ISSN 1830-3668

Jurnalul Oficial al Uniunii Europene

C 229

Ediția în limba română

Comunicări și informări

Anul 52

23 septembrie 2009

Numărul informării | Cuprins | Pagina

RO

(continuare în pagina următoare)

RO

I

(Rezoluții, recomandări și avize)

AVIZE

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR

Avizul Autorității Europene pentru Protecția Datelor privind propunerea de regulament al Parlamentului European și al Consiliului de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de azil prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe sau un apatrid [COM(2008) 820 final]

(2009/C 229/01)

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR,

având în vedere Tratatul de instituire a Comunității Europene, în special articolul 286,

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 [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 [2], în special articolul 41,

având în vedere solicitarea unui aviz în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001, primită din partea Comisiei la 3 decembrie 2008,

ADOPTĂ PREZENTUL AVIZ:

I. **INTRODUCERE**

Consultarea AEPD

1. Propunerea de regulament al Parlamentului European și al Consiliului de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de azil prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe sau un apatrid (denumită în continuare „propunerea" sau „propunerea Comisiei") a fost transmisă de către Comisie AEPD spre consultare la 3 decembrie 2008, în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001. Această consultare ar trebui menționată în mod explicit în preambulul regulamentului.

2. AEPD a contribuit la propunere într-o etapă inițială și multe dintre punctele pe care le-a ridicat în mod informal pe parcursul procesului de pregătire au fost luate în considerare de către Comisie în textul final al propunerii.

Propunerea în contextul acesteia

3. Propunerea este o reformare a Regulamentului (CE) nr. 343/2003 al Consiliului din 18 februarie 2003 de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de azil prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe [3] (denumit în continuare „Regulamentul Dublin"). Aceasta a fost prezentată de Comisie ca făcând parte din primul pachet de propuneri care vizează asigurarea unui grad sporit de armonizare în acest domeniu și a unor standarde de protecție mai ridicate pentru sistemul european comun de azil, astfel cum s-a solicitat prin Programul de la Haga din 4-5 noiembrie 2004 și după cum s-a enunțat în Planul strategic în materie de azil al Comisiei din 17 iunie 2008. Programul de la Haga a invitat Comisia să încheie evaluarea instrumentelor juridice ale primei faze și să înainteze Consiliului și Parlamentului European instrumentele și măsurile celei de a doua faze, în vederea adoptării acestora până în 2010.

[1] JO L 281, 23.11.1995, p. 31.
[2] JO L 8, 12.1.2001, p. 1.
[3] JO L 50, 25.2.2003, p. 1.

4. Propunerea a făcut obiectul unei evaluări intensive și al unui proces de consultare. Aceasta ține seama în special de rezultatele Raportului Comisiei asupra evaluării sistemului Dublin prezentat la 6 iunie 2007 ([1]), care a identificat o serie de deficiențe juridice și practice existente în sistemul actual, precum și contribuții primite de către Comisie din partea a diferite părți interesate ca răspuns la Cartea verde cu privire la viitorul sistem european comun de azil ([2]).

5. Obiectivul principal al propunerii este de a consolida eficiența sistemului Dublin și de a asigura standarde de protecție mai ridicate acordate solicitanților de protecție internațională care fac obiectul procedurii Dublin. În plus, aceasta vizează întărirea solidarității față de statele membre care se confruntă cu situații de presiuni deosebite ale migrației ([3]).

6. Prezenta propunere extinde domeniul de aplicare a Regulamentului Dublin pentru a include solicitanții (și beneficiarii) de protecție subsidiară. Modificarea este necesară pentru a asigura coerența cu acquis-ul comunitar, și anume Directiva 2004/83/CE a Consiliului din 29 aprilie 2004 privind standardele minime referitoare la condițiile pe care trebuie să le îndeplinească resortisanții țărilor terțe sau apatrizii pentru a putea beneficia de statutul de refugiat sau persoanele care, din alte motive, au nevoie de protecție internațională și referitoare la conținutul protecției acordate ([4]) (denumită în continuare „Directiva privind standardele minime"), care a introdus noțiunea de protecție subsidiară. De asemenea, propunerea aliniază definițiile și terminologia utilizate în Regulamentul Dublin la cele prevăzute de alte instrumente juridice în materie de azil.

7. Pentru a consolida eficiența sistemului, propunerea stabilește în special termenul pentru depunerea cererilor de reprimire și reduce termenul de răspuns la cererile de informații. De asemenea, aceasta clarifică clauzele de încetare a responsabilității, precum și împrejurările și procedurile de aplicare a clauzelor discreționare (umanitare și de suveranitate). Aceasta adaugă norme privind transferurile și extinde mecanismul existent de soluționare a litigiilor. De asemenea, propunerea cuprinde o dispoziție privind organizarea unui interviu obligatoriu.

8. În plus și pentru a spori nivelul de protecție acordată solicitanților, propunerea Comisiei prevede dreptul de a introduce o acțiune împotriva unei decizii de transfer, precum și obligația autorității competente de a decide dacă aplicarea acesteia ar trebui sau nu suspendată. Aceasta abordează dreptul la asistență juridică și/sau reprezentare și la asistență lingvistică. De asemenea, propunerea se referă la principiul conform căruia o persoană nu ar trebui supusă detenției numai pentru că solicită protecție internațională. Aceasta extinde, de asemenea, dreptul la reîntregirea familiei și abordează nevoile minorilor neînsoțiți și ale altor grupuri vulnerabile.

Punctele centrale ale avizului

9. Prezentul aviz urmează să abordeze în principal modificările textului care sunt cele mai relevante din punct de vedere al protecției datelor cu caracter personal:

— dispoziții vizând o mai bună punere în aplicare a dreptului la informare, de exemplu conținutul, forma și termenul de furnizare a informațiilor au fost clarificate și a fost propusă adoptarea unei broșuri comune de informare;

— un nou mecanism în domeniul schimbului de informații relevante între statele membre înainte de efectuarea transferurilor;

— utilizarea mijlocului de transmisie sigură DubliNet pentru schimbul de informații.

II. OBSERVAȚII GENERALE

10. AEPD susține obiectivele propunerii Comisiei, în special de a consolida eficiența sistemului Dublin și de a asigura standarde de protecție mai ridicate acordate solicitanților de protecție internațională care fac obiectul procedurii Dublin. De asemenea, aceasta înțelege motivele pentru care Comisia a decis să realizeze revizuirea sistemului Dublin.

11. Asigurarea unui nivel adecvat de protecție a datelor cu caracter personal reprezintă o condiție *sine qua non* pentru a asigura, de asemenea, punerea în aplicare eficientă și un înalt nivel de protecție a altor drepturi fundamentale. AEPD emite prezentul aviz fiind pe deplin conștientă de dimensiunea extinsă a propunerii privind drepturile fundamentale, care se referă nu numai la prelucrarea datelor cu caracter personal, ci și la numeroase alte drepturi ale resortisanților țărilor terțe și/sau ale apatrizilor, cum ar fi în special dreptul de azil, dreptul la informare într-un sens larg, dreptul la reîntregirea familiei, dreptul la o cale de atac eficientă, dreptul la libertate și liberă circulație, drepturile copilului și drepturile minorilor neînsoțiți.

12. Atât considerentul 34 al propunerii, cât și expunerea de motive subliniază eforturile depuse de legiuitor pentru a asigura coerența propunerii cu Carta drepturilor fundamentale. În acest context, expunerea de motive se referă în mod explicit la protecția datelor cu caracter personal și la dreptul de azil. De asemenea, expunerea de motive subliniază faptul că propunerea a făcut obiectul unei examinări aprofundate pentru a avea garanția că dispozițiile sale sunt pe deplin compatibile cu drepturile fundamentale, ca principii generale ale dreptului comunitar și internațional. Totuși, având în vedere sfera de competență a AEPD, prezentul aviz se va axa în principal pe aspectele propunerii privind protecția datelor. În acest context, AEPD salută atenția deosebită care a fost acordată în cadrul propunerii acestui drept fundamental și consideră că acest lucru este esențial pentru a asigura eficiența procedurii Dublin, cu respectarea deplină a cerințelor privind drepturile fundamentale.

([1]) COM(2007) 299.
([2]) COM(2007) 301.
([3]) A se vedea: Expunerea de motive a propunerii.
([4]) JO L 304, 30.9.2004, p. 12.

13. De asemenea, AEPD ia act de faptul că propunerea Comisiei urmărește coerența cu alte instrumente juridice care reglementează instituirea și/sau utilizarea altor sisteme informatice la scară largă. În special, aceasta dorește să sublinieze faptul că atât împărțirea responsabilităților cu privire la baza de date, cât și modul în care modelul de supraveghere este formulat în cadrul propunerii sunt coerente cu cadrul Sistemului de Informații Schengen II și cu Sistemul de informații privind vizele.

14. AEPD salută faptul că rolul său în domeniul supravegherii a fost clar stabilit, ceea ce nu s-a întâmplat, din motive evidente, în cazul textului anterior.

III. **DREPTUL LA INFORMARE**

15. Articolul 4 alineatul (1) literele (f)-(g) stipulează:

„De îndată ce o cerere de protecție internațională este prezentată, autoritățile competente ale statelor membre informează solicitantul de azil în ceea ce privește aplicarea prezentului regulament și, în special, referitor la:

(f) faptul că autoritățile competente pot face schimb de date referitoare la solicitant numai în scopul punerii în aplicare a obligațiilor care decurg din prezentul regulament;

(g) existența dreptului de acces la datele care îl (o) privesc și a dreptului de a solicita rectificarea datelor inexacte referitoare la persoana sa sau ștergerea datelor prelucrate în mod ilegal care îl (o) privesc, inclusiv dreptul de a primi informații privind procedurile de urmat pentru exercitarea acestor drepturi și datele de contact ale autorităților naționale pentru protecția datelor care tratează plângerile referitoare la protecția datelor cu caracter personal.”

Articolul 4 alineatul (2) descrie modalitățile prin care informațiile menționate la alineatul (1) al dispoziției ar trebui furnizate solicitantului.

16. Punerea în aplicare eficientă a dreptului la informare este esențială pentru buna funcționare a procedurii Dublin. În special, este esențial să se asigure faptul că informațiile sunt furnizate astfel încât să permită solicitantului de azil înțelegerea deplină a situației sale, precum și a sferei drepturilor, inclusiv a etapelor procedurale pe care le poate urma ulterior deciziilor administrative adoptate în cazul său.

