(2011) 937 final.

⁽⁴⁾ Astfel cum se menționează la punctele 8 și 9 din prezentul aviz.

I.2. Contextul propunerii

4. Scopul propunerii este de a crea o recunoaștere reciprocă a programelor de parteneriat comercial dintre UE și SUA – Programul Uniunii Europene referitor la operatorii economici autorizați (AEO) și Programul SUA privind parteneriatul vămi-comerț împotriva terorismului (C-TPAT) – în vederea facilitării relațiilor comerciale între operatorii care au investit în securitatea lanțului de aprovizionare și participă la unul dintre aceste programe.
5. Relațiile între UE și Statele Unite în domeniul vamal se bazează pe Acordul privind cooperarea vamală și asistența reciprocă în domeniul vamal (*Agreement on Customs Cooperation and Mutual Assistance in Customs Matters* – CMAA) ⁽¹⁾. Acest acord instituie Comitetul mixt de cooperare vamală (JCCC), format din reprezentanți ai autorităților vamale din UE și din Statele Unite. Recunoașterea reciprocă urmează să fie stabilită prin decizie a acestui comitet. Prin urmare, propunerea constă în:
 - memoriu explicativ;
 - propunerea de decizie a Consiliului, în care se afirmă că UE va adopta în cadrul JCCC pozițiile prevăzute în proiectul de decizie privind recunoașterea reciprocă;
 - proiectul de decizie al JCCC privind recunoașterea reciprocă a AEO din UE și C-TPAT din Statele Unite (denumit în continuare „proiectul de decizie”) ⁽²⁾.
6. Proiectul de decizie urmează să fie pus aplicare de către autoritățile vamale, care au instituit un proces de validări comune (procedura de cerere pentru acordarea statutului de membru operatorilor, evaluarea cererilor, acordarea statutului de membru și supravegherea acestui statut).
7. Astfel, buna funcționare a recunoașterii reciproce se întemeiază pe schimbul de informații între autoritățile vamale din UE și din Statele Unite privind operatorii comerciali care participă deja la un program de parteneriat.

II. ANALIZA PROIECTULUI DE DECIZIE

II.1. Prelucrarea datelor privind persoanele fizice

8. Deși scopul proiectului de decizie nu este prelucrarea datelor cu caracter personal, unele dintre informațiile care vor face obiectul schimburilor vor viza persoane fizice, în special dacă operatorul este o persoană fizică ⁽³⁾ sau denumirea oficială a persoanei juridice având calitate de operator identifică o persoană fizică ⁽⁴⁾.
9. Importanța protecției datelor într-un astfel de context a fost subliniată de către Curtea Europeană de Justiție prin Hotărârea *Schecke*. Conform Curții, persoanele juridice pot invoca protecția drepturilor la viață privată și protecția datelor cu caracter personal, astfel cum sunt recunoscute în Carta drepturilor fundamentale a UE, dacă denumirea oficială a persoanei juridice identifică una sau mai multe persoane fizice ⁽⁵⁾. Astfel, prezentul aviz va analiza modul în care schimbul de date cu caracter personal privind operatorii este reglementat în proiectul de decizie.

⁽¹⁾ Acordul dintre Comunitatea Europeană și Statele Unite ale Americii privind cooperarea vamală și asistența reciprocă în materie vamală (JO L 222, 12.8.1997, p. 17), disponibil la <http://ec.europa.eu/world/agreements/prepareCreateTreatiesWorkspace/treatiesGeneralData.do?step=0&redirect=true&treatyId=308> (rezumat și text complet).

⁽²⁾ Propunere de Decizie a Comitetului mixt de cooperare vamală SUA-UE cu privire la recunoașterea reciprocă a Programului Statelor Unite privind parteneriatul vămi-comerț împotriva terorismului și a Programului Uniunii Europene referitor la operatorii economici autorizați.

⁽³⁾ Datele sunt definite în articolul 2 litera (a) din Directiva 95/46/CE și articolul 2 litera (a) din Regulamentul (CE) nr. 45/2001, ca „reprezentând orice informație referitoare la o persoană fizică identificată sau identificabilă”.

⁽⁴⁾ A se vedea, de asemenea, Avizul AEPD privind propunerea de decizie a Consiliului privind poziția Uniunii în cadrul Comitetului mixt de cooperare vamală UE-Japonia cu privire la recunoașterea reciprocă a programelor referitoare la operatorii economici autorizați din Uniunea Europeană și Japonia, disponibil la: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:190:0002:0006:EN:PDF>

⁽⁵⁾ Curtea Europeană de Justiție, 9 noiembrie 2010, *Volker und Markus Schecke*, C-92/09 și C-93/09, punctul 53 (disponibil la <http://curia.europa.eu/juris/cgi-bin/gettext.pl?where=&lang=en&num=79898890C19090092&doc=T&ouvert=T&seance=ARRET>).