17. În ceea ce privește aspectele practice ale punerii în aplicare ale dreptului, AEPD dorește să facă trimitere la faptul că, în conformitate cu articolul 4 alineatul (1) litera (g) și alineatul (2) din propunere, statele membre ar trebui să utilizeze o broșură comună pentru solicitanți, care cuprinde, printre alte informații, „datele de contact ale autorităților naționale pentru protecția datelor care tratează plângerile referitoare la protecția datelor cu caracter personal”. În acest context, AEPD dorește să sublinieze faptul că, în timp ce autoritățile naționale pentru protecția datelor (denumite în continuare „APD”), menționate la articolul 4 alineatul (2) din propunere, sunt într-adevăr competente pentru a trata plângerile referitoare la protecția datelor cu caracter personal, formularea propunerii nu ar trebui să împiedice solicitantul (persoana vizată) să adreseze o plângere în principal controlorului pentru protecția datelor (în acest caz, autoritățile competente naționale însărcinate cu cooperarea Dublin). Dispoziția de la articolul 4 alineatul (2), în formularea actuală, pare să implice faptul că solicitantul ar trebui să adreseze cererea sa – direct și în fiecare caz – autorității naționale pentru protecția datelor, în timp ce, conform procedurii standard și practicii din statele membre, solicitantul depune plângerea prima dată la controlorul pentru protecția datelor.

18. AEPD propune, de asemenea, ca textul de la articolul 4 litera (g) să fie reformulat pentru a clarifica drepturile care trebuie acordate solicitantului. Formularea propusă este neclară, întrucât poate fi interpretată în sensul considerării „dreptului de a primi informații privind procedurile de urmat pentru exercitarea acestor drepturi (…)” drept parte a dreptului de acces la date și/sau a dreptului de a solicita rectificarea datelor inexacte (…). În plus, conform formulării actuale a dispoziției sus-menționate, statele membre trebuie să informeze solicitantul nu cu privire la conținutul drepturilor, ci cu privire la „existența” acestora. Având în vedere că aceasta din urmă pare a fi o chestiune stilistică, AEPD propune reformularea articolului 4 alineatul (1) litera (g) după cum urmează:

„De îndată ce o cerere de protecție internațională este prezentată, autoritățile competente ale statelor membre informează solicitanții de azil (…) referitor la (…):

(g) dreptul de acces la datele care îl (o) privesc și dreptul de a solicita rectificarea datelor inexacte referitoare la persoana sa sau ștergerea datelor prelucrate în mod ilegal care îl (o) privesc, precum și privind procedurile de urmat pentru exercitarea acestor drepturi, inclusiv datele de contact ale autorităților menționate la articolul 33 din prezentul regulament și ale autorităților naționale pentru protecția datelor.”

19. În ceea ce privește metodele de furnizare a informațiilor către solicitanți, AEPD face trimitere la lucrările întreprinse de Grupul de coordonare a supravegherii Eurodac [1] (alcătuit din reprezentanți ai autorității pentru protecția datelor din fiecare din statele participante și AEPD). Grupul respectiv examinează în prezent această chestiune în cadrul EURODAC în vederea propunerii unor orientări relevante, de îndată ce rezultatele investigațiilor naționale vor fi disponibile și vor fi reunite. Deși această investigație coordonată se referă în mod precis la EURODAC, constatările sale vor fi probabil de interes și în contextul Dublin întrucât abordează chestiuni precum limbile/traducerile și evaluarea înțelegerii reale a informațiilor de către solicitantul de azil etc.

[1] Pentru explicații privind lucrările și statutul acestui grup, a se vedea: http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/79. Acest grup exercită o supraveghere coordonată a sistemului EURODAC. Totuși, din punct de vedere al protecției datelor, lucrările sale vor avea, de asemenea, un impact în contextul general al schimbului de informații din cadrul sistemului Dublin. Aceste informații se referă la aceeași persoană vizată, iar schimbul acestora se face urmând aceeași procedură în privința acesteia.

IV. CĂTRE TRANSPARENȚĂ

20. În ceea ce privește autoritățile menționate la articolul 33 din propunere, AEPD salută publicarea de către Comisie a unei liste consolidate a autorităților menționate la alineatul (1) din dispoziția sus-menționată în *Jurnalul Oficial al Uniunii Europene*. În cazul în care există modificări ale listei, Comisia publică o dată pe an o listă consolidată actualizată. Publicarea listei consolidate va contribui la asigurarea transparenței și va facilita supravegherea de către APD.

V. UN NOU MECANISM ÎN DOMENIUL SCHIMBULUI DE INFORMAȚII

21. AEPD ia act de introducerea unui nou mecanism în domeniul schimbului de informații relevante între statele membre înainte de efectuarea transferurilor (prevăzut la articolul 30 din propunere). AEPD consideră că scopul acestui schimb de informații este legitim.

22. De asemenea, AEPD ia act de existența unor garanții specifice privind protecția datelor în cadrul propunerii, în conformitate cu articolul 8 alineatele (1)-(3) din Directiva 95/46/CE privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, precum: (a) consimțământul explicit al solicitantului și/sau al reprezentantului acestuia, (b) ștergerea imediată a datelor de către statul membru expeditor după încheierea transferurilor și (c) „prelucrarea datelor cu caracter personal privind sănătatea numai de un cadru medical supus, în conformitate cu dreptul intern ori cu normele stabilite de autoritățile naționale competente, obligației secretului profesional sau de altă persoană supusă, de asemenea, unei obligații echivalente în ceea ce privește secretul" (care a beneficiat de o instruire medicală corespunzătoare). De asemenea, aceasta susține faptul că schimbul se va realiza numai prin intermediul sistemului securizat „DubliNet" și de către autoritățile notificate în prealabil.

23. Modul în care acest mecanism urmează a fi structurat este de o deosebită importanță pentru respectarea de către acesta a regimului de protecție a datelor, în special având în vedere că schimbul de informații va acoperi, de asemenea, date cu caracter personal extrem de sensibile, cum ar fi de exemplu informații privind „orice nevoi speciale ale persoanei care va fi transferată, care, în cazuri specifice, pot include informații privind starea fizică și mentală a persoanei vizate". În acest context, AEPD susține pe deplin includerea articolului 36 din propunere care obligă statele membre să adopte măsurile necesare pentru a se asigura că orice utilizare frauduloasă a datelor (…) se pedepsește prin sancțiuni, inclusiv sancțiuni de natură administrativă și/sau penală în conformitate cu legislația națională.

VI. REGLEMENTAREA SCHIMBULUI DE INFORMAȚII ÎN CADRUL SISTEMULUI DUBLIN

24. Articolul 32 din propunerea Comisiei reglementează *schimbul de informații*. AEPD a contribuit într-o etapă inițială la această dispoziție și susține formularea propusă de Comisie.

25. AEPD subliniază că este important ca autoritățile din statele membre să facă schimb de informații referitoare la persoane utilizând rețeaua DubliNet. Aceasta permite nu numai garantarea unei mai bune securități, ci și asigurarea unei mai bune trasabilități a tranzacțiilor. În acest sens, AEPD face trimitere la documentul de lucru al serviciilor Comisiei din 6 iunie 2007 „Document de însoțire a Raportului Comisiei către Parlamentul European și Consiliu asupra evaluării sistemului Dublin" ([1]), în care Comisia reamintește faptul că „utilizarea rețelei DubliNet este obligatorie în toate cazurile, cu excepția derogărilor definite la articolul 15 alineatul (1) al doilea paragraf" din Regulamentul (CE) nr. 1560/2003 al Comisiei din 2 septembrie 2003 de stabilire a normelor de aplicare a Regulamentului (CE) nr. 343/2003 al Consiliului de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de azil prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe ([2]) (denumit în continuare „Regulamentul de aplicare a Convenției de la Dublin"). AEPD insistă asupra faptului că posibilitatea derogării de la utilizarea rețelei DubliNet menționate la articolul 15 alineatul (1) sus-menționat ar trebui interpretată în mod restrictiv.

26. Anumite dispoziții au fost adăugate sau reformulate în cadrul propunerii pentru a asigura acest lucru, iar AEPD salută toate aceste eforturi. De exemplu, noul articol 33 alineatul (4) din propunere a fost reformulat pentru a clarifica faptul că nu numai cererile, ci și răspunsurile și întreaga corespondență scrisă fac obiectul unor norme privind instituirea mijloacelor de transmisie electronică sigură [prevăzute la articolul 15 alineatul (1) din Regulamentul de aplicare a Convenției de la Dublin]. În plus, eliminarea alineatului (2) din cadrul noului articol 38, care în textul anterior (articolul 25) obliga statele membre să transmită cererile și răspunsurile „printr-un mijloc care furnizează o dovadă de primire", se face pentru a clarifica faptul că statele membre ar trebui să utilizeze rețeaua DubliNet și în această privință.

27. AEPD ia act de faptul că, în cadrul sistemului Dublin, schimbul de informații cu caracter personal nu a fost reglementat decât într-o mică măsură. Deși anumite aspecte ale schimbului au fost deja abordate în Regulamentul de aplicare a Convenției de la Dublin, este regretabil că prezentul regulament nu pare a acoperi toate aspectele schimbului de informații cu caracter personal ([3]).

28. În acest context, merită menționat faptul că această chestiune a schimbului de informații referitoare la solicitantul de azil a făcut, de asemenea, obiectul discuțiilor în cadrul Grupului de coordonare a supravegherii Eurodac. Fără a anticipa rezultatele lucrărilor grupului, AEPD dorește să menționeze deja în această etapă că una din posibilele recomandări ar putea fi adoptarea unui set de norme similare celor convenite în manualul Schengen SIRENE.

([1]) SEC(2007) 742.
([2]) JO L 222, 5.9.2003, p. 3.
([3]) Acest lucru devine și mai evident dacă este comparat cu măsura în care schimbul de informații suplimentare a fost reglementat în cadrul Sistemului de Informații Schengen (SIRENE).

VII. **CONCLUZII**

29. AEPD susține propunerea Comisiei de regulament de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de azil prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe sau un apatrid. Aceasta înțelege motivele pentru revizuirea sistemului actual.

30. AEPD salută coerența propunerii Comisiei cu alte instrumente juridice care reglementează cadrul juridic complex al acestui domeniu.