II.2. Aplicabilitatea cadrului UE privind protecția datelor

10. Datele vor fi prelucrate de către autoritățile vamale prevăzute la articolul 1 litera (b) din CMAA ⁽¹⁾. Această definiție se referă, în UE, la „serviciile competente” ale Comisiei Europene și la autoritățile vamale ale statelor membre UE. Conform legislației UE privind protecția datelor, prelucrarea datelor de către statele membre UE este reglementată de Directiva 95/46/CE (denumită în continuare „Directiva privind protecția datelor”) și de legislațiile naționale privind protecția datelor care transpun această directivă, în timp ce prelucrarea datelor cu caracter personal de către instituțiile și organismele UE este reglementată prin Regulamentul (CE) nr. 45/2001 (denumit în continuare „regulamentul”). Astfel, în cazul de față se aplică atât Directiva privind protecția datelor, cât și regulamentul.

II.3. Nivelul de protecție

11. Schimburile de informații se efectuează în format electronic și în conformitate cu CMAA. Conform articolului 17 alineatul (2) din CMAA, datele cu caracter personal pot fi transferate între părțile semnatare doar dacă partea care le primește garantează un nivel de protecție cel puțin echivalent cu cel aplicabil cazului respectiv în țara care transmite datele.
12. AEPD salută această prevedere, care ar trebui să fie înțeleasă ca încercând să asigure conformitatea cu legislația UE privind protecția datelor. Articolul 25 din Directiva privind protecția datelor și articolul 9 din regulamentul stabilesc regula principală potrivit căreia datele pot fi transferate între UE și țări terțe numai dacă țara destinatară asigură un nivel de protecție „adecvat” ⁽²⁾. Astfel, articolul 17 alineatul (2) din CMAA pare mai strict decât dispozițiile Directivei privind protecția datelor.
13. Prin urmare, ar trebui să se analizeze, pe baza tuturor datelor relevante, dacă autoritățile destinate din Statele Unite garantează un nivel echivalent de protecție (sau cel puțin un nivel „adecvat”). Analiza adecvării trebuie să aibă în vedere toate circumstanțele unui transfer sau ale unei categorii de transferuri ⁽³⁾.
14. Comisia Europeană nu a constatat că, în ansamblu, Statele Unite asigură un nivel adecvat de protecție. În lipsa unei decizii generale privind caracterul adecvat, operatorii ⁽⁴⁾ pot decide, sub supravegherea autorităților în materie de protecție a datelor ⁽⁵⁾, dacă nivelul de protecție asigurat în acel caz specific este adecvat. Statele membre ale UE (sau AEPD, în cazul în care transferurile sunt efectuate de instituții sau organisme ale UE) pot, de asemenea, să autorizeze un anumit transfer sau set de transferuri de date cu caracter personal către o țară terță atunci când operatorul oferă garanții adecvate ⁽⁶⁾.
15. Aceste decizii ad-hoc privind caracterul adecvat pot fi aplicate în acest caz dacă autoritățile vamale naționale și serviciile Comisiei Europene responsabile pentru probleme vamale prezintă suficiente dovezi în sprijinul afirmațiilor privind adoptarea unor garanții adecvate de către autoritățile vamale din Statele Unite în ceea ce privește transferurile prevăzute în proiectul de decizie ⁽⁷⁾.
16. Cu toate acestea, AEPD nu dispune de dovezi suficiente că autoritățile vamale din Statele Unite asigură un nivel de protecție a datelor „adecvat” sau „cel puțin echivalent cu cel aplicabil cazului respectiv în țara care transmite datele”, astfel cum se prevede la articolul 17 alineatul (2) din CMAA.

⁽¹⁾ A se vedea secțiunea I alineatul (2) din proiectul de decizie.

⁽²⁾ Regulamentul adaugă că aceste transferuri pot avea loc numai atunci când datele sunt transferate „exclusiv pentru a permite îndeplinirea sarcinilor care sunt de competența operatorului”.

⁽³⁾ A se vedea articolul 9 alineatele (1) și (2) din regulamentul, articolul 25 alineatele (1) și (2) din Directiva privind protecția datelor, precum și legislațiile naționale pentru protecția datelor de transpunere a acestora. A se vedea, de asemenea, Avizul privind cooperarea vamală comună între UE și Japonia menționat mai sus.

⁽⁴⁾ În aceste cazuri, autoritățile vamale din UE și statele sale membre.

⁽⁵⁾ În unele state membre, transferurile pot fi autorizate numai de către autoritățile pentru protecția datelor.

⁽⁶⁾ Articolul 26 alineatul (2) din Directiva privind protecția datelor și articolul 9 alineatul (7) din regulamentul.

⁽⁷⁾ A se vedea, de asemenea, scrisoarea AEPD privind „Transferurile de date cu caracter personal către țările terțe: «caracterul adecvat» al țărilor semnatare ale Convenției 108 a Consiliului Europei (cazul 2009-0333)”, disponibilă la adresa: http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Adminmeasures/2009/09-07-02_OLAF_transfer_third_countries_EN.pdf

17. Prin urmare, AEPD recomandă să se asigure că dovezile care demonstrează că autoritățile vamale din SUA garantează un nivel de protecție a datelor „adecvat” sau „cel puțin echivalent cu cel aplicabil cazului în speță în țara care transmite datele”, astfel cum se prevede la articolul 17 alineatul (2) din CMAA, vor fi puse la dispoziția AEPD și autorităților naționale. Această obligație ar trebui să fie introdusă de o dispoziție din proiectul de decizie.
18. În sfârșit, transferurile de date cu caracter personal din UE către țări care nu garantează un nivel „adecvat” de protecție pot fi permise, de asemenea, dacă se aplică una dintre excepțiile de la articolul 26 alineatul (1) din Directiva privind protecția datelor sau articolul 9 alineatul (6). În cazul de față, se poate argumenta că transferul este „necesar sau impus prin lege din motive legate de un interes public important” ⁽¹⁾. Totuși, aceste excepții ar trebui să fie interpretate restrictiv și nu pot forma baza unor transferuri masive sau sistematice de date cu caracter personal ⁽²⁾. AEPD consideră că aceste excepții ar putea să nu fie utile în cazul de față.

II.4. Limitarea la scopul în cauză

19. Secțiunea V alineatul (1) din proiectul de decizie prevede că datele transferate pot fi prelucrate numai de către autoritățile vamale destinate, în scopul aplicării proiectului de decizie, în conformitate cu articolul 17 din CMAA.
20. Totuși, prelucrarea în alte scopuri este permisă de secțiunea V alineatul (3) a patra liniuță și articolul 17 alineatul (3) din CMAA. Deoarece sfera proiectului de decizie depășește cooperarea în domeniul vamal și include lupta împotriva terorismului, AEPD recomandă ca în textul deciziei să se specifice toate scopurile posibile ale transferurilor de date cu caracter personal. În plus, toate datele transferate ar trebui să fie necesare și proporționale pentru îndeplinirea acestor scopuri. Ar trebui, de asemenea, să se specifice că persoanele vizate ar trebui informate în mod detaliat în privința tuturor scopurilor și condițiilor prelucrării datelor lor cu caracter personal.

II.5. Categoriile de date care urmează să facă obiectul schimburilor

21. Datele privind membrii programelor de parteneriat comercial care pot fi comunicate între autoritățile vamale sunt următoarele: numele; adresa; statutul de membru; data validării sau a autorizării; suspendările și revocările; numărul unic al autorizației sau numărul de identificare; și „detalii care pot fi stabilite de comun acord de către autoritățile vamale, sub rezerva, atunci când este cazul, a oricărui garanții necesare” ⁽³⁾. Deoarece ultima prevedere este formulată prea general, AEPD recomandă menționarea în mod specific a categoriilor de date care pot fi incluse.
22. AEPD observă, de asemenea, că informațiile transmise pot include date privind infracțiuni sau suspiciuni de comitere a unor infracțiuni, cum ar fi date referitoare la suspendarea și revocarea statutului de membru. AEPD subliniază că legislația UE privind protecția datelor restricționează prelucrarea datelor cu caracter personal referitoare la infracțiuni, condamnări penale sau măsuri de securitate ⁽⁴⁾. Prelucrarea acestor categorii de date poate fi supusă unor verificări prealabile ale AEPD și autorităților naționale de protecție a datelor din UE ⁽⁵⁾.

II.6. Transferuri ulterioare

23. Secțiunea V alineatul (3) a treia liniuță permite transferul de date către țări terțe sau organisme internaționale, cu acordul prealabil al autorității care furnizează informațiile și în conformitate cu condițiile specificate de aceasta. Transferurile ulterioare nu ar trebui să fie permise fără prezentarea unei justificări.

⁽¹⁾ A se vedea articolul 9 alineatul (6) litera (d) din regulament sau articolul 26 alineatul (1) litera (d) din Directiva privind protecția datelor, care, conform considerentului 58 din Directiva privind protecția datelor, include transferurile între autoritățile fiscale sau vamale.