31. AEPD salută atenția deosebită acordată în cadrul propunerii respectării drepturilor fundamentale, în special protecției datelor cu caracter personal. AEPD consideră că această abordare reprezintă o condiție prealabilă esențială pentru îmbunătățirea procedurii Dublin. Aceasta atrage în mod deosebit atenția legiuitorului asupra noilor mecanisme de schimb de date, care vor implica, printre altele, datele cu caracter personal extrem de sensibile ale solicitanților de azil.

32. De asemenea, AEPD dorește să facă trimitere la lucrările importante întreprinse în acest domeniu de Grupul de coordonare a supravegherii Eurodac și consideră că rezultatele lucrărilor grupului pot contribui în mod util la o mai bună formulare a caracteristicilor sistemului.

33. AEPD consideră că unele din observațiile formulate în prezentul aviz pot fi dezvoltate ulterior luând în considerare aspectele practice ale punerii în aplicare a sistemului revizuit. În special, aceasta intenționează să contribuie la definirea măsurilor de punere în aplicare privind schimbul de informații prin intermediul rețelei DubliNet astfel cum se menționează la punctele 24-27 din prezentul aviz.

Adoptat la Bruxelles, 18 februarie 2009.

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor

Avizul Autorității Europene pentru Protecția Datelor privind propunerea de regulament al Parlamentului European și al Consiliului privind instituirea sistemului „Eurodac" pentru compararea amprentelor digitale în scopul aplicării eficiente a Regulamentului (CE) nr. […/…] (de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de azil prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid) [COM(2008) 825]

(2009/C 229/02)

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR,

având în vedere Tratatul de instituire a Comunității Europene, în special articolul 286,

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 [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 [2], în special articolul 41,

având în vedere solicitarea unui aviz în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001 primită la 3 decembrie 2008 din partea Comisiei,

ADOPTĂ PREZENTUL AVIZ:

I. INTRODUCERE

Consultarea AEPD

1. Propunerea de regulament al Parlamentului European și al Consiliului privind instituirea sistemului „Eurodac" pentru compararea amprentelor digitale în scopul aplicării eficiente a Regulamentului (CE) nr. […/…] [de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de azil prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid] (denumită în continuare „propunerea" sau „propunerea Comisiei") a fost transmisă de către Comisie AEPD spre consultare la 3 decembrie 2008, în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001. Această consultare ar trebui menționată în mod explicit în preambulul regulamentului.

2. Astfel cum a fost menționat în expunerea de motive, AEPD a contribuit la prezenta propunere într-un stadiu inițial, iar multe dintre punctele pe care le-a ridicat în mod informal au fost luate în considerare în textul final al propunerii Comisiei.

Propunerea în contextul acesteia

3. Regulamentul (CE) nr. 2725/2000 al Consiliului [3] privind instituirea sistemului „Eurodac" (denumit în continuare „Regulamentul Eurodac") a intrat în vigoare la 15 decembrie 2000. Eurodac, sistem informatic comunitar, a fost conceput să faciliteze aplicarea Convenției de la Dublin, menită să instituie un mecanism clar și operativ de determinare a responsabilității privind cererile de azil prezentate într-unul dintre statele membre. Convenția de la Dublin a fost ulterior înlocuită de un instrument legislativ comunitar, Regulamentul (CE) nr. 343/2003 al Consiliului din 18 februarie 2003 de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de azil prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe [4] (denumit în continuare „Regulamentul Dublin") [5]. EURODAC a devenit operațional la 15 ianuarie 2003.

4. Propunerea reprezintă o revizuire a Regulamentului Eurodac și a regulamentului de punere în aplicare a acestuia, Regulamentul (CE) nr. 407/2002 al Consiliului, și vizează *inter alia*:

   — îmbunătățirea eficienței punerii în aplicare a Regulamentului Eurodac;

   — garantarea coerenței cu acquis-ul în domeniul azilului, astfel cum a evoluat în urma adoptării regulamentului sus-menționat;

   — actualizarea unei serii de dispoziții ținând seama de evoluțiile factuale ulterioare adoptării regulamentului;

   — instituirea unui nou cadru de gestionare.

5. De asemenea, ar trebui subliniat faptul că unul dintre obiectivele principale ale propunerii este de a garanta mai eficient respectarea drepturilor fundamentale, în special protecția datelor cu caracter personal. Prezentul aviz va analiza dacă dispozițiile propunerii vizate îndeplinesc corespunzător acest obiectiv.

[1] JO L 281, 23.11.1995, p. 31.
[2] JO L 8, 12.1.2001, p. 1.
[3] JO L 316, 15.12.2000, p. 1.
[4] JO L 50, 25.2.2003, p. 1.
[5] Regulamentul Dublin face în prezent, de asemenea, obiectul unei revizuiri [COM(2008) 820 final], 3.12.2008 (versiune reformată). AEPD a emis, de asemenea, un aviz privind propunerea Dublin.

6. Propunerea ține seama de rezultatele Raportului Comisiei de evaluare a sistemului Dublin din iunie 2007 (denumit în continuare „raportul de evaluare"), care acoperă primii 3 ani de funcționare a Eurodac (2003-2005).

7. Deși recunoaște că sistemul instituit de regulament a fost pus în aplicare în statele membre în general în mod satisfăcător, raportul de evaluare al Comisiei a identificat anumite dificultăți legate de eficiența dispozițiilor actuale și a evidențiat punctele care trebuie soluționate în vederea îmbunătățirii sistemului Eurodac și a facilitării aplicării Regulamentului Dublin. În special, raportul de evaluare a constatat faptul că unele din statele membre transmit în continuare amprentele digitale cu întârziere. Regulamentul Eurodac nu fixează în prezent decât un termen foarte vag pentru transmiterea amprentelor digitale, ceea ce, în practică, poate cauza întârzieri semnificative. Aceasta reprezintă un aspect crucial pentru eficiența sistemului, deoarece transmiterea tardivă poate conduce la rezultate contrare principiilor de responsabilitate prevăzute de Regulamentul Dublin.

8. Raportul de evaluare a subliniat, de asemenea, faptul că absența unei metode eficiente care să permită statelor membre să se informeze reciproc în privința statutului unui solicitant de azil a condus în numeroase cazuri la gestionarea ineficientă a ștergerilor de date. Statele membre care introduc date referitoare la o anumită persoană adesea nu sunt la curent cu faptul că un alt stat membru de origine a șters date și, prin urmare, nu știu că ar trebui, de asemenea, să șteargă datele referitoare la acea persoană. În consecință, nu se poate asigura în mod corespunzător respectarea principiului conform căruia „niciun fel de date nu trebuie păstrate într-o formă care permite identificarea persoanelor vizate o perioadă mai lungă decât este necesar în vederea atingerii scopurilor pentru care au fost colectate".

9. În plus, conform analizei prezentate în raportul de evaluare, desemnarea imprecisă a autorităților naționale care au acces la Eurodac limitează rolul de monitorizare al Comisiei și al Autorității Europene pentru Protecția Datelor.

Punctele centrale ale avizului

10. Având în vedere rolul său actual de autoritate de supraveghere a Eurodac, AEPD este în mod deosebit interesată de propunerea Comisiei și de rezultatele pozitive ale revizuirii sistemului Eurodac în ansamblu.

11. AEPD remarcă faptul că propunerea implică diferite aspecte legate de drepturile fundamentale ale solicitanților de azil, precum dreptul de azil, dreptul la informare în sens larg și dreptul la protecția datelor cu caracter personal. Totuși, având în vedere misiunea AEPD, prezentul aviz se va axa în principal pe chestiunile de protecție a datelor abordate de regulamentul revizuit. În acest sens, AEPD salută atenția deosebită acordată în cadrul propunerii respectării și protecției datelor cu caracter personal. Cu această ocazie, AEPD subliniază că asigurarea unui înalt nivel de protecție a datelor cu caracter personal și punerea în aplicare mai eficientă a acestuia ar trebui considerate o condiție prealabilă esențială pentru îmbunătățirea funcționării Eurodac.

12. Prezentul aviz abordează în principal următoarele modificări ale textului, dat fiind că acestea sunt cele mai relevante din punct de vedere al protecției datelor cu caracter personal:

— supravegherea de către AEPD, inclusiv în cazurile în care o parte a gestionării sistemului este încredințată unei alte entități (precum o companie privată);

— procedura de luare a amprentelor digitale, inclusiv definirea limitelor de vârstă;

— drepturile persoanei vizate.

II. **OBSERVAȚII GENERALE**

13. AEPD salută faptul că propunerea vizează coerența cu alte instrumente juridice care reglementează instituirea și/sau utilizarea altor sisteme IT la scară largă. În special, împărțirea responsabilităților privind baza de date, precum și modul în care modelul de supraveghere a fost formulat în cadrul propunerii sunt coerente cu instrumentele juridice de instituire a Sistemului de Informații Schengen II (SIS II) și a Sistemului de Informații privind Vizele (VIS).

14. AEPD ia act de coerența propunerii cu Directiva 95/46/CE și cu Regulamentul (CE) nr. 45/2001. În acest context, AEPD salută în special noile considerente 17, 18 și 19, care stipulează că Directiva 95/46/CE și Regulamentul (CE) nr. 45/2001 se aplică prelucrării datelor cu caracter personal, efectuată în aplicarea regulamentului propus, de către statele membre și, respectiv, de către instituțiile și organele comunitare implicate.

15. În cele din urmă, AEPD atrage atenția asupra necesității de a asigura, de asemenea, coerența deplină între Regulamentul Eurodac și Regulamentul Dublin și, cu ocazia prezentului aviz, oferă indicații mai precise cu privire la această coerență. Totuși, AEPD remarcă faptul că, în anumite privințe, această chestiune a fost deja abordată în cadrul propunerii, de exemplu în expunerea de motive, care menționează că „coerența cu Regulamentul Dublin (precum și soluționarea preocupărilor privind protecția datelor, în special respectarea principiului proporționalității) va fi garantată prin alinierea perioadei de conservare a datelor privind resortisanții țărilor terțe sau apatrizii cărora li s-au luat amprentele digitale în legătură cu trecerea ilegală a frontierei externe cu perioada pentru care articolul 14 alineatul (1) din Regulamentul Dublin atribuie responsabilitatea pe baza acestor informații (și anume un an)".