⁽²⁾ Documentul de lucru al Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal din 25 noiembrie 2005 privind o interpretare comună a articolului 26 alineatul (1) din Directiva 95/46/CE din 24 octombrie 1995 (WP114), paginile 7-9, disponibil la: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_en.pdf

⁽³⁾ A se vedea secțiunea IV alineatul (3) literele (a)-(g) din proiectul de decizie.

⁽⁴⁾ A se vedea articolul 8 alineatul (5) din Directiva 95/46/CE și articolul 10 alineatul (5) din Regulamentul (CE) nr. 45/2001.

⁽⁵⁾ A se vedea articolul 27 alineatul (a) din Regulamentul (CE) nr. 45/2001 și legislațiile naționale privind protecția datelor care pun în aplicare articolul 20 din Directiva 95/46/CE.

24. Astfel, se pare că secțiunea V alineatul (3) ar trebui să includă o dispoziție similară celei de la articolul 17 alineatul (2) din CMAA, care să prevadă că datele cu caracter personal pot fi transmise către o țară terță numai atunci când țara destinatară garantează un nivel de protecție cel puțin echivalent cu cel impus de proiectul de decizie. În caz contrar, protecția datelor cu caracter personal asigurată în temeiul acestui proiect poate fi eludată de transferurile ulterioare.
25. În orice caz, această dispoziție ar trebui să specifice scopurile unor astfel de transferuri și situațiile specifice în care acestea sunt permise. În plus, ar trebui să menționeze explicit că necesitatea și proporționalitatea transferurilor internaționale ulterioare vor fi evaluate de la caz la caz și că nu sunt permise transferuri masive sau sistematice. Obligația de a informa persoanele vizate în privința posibilității unui transfer internațional ulterior ar trebui, de asemenea, să fie inclusă în text.

II.7. Păstrarea datelor

26. AEPD salută secțiunea V alineatul (2), care interzice prelucrarea sau păstrarea informațiilor pentru o perioadă mai lungă decât este necesar în scopul transferului. Totuși, se recomandă stabilirea unei perioade maxime de păstrare.

II.8. Securitate și stabilirea responsabilității

27. Secțiunea IV prevede că schimburile de informații vor avea loc în format electronic. Conform AEPD, în această secțiune ar trebui indicate detalii suplimentare privind sistemul de schimb de informații care urmează a fi instituit. În orice caz, sistemul selectat ar trebui să integreze sistemele de protecție a vieții private și a datelor încă din faza de proiectare (principiul confidențialității prin proiectare).
28. În această privință, AEPD salută garanțiile de securitate prevăzute în secțiunea V alineatul (3) prima și a doua liniuță, care includ mijloace de control al accesului, „protecție împotriva accesului neautorizat, diseminării și modificării, ștergerii sau distrugerii” și de verificare a utilizării datelor exclusiv în scopul proiectului de decizie. De asemenea, AEPD salută jurnalele de acces prevăzute la secțiunea V alineatul (3) a cincea liniuță.
29. AEPD recomandă, de asemenea, includerea în aceste dispoziții a obligației de a efectua o evaluare a impactului asupra protecției datelor (inclusiv o evaluare a riscurilor) înaintea începerii transferului de date. Evaluarea ar trebui să includă o evaluare a riscurilor, dar și măsurile preconizate pentru combaterea acestor riscuri⁽¹⁾. Textul ar trebui, de asemenea, să specifice că îndeplinirea și aplicarea acestor măsuri trebuie să fie auditate și raportate periodic. Acest lucru este cu atât mai important având în vedere eventualitatea prelucrării de date sensibile.

II.9. Calitatea datelor și drepturile persoanelor vizate

30. AEPD salută prevederea prin care autoritățile vamale sunt obligate să se asigure că informațiile transferate sunt exacte și actualizate în mod regulat [a se vedea secțiunea V alineatele (2) și (5)]. AEPD salută, de asemenea, secțiunea V alineatul (4) care garantează dreptul de acces și rectificarea datelor cu caracter personal pentru operatorii care sunt membri ai programelor de parteneriat.
31. Cu toate acestea, AEPD observă că exercitarea acestor drepturi este reglementată de legislația vamală națională. În ceea ce privește datele furnizate de UE autorităților vamale, dar și pentru a garanta un nivel „adecvat” de protecție (a se vedea secțiunea II.3 din prezentul aviz), aceste drepturi ar trebui să fie limitate numai atunci când o astfel de restricție este necesară pentru protejarea unor interese economice sau financiare importante.
32. În plus, AEPD salută faptul că autoritățile vamale sunt obligate să șteargă datele primite în cazul în care acestea au fost colectate sau prelucrate cu încălcarea proiectului de decizie sau a CMAA⁽²⁾. AEPD reamintește că, în conformitate cu articolul 17 alineatul (2) din CMAA, această dispoziție se aplică oricărei prelucrări care contravine legislației UE privind protecția datelor.