III. OBSERVAȚII SPECIFICE

III.1. Supravegherea de către Autoritatea Europeană pentru Protecția Datelor

16. AEPD salută modelul de supraveghere prevăzut în cadrul propunerii, precum și sarcinile specifice care i-au fost încredințate în temeiul articolelor 25 și 26 din propunere. Articolul 25 încredințează AEPD două sarcini de supraveghere:

— „verifică dacă activitățile de prelucrare a datelor cu caracter personal desfășurate de Autoritatea de gestionare sunt realizate în conformitate cu regulamentul" [articolul 25 alineatul (1)] și

— „garantează că, cel puțin la fiecare patru ani, se realizează un audit al activităților de prelucrare a datelor cu caracter personal desfășurate de Autoritatea de gestionare, în conformitate cu normele internaționale de audit".

Articolul 26 abordează chestiunea cooperării dintre autoritățile naționale de supraveghere și AEPD.

17. De asemenea, AEPD remarcă faptul că propunerea avansează o abordare similară celei utilizate în cadrul SIS II și VIS: un sistem stratificat de supraveghere prin care autoritățile pentru protecția datelor (APD) și AEPD supraveghează nivelul național și, respectiv, nivelul european, cu un sistem de cooperare instituit între cele două niveluri. Modul în care modelul de supraveghere este preconizat în cadrul propunerii reflectă, de asemenea, practica actuală, care s-a dovedit eficientă și a încurajat o strânsă colaborare între AEPD și APD. Prin urmare, AEPD salută formalizarea acestuia în cadrul propunerii și faptul că, atunci când a prevăzut acest lucru, legiuitorul a asigurat coerența cu sistemele de supraveghere ale altor sisteme IT la scară largă.

III.2. Subcontractare

18. AEPD ia act de faptul că propunerea nu abordează chestiunea subcontractării unei părți a sarcinilor Comisiei către o altă organizație sau entitate (precum o companie privată). Totuși, subcontractarea este utilizată în mod obișnuit de Comisie în gestionarea și dezvoltarea atât a sistemului, cât și a infrastructurii de comunicare. Deși subcontractarea în sine nu este contrară cerințelor de protecție a datelor, ar trebui instituite garanții importante pentru a asigura faptul că aplicabilitatea Regulamentului (CE) nr. 45/2001, inclusiv supravegherea de către AEPD a protecției datelor, rămâne în întregime neafectată de subcontractarea activităților. În plus, ar trebui de asemenea adoptate garanții suplimentare cu un caracter mai tehnic.

19. În acest sens, AEPD propune ca în cadrul revizuirii Regulamentului Eurodac să se prevadă garanții juridice similare celor avute în vedere în cadrul instrumentelor juridice ale SIS II, precizând că, și atunci când Comisia încredințează gestionarea sistemului unei alte autorități, aceasta „nu aduce atingere niciunui mecanism de control efectiv exercitat, în conformitate cu dreptul comunitar, de către Curtea de Justiție, Curtea de Conturi sau de către Autoritatea Europeană pentru Protecția Datelor" [articolul 15 alineatul (7), Decizia și Regulamentul SIS II].

20. Dispozițiile sunt și mai precise la articolul 47 din Regulamentul SIS II, care stipulează: „În cazul în care (…) Comisia deleagă responsabilități către un alt organism sau alte organisme, (…) aceasta se asigură că Autoritatea Europeană pentru Protecția Datelor are dreptul și posibilitatea de a-și îndeplini pe deplin misiunea, inclusiv de a proceda la verificări la fața locului și de a exercita orice alte competențe care i-au fost conferite în temeiul articolului 47 din Regulamentul (CE) nr. 45/2001".

21. Dispozițiile sus-menționate oferă o claritate necesară în ceea ce privește consecințele subcontractării unei părți a sarcinilor Comisiei către alte autorități. Prin urmare, AEPD propune adăugarea în textul propunerii Comisiei a unor dispoziții vizând același efect.

III.3. Procedura de luare a amprentelor digitale [articolul 3 alineatul (5) și articolul 6]

22. Articolul 3 alineatul (5) din propunere abordează procedura de luare a amprentelor digitale. Dispoziția respectivă stipulează că procedura „se stabilește și aplică în conformitate cu practica națională a statului membru în cauză și în conformitate cu garanțiile prevăzute de Carta drepturilor fundamentale a Uniunii Europene, de Convenția pentru apărarea drepturilor omului și a libertăților fundamentale și Convenția europeană a drepturilor omului și de Convenția Organizației Națiunilor Unite cu privire la drepturile copilului". Articolul 6 din propunere prevede că limita inferioară de vârstă pentru luarea amprentelor digitale ale unui solicitant este de 14 ani, iar acestea se iau în termen de cel mult 48 de ore de la data depunerii cererii.

23. În primul rând, în ceea ce privește limita de vârstă, AEPD subliniază necesitatea de a asigura coerența propunerii cu Regulamentul Dublin. Sistemul Eurodac a fost instituit în vederea asigurării aplicării eficiente a Regulamentului Dublin. Aceasta înseamnă că, în cazul în care rezultatele revizuirii în curs a Regulamentului Dublin au un impact asupra aplicării acestuia pentru solicitanții de azil minori, acest lucru ar trebui să se reflecte în Regulamentul Eurodac [1].

[1] În acest sens, AEPD atrage atenția asupra faptului că propunerea Comisiei privind revizuirea Regulamentului Dublin prezentată la 3 decembrie 2008 [COM(2008) 820 final] definește un „minor" drept „un resortisant al unei țări terțe sau un apatrid cu vârsta sub 18 ani".

24. În al doilea rând, în ceea ce privește stabilirea limitelor de vârstă pentru luarea amprentelor digitale în general, AEPD dorește să sublinieze că majoritatea documentației disponibile în prezent tinde să indice faptul că exactitatea identificării prin luarea amprentelor digitale descrește odată cu procesul de îmbătrânire. În acest sens, este de dorit să se urmeze îndeaproape studiul privind luarea amprentelor digitale realizat în cadrul punerii în aplicare a VIS. Fără a anticipa rezultatele studiului, AEPD dorește să sublinieze deja în această etapă că în toate cazurile în care luarea amprentelor digitale se dovedește imposibilă sau ar conduce la rezultate care nu sunt fiabile, este important să se facă trimitere la proceduri alternative, care ar trebui să respecte pe deplin demnitatea persoanei.

25. În al treilea rând, AEPD remarcă eforturile depuse de legiuitor pentru a asigura respectarea cerințelor internaționale și europene în materie de drepturile omului de către dispozițiile privind luarea amprentelor digitale. Totuși, aceasta atrage atenția asupra dificultăților întâlnite în câteva state membre privind determinarea vârstei tinerilor solicitanți de azil. Foarte adesea, solicitanții de azil sau imigranții ilegali nu posedă documente de identificare, iar pentru a stabili dacă ar trebui să li se ia amprente digitale, trebuie determinată vârsta acestora. Metodele utilizate în această privință fac obiectul unor dezbateri numeroase în diferite state membre.

26 În acest sens, AEPD atrage atenția asupra faptului că Grupul de coordonare a supravegherii Eurodac ([1]) a lansat o inspecție coordonată privind această chestiune, ale cărei rezultate – preconizate pentru prima jumătate a anului 2009 – ar trebui să faciliteze stabilirea unor proceduri comune în această privință.

27. Ca observație finală asupra acestei chestiuni, AEPD consideră că sunt necesare o mai bună coordonare și o mai bună armonizare la nivelul UE a procedurilor de luare a amprentelor digitale cât mai mult posibil.

III.4. **Cele mai bune tehnici existente (articolul 4)**

28. Articolul 4 alineatul (1) din propunere stipulează: „După o perioadă de tranziție, o autoritate de administrare, finanțată de la bugetul general al Uniunii Europene, este responsabilă de gestionarea operațională a Eurodac. Autoritatea de gestionare asigură, în cooperare cu statele membre, faptul că sistemul central dispune în orice moment de cea mai bună tehnologie existentă, sub rezerva unei analize cost-beneficiu". Deși AEPD salută cerința prevăzută la articolul 4 alineatul (1), aceasta dorește să remarce faptul că expresia „cea mai bună tehnologie existentă" menționată în cadrul dispoziției de mai sus ar trebui înlocuită cu formularea „cele mai bune tehnici existente", care include atât tehnologia utilizată, cât și modul în care instalația este concepută, construită, întreținută și exploatată.

III.5. **Ștergerea anticipată a datelor (articolul 9)**

29. Articolul 9 alineatul (1) din propunere abordează chestiunea ștergerii anticipate a datelor. Dispoziția respectivă obligă statul membru de origine să șteargă din sistemul central „datele privind persoanele care au dobândit cetățenia oricărui stat membru înainte de expirarea perioadei menționate la articolul 8" de îndată ce statul membru de origine află că persoana în cauză a dobândit cetățenia. AEPD salută obligația de a șterge datele, având în vedere că aceasta corespunde întru totul principiului privind calitatea datelor. În plus, AEPD consideră că revizuirea dispoziției respective oferă posibilitatea de a încuraja statele membre să instituie proceduri care să asigure ștergerea fiabilă și la timp (automată dacă este posibil) a datelor atunci când o persoană obține cetățenia unuia dintre statele membre.

30. De asemenea, AEPD dorește să sublinieze că articolul 9 alineatul (2), care abordează ștergerea anticipată, ar trebui reformulat, întrucât formularea propusă este neclară. Ca observație stilistică, AEPD propune înlocuirea în cadrul dispoziției a cuvântului „acesta" cu cuvântul „acestea".

III.6. **Perioada de conservare a datelor referitoare la un resortisant al unei țări terțe care este reținut pentru trecerea ilegală a frontierei (articolul 12)**

31. Articolul 12 din propunere abordează conservarea datelor. AEPD dorește să remarce faptul că stabilirea unui interval de 1 an ca perioadă de conservare a datelor (în loc de 2 ani în textul actual al regulamentului) constituie o bună aplicare a principiului privind calitatea datelor care stipulează că datele nu ar trebui conservate mai mult timp decât este necesar pentru îndeplinirea scopului în care sunt prelucrate. Aceasta reprezintă o îmbunătățire salutară a textului.

III.7. **Lista autorităților care au acces la EURODAC (articolul 20)**

32. Dispoziția care prevede publicarea de către Autoritatea de gestionare a listei autorităților care au acces la Eurodac este salutară. Aceasta va facilita obținerea unei mai mari transparențe și crearea unui instrument practic pentru o mai bună supraveghere a sistemului, de exemplu prin APD.

III.8. **Înregistrări (articolul 21)**

33. Articolul 21 din propunere se referă la evidența tuturor operațiunilor de prelucrare a datelor în cadrul sistemului central. Articolul 21 alineatul (2) precizează că aceste evidențe ar trebui folosite numai pentru controlul, din prisma protejării datelor, al admisibilității prelucrării (…) În această privință, ar putea fi clarificat faptul că aceasta include, de asemenea, măsuri de audit intern.

([1]) Pentru explicații privind lucrările și statutul acestui grup, a se vedea: http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/79. Acest grup exercită o supraveghere coordonată a sistemului EURODAC.

III.9. **Drepturile persoanelor vizate (articolul 23)**

34. Articolul 23 alineatul (1) litera (e) din propunere are următorul conținut:

„O persoană care intră sub incidența prezentului regulament este informată de către statul membru de origine (…) cu privire la:

(e) existența dreptului de acces la datele care le privesc și a dreptului de a cere rectificarea datelor eronate referitoare la acestea sau ștergerea datelor care le privesc prelucrate în mod ilegal, inclusiv a dreptului de a primi informații despre procedurile de exercitare a acestor drepturi și datele de contact ale autorităților naționale de supraveghere menționate la articolul 25 alineatul (1), care soluționează plângerile referitoare la protecția datelor cu caracter personal".

35. AEPD ia act de faptul că punerea în aplicare eficientă a dreptului la informare este esențială pentru buna funcționare a Eurodac. În special, este esențial să se asigure că informațiile sunt furnizate astfel încât să permită solicitantului de azil înțelegerea deplină a situației sale, precum și a sferei drepturilor, inclusiv a etapelor procedurale pe care le poate urma ulterior deciziilor administrative adoptate în cazul său.

36. În ceea ce privește aspectele practice ale punerii în aplicare a dreptului, AEPD dorește să sublinieze că, deși APD sunt într-adevăr competente să soluționeze plângeri referitoare la protecția datelor cu caracter personal, formularea propunerii nu ar trebui să împiedice solicitantul (persoana vizată) să adreseze o plângere în principal controlorului pentru protecția datelor. Dispoziția de la articolul 23 alineatul (1) litera (e) în formularea sa actuală pare să implice faptul că solicitantul ar trebui să formuleze cererea – direct și în fiecare caz – către APD, în timp ce, conform procedurii standard și practicii din statele membre, solicitantul adresează plângerea prima dată controlorului pentru protecția datelor.

37. De asemenea, AEPD propune reformularea literei (e) de la articolul 23 alineatul (1) pentru a clarifica drepturile care trebuie acordate solicitantului. Formularea propusă este neclară, întrucât poate fi interpretată în sensul considerării „dreptului de a primi informații despre procedurile de exercitare a acestor drepturi (…)" ca parte a dreptului de acces la date și/sau a dreptului de a cere rectificarea datelor eronate (…). În plus, conform formulării actuale a dispoziției sus-menționate, statele membre trebuie să informeze persoana care intră sub incidența regulamentului nu cu privire la conținutul drepturilor, ci cu privire la „existența" acestora. Având în vedere că cea din urmă pare a fi o chestiune stilistică, AEPD propune ca articolul 23 alineatul (1) litera (e) să fie reformulat după cum urmează:

„O persoană care intră sub incidența prezentului regulament este informată de către statul membru de origine (…) cu privire la(…):

(g) dreptul de acces la datele care o privesc și dreptul de a cere rectificarea datelor eronate referitoare la aceasta sau ștergerea datelor care o privesc prelucrate în mod ilegal, precum și despre procedurile de exercitare a acestor drepturi, inclusiv datele de contact ale autorităților naționale de supraveghere menționate la articolul 25 alineatul (1)".

38. Urmând aceeași logică, articolul 23 alineatul (10) ar trebui modificat după cum urmează: „În fiecare stat membru, autoritatea națională de supraveghere asistă, după caz (sau: la cererea persoanei vizate), persoanele vizate în conformitate cu articolul 28 alineatul (4) din Directiva 95/46/CE în exercitarea drepturilor acestora". Din nou, AEPD dorește să sublinieze că o intervenție a APD nu ar trebui, în principiu, să fie necesară; dimpotrivă, controlorul pentru protecția datelor ar trebui încurajat să răspundă într-un mod adecvat la plângerile persoanelor vizate. Același lucru se aplică atunci când este necesară cooperarea între autorități din diferite state membre. Controlorii pentru protecția datelor ar trebui să fie în principal responsabili de gestionarea cererilor și să coopereze în acest sens.

39. În ceea ce privește articolul 23 alineatul (9), AEPD salută nu numai scopul în sine al dispoziției respective (care are în vedere controlul utilizării „căutărilor speciale" astfel cum au recomandat autoritățile pentru protecția datelor în primul lor raport privind inspecțiile coordonate), ci ia act cu satisfacție și de procedura propusă pentru îndeplinirea acestuia.

40. În ceea ce privește metodele de furnizare a informațiilor către solicitanți, AEPD face trimitere la lucrările întreprinse de Grupul de coordonare a supravegherii Eurodac. Grupul respectiv examinează în prezent această chestiune în cadrul EURODAC pentru a propune – de îndată ce rezultatele investigațiilor naționale vor fi cunoscute și reunite – orientări relevante.

IV. **CONCLUZII**

41. AEPD susține propunerea de regulament al Parlamentului European și al Consiliului privind instituirea sistemului „Eurodac" pentru compararea amprentelor digitale în scopul aplicării eficiente a Regulamentului (CE) nr. […/…] de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de azil prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid.

42. AEPD salută modelul de supraveghere propus în cadrul propunerii, precum și rolul și sarcinile care i-au fost încredințate în cadrul noului sistem. Modelul preconizat reflectă practica actuală, care s-a dovedit eficientă.

43. AEPD ia act de faptul că propunerea vizează coerența cu alte instrumente juridice care reglementează instituirea și/sau utilizarea altor sisteme IT la scară largă.

44. AEPD salută atenția deosebită acordată în cadrul propunerii respectării drepturilor fundamentale, în special protecției datelor cu caracter personal. Astfel cum a fost, de asemenea, menționat în avizul privind revizuirea Regulamentului Dublin, AEPD consideră această abordare drept o condiție prealabilă esențială pentru îmbunătățirea procedurilor de azil în Uniunea Europeană.

45. AEPD atrage atenția asupra necesității de a asigura coerența deplină între Regulamentul Eurodac și Regulamentul Dublin.

46. AEPD consideră că sunt necesare o mai bună coordonare și o mai bună armonizare la nivelul UE a procedurilor de luare a amprentelor digitale, care se referă la solicitanții de azil sau la orice alte persoane care fac obiectul procedurii Eurodac. Aceasta atrage în mod deosebit atenția asupra chestiunii limitelor de vârstă pentru luarea amprentelor digitale și, în special, asupra dificultăților întâlnite în câteva state membre privind determinarea vârstei tinerilor solicitanți de azil.

47. AEPD insistă asupra clarificării dispozițiilor privind drepturile persoanelor vizate și, în special, subliniază faptul că controlorii pentru protecția datelor la nivel național sunt în principal responsabili de asigurarea aplicării acestor drepturi.

Adoptat la Bruxelles, 18 februarie 2009.

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor

Avizul Autorității Europene pentru Protecția Datelor privind Inițiativa Republicii Franceze în vederea adoptării deciziei Consiliului referitoare la utilizarea tehnologiei informației în domeniul vamal (5903/2/09 REV 2)

(2009/C 229/03)

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR,

având în vedere Tratatul de instituire a Comunității Europene, în special articolul 286,

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 ([1]),

având în vedere Decizia-cadru 2008/977/JAI a Consiliului din 27 noiembrie 2008 privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală ([2]),

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 ([3]) și, în special, articolul 41 al acestuia,

ADOPTĂ PREZENTUL AVIZ:

I. INTRODUCERE

Consultarea AEPD

1. Inițiativa Republicii Franceze în vederea adoptării deciziei Consiliului referitoare la utilizarea tehnologiei informației în domeniul vamal a fost publicată în Jurnalul Oficial la 5 februarie 2009 ([4]). Nu a fost solicitată consilierea AEPD cu privire la această inițiativă nici de către statul membru care a propus-o, nici de către Consiliu. Cu toate acestea, Comisia pentru libertăți civile, justiție și afaceri interne din cadrul Parlamentului European i-a solicitat AEPD să formuleze observații pe marginea inițiativei Franței, în conformitate cu articolul 41 din Regulamentul (CE) nr. 45/2001, în contextul avizului Parlamentului European cu privire la inițiativă. În cazurile similare ([5]), în care AEPD a emis un aviz cu privire la propria inițiativă, prezentul aviz trebuie să fie de asemenea considerat drept o reacție la solicitarea Parlamentului European.

2. În opinia AEPD, prezentul aviz ar trebui menționat în preambulul la decizia Consiliului, în același mod în care avizul acesteia este menționat într-o serie de instrumente juridice adoptate pe baza unei propuneri a Comisiei.

3. Chiar dacă, în cazul unui stat membru care preia inițiativa privind o măsură legislativă în conformitate cu titlul VI din Tratatul UE, nu este stipulată nicio obligație legală de a solicita consilierea AEPD, normele aplicabile nici nu împiedică solicitarea unei asemenea consilieri. AEPD își exprimă regretul că nici Republica Franceză, nici Consiliul nu i-au solicitat consilierea în cazul de față.

4. AEPD subliniază faptul că, datorită evoluțiilor în curs în privința propunerii în cadrul Consiliului, observațiile prezentate în prezentul aviz se bazează pe versiunea propunerii din 24 februarie 2009 (5903/2/09 REV 2), care a fost publicată pe site-ul web al Parlamentului European ([6]).

5. AEPD a identificat nevoia de explicații suplimentare cu privire la justificarea inițiativei în sine, precum și cu privire la unele articole și mecanisme specifice din cadrul inițiativei. AEPD își exprimă regretul cu privire la absența unui studiu de impact sau a unei expuneri de motive care să însoțească inițiativa. Aceasta reprezintă un element necesar care consolidează transparența și, în general, calitatea procesului legislativ. Informațiile explicative ar facilita, de asemenea, evaluarea unei serii de sugestii din cadrul propunerii, de exemplu în ceea ce privește necesitatea și justificarea accesului la SIV care urmează să fie acordat Europol și Eurojust.

6. AEPD a luat în considerare Avizul 09/03 emis, la 24 martie 2009, de Autoritatea comună de control al vămilor cu privire la proiectul de decizie a Consiliului privind utilizarea tehnologiei informației în domeniul vamal.