⁽¹⁾ Astfel cum se prevede deja în articolul 33 din noua propunere pentru un regulament privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date (Regulamentul general privind protecția datelor) [COM(2012) 11/4, proiect].

⁽²⁾ A se vedea secțiunea V alineatul (5) din proiectul de decizie.

33. AEPD este de acord cu obligația impusă autorităților vamale de a-i informa pe membrii programului în privința opțiunilor lor de a apela la căi de atac ⁽¹⁾. Cu toate acestea, trebuie să se clarifice care sunt căile de atac în cazul unei încălcări a garanțiilor de protecție a datelor prevăzute de proiectul de decizie. Această dispoziție ar trebui, de asemenea, să specifice o obligație de a informa și celelalte persoane vizate (operatorii care solicită statutul de membru) în privința opțiunilor pe care le au cu privire la căile de atac.

II.10. Supraveghere

34. AEPD salută secțiunea V alineatul (6) care supune întreaga secțiune V „supravegherii și verificării independente” de către Înaltul Responsabil pentru Protecția Vieții Private din cadrul Departamentului pentru Securitate Internă al Statelor Unite, AEPD și autoritățile naționale de protecție a datelor.
35. Ar trebui să se specifice, de asemenea, că AEPD și autoritățile naționale de protecție a datelor ar trebui să supravegheze menținerea unui nivel „adecvat” al protecției acordate datelor cu caracter personal de către autoritatea vamală de destinație (a se vedea secțiunea III punctul 1). Secțiunea IV ar trebui, de asemenea, să facă obiectul supravegherii și revizuirii.

III. CONCLUZIE

36. AEPD salută garanțiile prevăzute în proiectul de decizie, în special în ceea ce privește securitatea datelor. Totuși, AEPD și autoritățile naționale de protecție a datelor ar trebui să dispună de date care să demonstreze că autoritățile vamale din Statele Unite asigură un nivel de protecție a datelor „adecvat” sau „cel puțin echivalent cu cel aplicabil cazului respectiv în țara care transmite datele”, astfel cum se prevede la articolul 17 alineatul (2) din CMAA. Această obligație ar trebui să fie introdusă de o dispoziție în proiectul de decizie.

37. În plus, AEPD recomandă următoarele:

- menționarea scopului (scopurilor) schimburilor de date prevăzute în proiectul de decizie care trebuie să fie necesare și proporționale;
- menționarea categoriilor de date incluse la secțiunea IV alineatul (3) litera (g);
- menționarea faptului că, în cazul în care necesitatea transferurilor internaționale ulterioare este justificată, acestea ar trebui permise numai de la caz la caz, în scopuri compatibile și dacă țara de destinație garantează un nivel de protecție cel puțin echivalent cu cel acordat de proiectul de decizie;
- includerea unei obligații de informare a tuturor persoanelor vizate în privința celor de mai sus;
- completarea dispozițiilor privind securitatea;
- menționarea perioadelor maxime de păstrare;
- absența limitării drepturilor persoanelor vizate din UE dacă o astfel de restricție nu este necesară pentru protejarea unor interese economice sau financiare importante;
- garantarea dreptului de exercitare a căilor de atac;
- supunerea secțiunii IV supravegherii și revizuirii;
- menționarea faptului că AEPD, autoritățile naționale de protecție a datelor din UE și Înaltul Responsabil pentru Protecția Vieții Private din cadrul Departamentului pentru Securitate Internă al Statelor Unite ar trebui să supravegheze caracterul efectiv și conformitatea cu cerințele UE a garanțiilor instituite de autoritatea vamală de destinație pentru asigurarea unei protecții adecvate a datelor cu caracter personal.

⁽¹⁾ A se vedea secțiunea V alineatul (4), ultima teză.

38. AEPD observă, de asemenea, că propunerea poate implica prelucrarea de date cu caracter personal referitoare la infracțiuni sau suspiciuni de comitere a unor infracțiuni. Conform legislației UE, aceste date fac obiectul unor garanții mai stricte și pot fi supuse unei verificări prealabile din partea AEDP și a autorităților naționale de protecție a datelor din UE.

Adoptat la Bruxelles, 9 februarie 2012.

Giovanni BUTTARELLI
*Adjunctul Autorității Europene pentru Protecția
Datelor*