Propunerea și contextul acesteia

7. Cadrul juridic pentru Sistemul de Informații al Vămilor (denumit în continuare „SIV") este reglementat în momentul de față atât de instrumente din primul pilon, cât și de instrumente din al treilea pilon. Cadrul juridic al celui de al treilea pilon care reglementează sistemul constă în principal din Convenția din 26 iulie 1995, încheiată în temeiul articolului K.3 din Tratatul privind Uniunea Europeană, privind utilizarea tehnologiei informației în domeniul vamal [denumită în continuare „Convenția" ([7])], precum și din protocoalele din 12 martie 1999 și 8 martie 2003.

8. Mecanismele existente privind protecția datelor implică aplicarea Convenției Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal din 28 ianuarie 1981 (denumită în continuare „Convenția nr. 108 a Consiliului Europei"). În plus, Decizia-cadru 2008/977/JAI se aplică SIV în temeiul propunerii.

([1]) JO L 281, 23.11.1995, p. 31.
([2]) JO L 350, 30.12.2008, p. 60.
([3]) JO L 8, 12.1.2001, p. 1.
([4]) JO C 29, 5.2.2009, p. 6.
([5]) A se vedea, cel mai recent, Avizul Autorității Europene pentru Protecția Datelor privind Inițiativa a 15 state membre în vederea adoptării unei decizii a Consiliului privind consolidarea Eurojust și modificarea Deciziei 2002/187/JAI, JO C 310, 5.12.2008, p. 1.
([6]) http://www.europarl.europa.eu/meetdocs/2004_2009/organes/libe/libe_20090330_1500.htm
([7]) JO C 316, 27.11.1995, p. 33.

9. Partea sistemului care ține de primul pilon este reglementată de Regulamentul (CE) nr. 515/97 al Consiliului din 13 martie 1997 privind asistența reciprocă între autoritățile administrative ale statelor membre și cooperarea dintre acestea și Comisie în vederea asigurării aplicării corespunzătoare a legislației din domeniile vamal și agricol ([1]).

10. Obiectivul Convenției SIV, în conformitate cu dispozițiile articolului 2 alineatul (2), a fost acela de a „ajuta la prevenirea, investigarea și urmărirea penală a infracțiunilor grave împotriva legislațiilor naționale întărind, printr-o rapidă difuzare a informațiilor, eficacitatea procedurilor de cooperare și de control ale autorităților vamale ale statelor membre".

11. În conformitate cu Convenția SIV, Sistemul de Informații al Vămilor este format dintr-o bază de date centrală accesibilă prin terminalele aflate în fiecare din statele membre. Alte trăsături principale sunt următoarele:

— Convenția SIV prevede că SIV poate include numai date, inclusiv date cu caracter personal, necesare atingerii scopului, din următoarele categorii: (a) mărfuri; (b) mijloace de transport; (c) întreprinderi; (d) persoane; (e) tendințe de fraudă; (f) competențe disponibile ([2]);

— statele membre stabilesc elementele care urmează să fie incluse în SIV corespunzătoare fiecăreia dintre ultimele trei categorii, în măsura în care această acțiune este necesară pentru atingerea obiectivului sistemului. Datele cu caracter personal nu trebuie în niciun caz să fie introduse în ultimele două categorii. Accesul direct la datele cuprinse în Sistemul de Informații al Vămilor este rezervat în momentul de față exclusiv autorităților naționale desemnate de fiecare stat membru. Aceste autorități naționale sunt autorități vamale, dar pot include în egală măsură alte autorități abilitate, în conformitate cu actele cu putere de lege, normele administrative și procedurile statului membru respectiv, să acționeze în vederea atingerii obiectivului Convenției;

— statele membre pot utiliza datele din Sistemul de Informații al Vămilor numai pentru a atinge obiectivul Convenției; cu toate acestea, sub rezerva unei autorizări prealabile și a condițiilor impuse de către statul membru care le-a introdus în sistem, acestea pot să utilizeze respectivele date, în scop administrativ sau în alt scop. A fost instituită o autoritate comună de control pentru a supraveghea partea din SIV care ține de al treilea pilon.

12. Inițiativa Franței, care se bazează pe articolul 30 alineatul (1) litera (a) și articolul 34 alineatul (2) din Tratatul privind Uniunea Europeană, este menită să înlocuiască Convenția SIV, precum și Protocolul din 12 martie 1999 și Protocolul din 8 martie 2003 pentru a alinia partea din sistem care ține de al treilea pilon la instrumentele primului pilon.

13. Cu toate acestea, propunerea depășește cadrul înlocuirii textului Convenției SIV cu o decizie a Consiliului. Aceasta modifică un număr semnificativ de dispoziții ale Convenției și extinde actualul domeniu de acces la SIV prin acordarea accesului pentru Europol și Eurojust. În plus, propunerea include dispoziții similare cu privire la funcționarea SIV, astfel cum se prevede în Regulamentul (CE) nr. 766/2008 menționat anterior, de exemplu în măsura în care este vizată crearea unei baze de date pentru identificarea dosarelor vamale (capitolul VI).

14. De asemenea, propunerea ține seama de noi instrumente juridice precum Decizia-cadru 2008/977/JAI și Decizia-cadru 2006/960/JAI din 13 decembrie 2006 privind simplificarea schimbului de informații și date operative între autoritățile de aplicare a legii ale statelor membre ale Uniunii Europene ([3]).

15. Propunerea vizează, printre altele:

— consolidarea cooperării între autoritățile vamale, prin stabilirea de proceduri conform cărora administrațiile vamale să poată acționa în comun și să poată face schimb de date cu caracter personal și de alte date referitoare la activitățile de trafic ilicit, utilizând noi tehnologii pentru gestionarea și transmiterea unor astfel de informații. Aceste operațiuni de prelucrare fac obiectul dispozițiilor Convenției nr. 108 a Consiliului Europei, al Deciziei-cadru 2008/977/JAI și al principiilor incluse în Recomandarea R (87) 15 a Comitetului de Miniștri al Consiliului Europei din 17 septembrie 1987, care reglementează utilizarea datelor cu caracter personal în sectorul polițienesc;

— creșterea gradului de complementaritate cu acțiunile întreprinse în contextul cooperării cu Europol și Eurojust, permițând accesul acestor organisme la Sistemul de Informații al Vămilor.

16. În acest context, obiectivul SIV, în conformitate cu articolul 1 din propunere, este acela de a „ajuta la prevenirea, investigarea și urmărirea penală a infracțiunilor grave împotriva legislațiilor naționale, întărind, printr-o mai rapidă difuzare a informațiilor, eficacitatea procedurilor de cooperare și de control ale autorităților vamale ale statelor membre". Această dispoziție reflectă în mare măsură articolul 2 alineatul (2) din Convenția SIV.

17. Pentru a atinge acest obiectiv, propunerea extinde domeniul de utilizare a datelor SIV, incluzând căutări în sisteme și posibilitatea de a efectua analize strategice sau operaționale. AEPD ia act de extinderea scopului și a listei de categorii de date cu caracter personal care urmează să fie colectate și prelucrate, precum și de extinderea listei de persoane vizate care au acces direct la SIV.

([1]) JO L 82, 22.3.1997, p. 1.

([2]) Propunerea adaugă o nouă categorie: (g) reținerea, punerea sub sechestru sau confiscarea articolelor.

([3]) JO L 386, 29.12.2006, p. 89.

Punctele centrale ale avizului

18. Având în vedere rolul său actual de autoritate de control pentru partea centrală din partea din SIV care ține de primul pilon, AEPD este în special interesată de inițiativă și de recentele evoluții din cadrul Consiliului privind conținutul acesteia. AEPD pune accentul pe nevoia de a asigura o abordare coerentă și cuprinzătoare pentru a alinia părțile din sistem care țin de primul și al treilea pilon.

19. AEPD ia act de faptul că propunerea implică diferite aspecte privind drepturile fundamentale, în special protecția datelor cu caracter personal, precum și dreptul la informare și alte drepturi ale persoanelor vizate.

20. În ceea ce privește actualul sistem de protecție a datelor din Convenția SIV, AEPD trebuie să menționeze că o serie de dispoziții ale Convenției actuale au necesitat modificări și actualizare, având în vedere că acestea nu mai respectă actualele cerințe și standarde privind protecția datelor. AEPD profită de această ocazie pentru a sublinia că asigurarea unui înalt nivel de protecție a datelor cu caracter personal și punerea în aplicare mai eficientă a acestuia ar trebui să fie considerate drept o condiție prealabilă esențială pentru îmbunătățirea activității SIV.

21. După câteva observații generale, prezentul aviz urmează să abordeze în principal următoarele chestiuni relevante din punct de vedere al protecției datelor cu caracter personal:

— garanțiile privind protecția datelor în sistem;

— baza de date pentru identificarea dosarelor vamale;

— accesul Eurojust și Europol la sistem (proporționalitatea și necesitatea accesului care urmează să fie acordat acestor organisme);

— modelul de supraveghere pentru SIV în ansamblul său;

— lista autorităților care beneficiază de acces la SIV.

II. **OBSERVAȚII GENERALE**

Coerența dintre părțile din sistem care țin de primul și al treilea pilon

22. După cum s-a menționat în observațiile introductive, AEPD este în special interesată de noile evoluții privind partea din SIV care ține de al treilea pilon, având în vedere că acesta exercită deja sarcini de supraveghere pentru partea centrală din partea care ține de primul pilon, în conformitate cu noul Regulament (CE) nr. 766/2008 al Parlamentului European și al Consiliului [1] în vederea asigurării aplicării corespunzătoare a legislației din domeniile vamal și agricol.

23. În acest context, AEPD dorește să atragă atenția legislatorului asupra faptului că a făcut deja observații cu privire la chestiunile referitoare la supravegherea părții din SIV care ține de primul pilon într-o serie de avize, în special în avizul său din 22 februarie 2007 [2].

24. În avizul respectiv, AEPD a subliniat faptul că „crearea și actualizarea diferitelor instrumente care au ca scop întărirea cooperării comunitare, de exemplu SIV, atrag după sine o creștere a schimbului de informații cu caracter personal care vor fi inițial colectate și schimbate ulterior cu autoritățile administrative ale statelor membre și, în unele cazuri, cu țări terțe. Prelucrarea și comunicarea ulterioară a informațiilor cu caracter personal poate include informații privind implicarea pretinsă sau confirmată a unor persoane fizice în acțiuni contravenționale în domeniul operațiunilor vamale și agricole […]. În continuare, importanța sa este mărită dacă se ia în considerare tipul de date colectate și comunicate, în special suspiciunile privind persoane fizice care au fost implicate în contravenții, respectiv finalitatea și rezultatul prelucrărilor."

Nevoia unei abordări strategice a SIV în ansamblul său

25. AEPD subliniază faptul că, spre deosebire de modificările introduse prin Regulamentul (CE) nr. 766/2008 la instrumentele primului pilon care reglementează SIV, propunerea prevede o revizuire completă a Convenției SIV, care îi oferă legislatorului posibilitatea de a avea o mai bună viziune de ansamblu pentru întregul sistem, pe baza unei abordări coerente și cuprinzătoare.

26. Din punctul de vedere al AEPD, abordarea respectivă trebuie să fie orientată spre viitor. Noile evoluții precum adoptarea Deciziei-cadru 2008/977/JAI și (eventuala) viitoare intrare în vigoare a Tratatului de la Lisabona ar trebui să se reflecte în mod corespunzător și să fie luate în considerare atunci când se ia decizia cu privire la conținutul propriu-zis al propunerii.

27. În ceea ce privește intrarea în vigoare a Tratatului de la Lisabona, AEPD atrage atenția legislatorului asupra nevoii de analiză profundă cu privire la eventualele efecte pe care abolirea structurii pe piloni a UE ar putea să o aibă asupra SIV atunci când Tratatul de la Lisabona intră în vigoare, având în vedere că sistemul se bazează actualmente pe o combinație de instrumente din primul și al treilea pilon. AEPD regretă lipsa de informații explicative cu privire la această importantă evoluție viitoare, care ar afecta în mod semnificativ cadrul juridic care va reglementa SIV pe viitor. Într-un sens mai larg, AEPD formulează o întrebare cu privire la oportunitatea, în cazul în care legislatorul amână revizuirea până la intrarea în vigoare a Tratatului de la Lisabona, a evitării oricăror eventuale incertitudini juridice.

AEPD pledează pentru coerența cu alte sisteme la scară largă

28. Din punctul de vedere al AEPD, înlocuirea Convenției SIV în ansamblul său oferă, de asemenea, o bună oportunitate de a asigura coerența SIV cu alte sisteme și mecanisme care s-au dezvoltat de la adoptarea convenției. În acest sens, AEPD pledează pentru coerență și în privința unui model de supraveghere cu alte instrumente juridice, în special cu cele care instituie Sistemul de Informații Schengen II și Sistemul de Informații privind Vizele.

[1] JO L 218, 13.8.2008, p. 48.

[2] Avizul din 22 februarie 2007 privind propunerea de regulament [COM(2006) 866 final], (JO C 94, 28.4.2007, p. 3).

Raportul cu Decizia-cadru 2008/977/JAI

29. AEPD salută faptul că propunerea ține seama de Decizia-cadru privind protecția datelor cu caracter personal, având în vedere schimbul de date dintre statele membre care se desfășoară în cadrul SIV. Articolul 20 din propunere stipulează clar faptul că Decizia-cadru 2008/977/JAI se aplică protecției schimbului de date în conformitate cu prezenta decizie, sub rezerva unor dispoziții contrare în această decizie. AEPD ia act, de asemenea, de faptul că propunerea face trimitere la decizia-cadru și în partea dispozitivă, de exemplu la articolul 4 alineatul (5), care stipulează că datele enumerate la articolul 6 din Decizia-cadru 2008/977/JAI nu se includ, la articolul 8 privind utilizarea datelor obținute din SIV pentru atingerea obiectivului menționat la articolul 1 alineatul (2) din decizie, la articolul 22 din propunere care vizează drepturile persoanelor în ceea ce privește datele cu caracter personal din SIV și la articolul 29, care se referă la responsabilități și obligații.

30. AEPD consideră că principiile și conceptele instituite de respectiva decizie-cadru sunt potrivite în contextul SIV și prin urmare ar trebui să fie aplicabile atât din motive de securitate juridică, cât și din motive de coerență între regimurile juridice.

31. Acestea fiind menționate, AEPD subliniază, cu toate acestea, faptul că legislatorul ar trebui să prevadă garanțiile necesare că, în așteptarea punerii în aplicare integrale a Deciziei-cadru 2008/977/JAI, în conformitate cu dispozițiile finale ale acesteia, nu va fi detectată nicio lacună în sistemul de protecție a datelor. Cu alte cuvinte, AEPD dorește să sublinieze că este în favoarea abordării în cadrul căreia garanții necesare și adecvate sunt puse în aplicare înainte de desfășurarea unor noi schimburi de date.

III. **OBSERVAȚII SPECIFICE**

Garanții privind protecția datelor

32. AEPD consideră că punerea în aplicare eficientă a dreptului la protecția datelor și dreptul la informare reprezintă elemente esențiale pentru funcționarea adecvată a Sistemului de Informații al Vămilor. Garanțiile privind protecția datelor nu sunt necesare numai pentru a asigura protecția eficientă a persoanelor care fac obiectul SIV, dar ar trebui, de asemenea, să servească la facilitarea unei funcționări adecvate și mai eficiente a sistemului.

33. AEPD atrage de asemenea atenția legislatorului asupra faptului că nevoia de garanții solide și eficiente privind protecția datelor este și mai evidentă atunci când se consideră că SIV este o bază de date întemeiată mai degrabă pe „suspiciuni" decât pe convingeri sau pe alte decizii juridice sau administrative. Această situație este reflectată la articolul 5 din propunere, care stipulează că „datele referitoare la categoriile menționate la articolul 3 se introduc în Sistemul de Informații al Vămilor doar în scopul observării și informării, al supravegherii discrete, al controalelor specifice și al analizei operaționale sau strategice. În sensul acțiunilor propuse (…), datele cu caracter personal (…) pot fi introduse în Sistemul de Informații al Vămilor numai în cazul în care, în special pe baza unor activități ilegale prealabile, există indicii concrete sugerând că persoana respectivă a comis sau că este în curs de a comite ori că va comite infracțiuni grave împotriva legislațiilor naționale." Având în vedere această caracteristică a SIV, propunerea necesită garanții echilibrate, eficiente și actualizate în materie de protecție a datelor cu caracter personal și de mecanisme de control.

34. În ceea ce privește dispozițiile specifice din propunerea privind protecția datelor cu caracter personal, AEPD ia act de eforturile depuse de legislator pentru a furniza mai multe garanții decât cele disponibile în Convenția SIV. Cu toate acestea, AEPD trebuie să mai exprime o serie de preocupări serioase cu privire la dispozițiile referitoare la protecția datelor și în special cu privire la punerea în aplicare a principiului limitării scopului.

35. De asemenea, ar trebui să se menționeze în acest context faptul că observațiile referitoare la garanțiile privind protecția datelor din prezentul aviz nu se limitează numai la dispozițiile care modifică sau extind domeniul de aplicare a Convenției SIV, ci privesc, de asemenea, părți care sunt copiate din actualul text al convenției. Motivul pentru această stare de fapt, după cum se menționează în observațiile generale, este că, din punctul de vedere al AEPD, unele dintre dispozițiile Convenției nu par a mai satisface actualele cerințe privind protecția datelor, iar inițiativa Franței reprezintă o bună oportunitate pentru a avea o nouă perspectivă asupra sistemului în ansamblul său și pentru a asigura nivelul adecvat de protecție a datelor, echivalent celui din partea sistemului care ține de primul pilon.

36. AEPD ia notă cu satisfacție de faptul că numai o listă închisă și completă a datelor cu caracter personal poate fi inclusă în SIV. De asemenea, AEDP salută faptul că propunerea furnizează o definiție mai extinsă a termenului „date cu caracter personal", prin comparație cu Convenția SIV. În conformitate cu articolul 2 alineatul (2) din propunere, termenul „date cu caracter personal" înseamnă orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată"); o persoană identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un număr de identificare sau la unul sau mai mulți factori specifici identității sale fizice, psihologice, psihice, economice, culturale sau sociale.

Limitarea scopului

37. Un exemplu de dispoziții care ridică probleme serioase privind protecția datelor este articolul 8 din propunere, care stipulează că statele membre pot utiliza datele obținute din Sistemul de Informații al Vămilor numai pentru atingerea obiectivului menționat la articolul 1 alineatul (2). Cu toate acestea, statele membre pot să utilizeze respectivele date în scop administrativ sau în alt scop, sub rezerva unei autorizări prealabile și a oricăror condiții impuse de către statul membru care a introdus datele în sistem. O astfel de utilizare în alt scop trebuie să respecte actele cu putere de lege, normele administrative și procedurale ale statului membru care caută să utilizeze datele în conformitate cu articolul 3 alineatul (2) din Decizia-cadru 2008/977/JAI. Această dispoziție privind utilizarea datelor obținute din SIV este esențială pentru structura sistemului și prin urmare necesită o atenție specială.

38. Articolul 8 din propunere face trimitere la articolul 3 alineatul (2) din Decizia-cadru 2008/977/JAI, care abordează „Principii de legalitate, proporționalitate și scop". Articolul 3 din decizia-cadru stipulează următoarele:

„1. Datele cu caracter personal pot fi colectate de autoritățile competente numai în scopuri specifice, explicite și legitime în cadrul sarcinilor lor și pot fi prelucrate doar în scopurile pentru care au fost colectate. Prelucrarea datelor trebuie să fie legală și adecvată, relevantă și să nu fie excesivă în raport cu scopurile pentru care au fost colectate.

2. Prelucrarea suplimentară într-un alt scop este permisă în măsura în care:

(a) este compatibilă cu scopul în care au fost colectate datele;

(b) autoritățile competente sunt autorizate să prelucreze astfel de date în acest alt scop, în conformitate cu dispozițiile legale aplicabile; și

(c) prelucrarea este necesară și proporțională în raport cu acest alt scop."

39. Fără a aduce atingere aplicării articolului 3 alineatul (2) din Decizia-cadru 2008/977/JAI care prevede condițiile generale în care prelucrarea în alt scop poate fi permisă, AEPD atrage atenția asupra faptului că dispozițiile de la articolul 8 din propunere, prin permiterea utilizării datelor din SIV în orice eventual scop administrativ sau în alt scop care nu a fost definit de propunere, ridică problema respectării cerințelor de protecție a datelor, în special a principiului limitării scopului. În plus, instrumentele din primul pilon nu permit o asemenea utilizare generală. Prin urmare, AEPD solicită specificarea scopurilor în care pot fi utilizate datele. Aceasta este de o importanță vitală din perspectiva protecției datelor, deoarece abordează principiile de bază ale utilizării datelor în sistemele la scară largă: „datele ar trebui să fie utilizate numai în scopuri bine definite și clar limitate reglementate de cadrul juridic".

Transferul de date către țări terțe

40. Articolul 8 alineatul (4) din propunere se referă la datele care urmează să fie transferate către țări terțe sau organizații internaționale. Respectiva dispoziție stipulează că, „sub rezerva autorizării prealabile a statului membru care le-a introdus în sistem și a oricăror condiții pe care acesta le-a impus, datele obținute din SIV pot fi transferate (…) unor state terțe, precum și unor organizații internaționale sau regionale care doresc să le utilizeze. Fiecare stat membru ia măsuri speciale pentru a asigura securitatea acestor date atunci când ele sunt transferate către servicii situate în afara teritoriului propriu. Detaliile referitoare la aceste măsuri trebuie să fie transmise autorității comune de control menționate la articolul 25."

41. AEPD ia act de faptul că articolul 11 din Decizia-cadru privind protecția datelor cu caracter personal se aplică în acest context. Cu toate acestea, ar trebui să se sublinieze că, având în vedere caracterul general al aplicării dispozițiilor articolului 8 alineatul (4) din propunere, care în principiu permite statelor membre să transfere datele obținute din SIV unor state terțe, precum și unor organizații internaționale sau regionale care doresc să le utilizeze, garanțiile prevăzute în aceste dispoziții nu sunt nici pe departe suficiente din punct de vedere al protecției datelor cu caracter personal. AEPD solicită o reanalizare a articolului 8 alineatul (4) pentru a se asigura un sistem uniform de evaluare a caracterului adecvării printr-un mecanism potrivit, de exemplu comitetul la care se face trimitere la articolul 26 din propunere ar putea fi implicat într-o astfel de evaluare.

Alte garanții privind protecția datelor

42. AEPD ia act cu satisfacție de dispozițiile privind modificarea datelor (capitolul IV, articolul 13), care constituie un element important al principiului privind calitatea datelor. AEPD salută în special domeniul de aplicare al respectivelor dispoziții, extins și modificat față de Convenția SIV, ceea ce adaugă în momentul de față rectificarea și ștergerea datelor. De exemplu, articolul 13 alineatul (2) stipulează că, în cazul în care un stat membru furnizor sau Europol constată sau sunt atenționate asupra faptului că datele pe care le-au inclus conțin erori de fapt sau că au fost introduse sau că sunt păstrate contrar dispozițiilor prezentei decizii, acesta modifică, completează, rectifică sau șterge aceste date după caz și informează celelalte state membre și Europol cu privire la aceasta.

43. AEPD ia act de dispozițiile capitolului V privind reținerea datelor, care se bazează în principal pe Convenția SIV și, printre altele, prevede termene pentru reținerea datelor copiate din SIV.

44. Capitolul IX (Protecția datelor cu caracter personal) reflectă multe dintre dispozițiile Convenției SIV. Acesta permite, cu toate acestea, modificarea semnificativă reprezentată de aplicarea Deciziei-cadru privind protecția datelor cu caracter personal în cazul SIV și menționarea la articolul 22 din propunere a faptului că „drepturile persoanelor, în ceea ce privește datele cu caracter personal din Sistemul de Informații al Vămilor, în special dreptul de acces, dreptul de a rectifica, de a șterge sau de a bloca date, se exercită în conformitate cu actele cu putere de lege, normele administrative și procedurale ale statului membru care pune în aplicare Decizia-cadru 2008/977/JAI și în care aceste drepturi sunt invocate." În acest context, AEPD dorește să sublinieze în special importanța menținerii procedurii prin care persoanele vizate să își ceară propriile drepturi și să poată solicita accesul în fiecare stat membru. AEPD va analiza cu atenție aspectele practice ale punerii în aplicare a acestui important drept al persoanelor vizate.

45. De asemenea, propunerea extinde domeniul de aplicare a Convenției CIS atunci când este vorba de interzicerea copierii datelor din SIV în alte fișiere de date naționale. Convenția SIV menționează explicit la articolul 14 alineatul (2) că „datele cu caracter personal incluse de alte state membre nu pot fi copiate din SIV în alte fișiere de date naționale". La articolul 21 alineatul (3), propunerea permite „copierea în sistemele de gestionare a riscurilor utilizate pentru a orienta controalele vamale la nivel național sau copierea într-un sistem de analiză operațională care să permită coordonarea acțiunilor". În această privință, AEPD împărtășește părerea exprimată de Autoritatea comună de control al vămilor în Avizul 09/03, în special cu privire la termenul „sisteme de gestionare a riscurilor", precum și la nevoia de a stipula în continuare când și în ce context ar fi posibilă copierea permisă la articolul 21 alineatul (3).

46. AEPD salută dispozițiile privind securitatea, care sunt esențiale pentru funcționarea eficientă a SIV (capitolul XII).

Baza de date pentru identificarea dosarelor vamale

47. Propunerea adaugă dispoziții privind baza de date pentru identificarea dosarelor vamale (articolele 16-19). Aceasta reflectă crearea bazei de date pentru identificarea dosarelor vamale în instrumentul primului pilon. Deși AEPD nu pune sub semnul întrebării necesitatea unor astfel de baze de date noi în cadrul SIV, aceasta atrage atenția asupra necesității unor garanții adecvate privind protecția datelor. În acest context, AEPD salută faptul că excepția prevăzută la articolul 21 alineatul (3) nu se aplică bazelor de date pentru identificarea dosarelor vamale.

Accesul la SIV pentru Europol și Eurojust

48. Propunerea acordă accesul la sistem pentru Oficiul European de Poliție (Europol) și pentru Unitatea Europeană de Cooperare Judiciară (Eurojust).

49. Înainte de toate, AEPD subliniază nevoia de a defini în mod clar scopul accesului și de a evalua proporționalitatea și necesitatea extinderii accesului. Lipsesc informațiile cu privire la motivarea necesității extinderii accesului la sistem pentru Europol și Eurojust. AEPD subliniază, de asemenea, că, atunci când sunt în joc accesul la bazele de date, funcționalitățile și prelucrarea informațiilor cu caracter personal, există o nevoie clară de a evalua în prealabil nu numai utilitatea unui asemenea acces, ci și necesitatea reală și fondată a unei propuneri de acest tip. AEPD subliniază faptul că nu a fost oferită nicio justificare în privința motivelor.

50. AEPD solicită, de asemenea, includerea în text a unei definiții clare a misiunilor exacte pentru care Europol și Eurojust pot garanta accesul la date.

51. Conform articolului 11, „în limitele mandatului său și în scopul îndeplinirii sarcinilor sale, Europol are dreptul de a avea acces la datele introduse în SIV, de a consulta datele în mod direct, de a introduce datele în sistem".

52. AEPD salută limitările introduse în propunere, precum, în special:

— supunerea utilizării informațiilor din SIV consimțământului statului membru care a introdus datele în sistem;

— limitările impuse comunicării de date de către Europol unor țări terțe (din nou, numai cu acordul statului membru care a introdus datele în sistem);

— limitarea accesului la SIV (personal autorizat);

— revizuirea de către organismul comun de control a activităților Europol.

53. De asemenea, AEPD ar dori să menționeze că, de fiecare dată când propunerea face trimitere la Convenția Europol, ar trebui să se țină seama de decizia Consiliului în temeiul căreia, începând cu 1 ianuarie 2010, Europol va deveni agenție a UE.

54. Articolul 12 din propunere abordează chestiunea accesului Eurojust la SIV. Acesta stipulează că „Sub rezerva capitolului IX, membrii și asistenții acestora au dreptul, în limitele mandatului lor și în scopul îndeplinirii sarcinilor lor, de a avea acces la datele introduse în SIV în conformitate cu articolele 1, 3, 4, 5 și 6 și de a le consulta." Propunerea prevede mecanisme privind consimțământul statului membru care a introdus datele, similare cu cele prevăzute pentru Europol. Observațiile anterioare privind nevoia de justificare a necesității de a oferi acces, precum și nevoia de limitări adecvate și necesare în cazul în care este permis accesul se aplică și în cazul Eurojust.

55. AEPD salută limitarea accesului la SIV numai la membrii naționali, la supleanții lor și la asistenții acestora. Cu toate acestea, AEPD ia act de faptul că articolul 12 alineatul (1) se referă numai la membrii naționali și la asistenții acestora, pe când alte alineate de la articolul 12 se referă și la supleanții membrilor naționali. Legislatorii ar trebui să asigure claritatea și coerența în acest context.

Supraveghere – Către un model coerent, constant și cuprinzător

56. În ceea ce privește supravegherea propusă pentru partea din SIV care ține de al treilea pilon, AEPD atrage atenția legislatorului asupra necesității de a asigura o supraveghere constantă și cuprinzătoare a sistemului în ansamblul său. Ar trebui să se țină seama de cadrul juridic complex care reglementează SIV, bazat pe două temeiuri juridice și ar trebui să se evite existența a două modele diferite de supraveghere, din motive de claritate juridică și din rațiuni de ordin practic.

57. După cum s-a menționat anterior în aviz, AEPD acționează în momentul de față în calitate de autoritate de supraveghere a părții centrale din partea sistemului care ține de primul pilon. Această situație este conformă articolului 37 din Regulamentul (CE) nr. 515/97, care stipulează că „Autoritatea Europeană pentru Protecția Datelor controlează conformitatea SIV cu Regulamentul (CE) nr. 45/2001". AEPD ia act de faptul că modelul de supraveghere, astfel cum figurează în propunerea Franței, nu ține seama de acest rol. Modelul de supraveghere se bazează pe rolul autorității comune de control al SIV.

58. Deși apreciază activitățile desfășurate de autoritatea comună de control al SIV, AEPD evidențiază două motive pentru care ar trebui aplicat un model de supraveghere coordonată, conform sarcinilor sale actuale de supraveghere în cadrul altor sisteme la scară largă. În primul rând, un astfel de model ar asigura coerența internă dintre părțile sistemului care țin de primul și al treilea pilon. În al doilea rând, acesta ar asigura coerența cu modelele instituite în cadrul altor sisteme la scară largă. Prin urmare, AEPD recomandă aplicarea pentru SIV, în ansamblul său, a unui model similar celui utilizat în SIS II („supraveghere coordonată" sau „model stratificat"). După cum s-a menționat în avizul AEPD privind partea din SIV care ține de primul pilon, „în cadrul SIS II, legislatorul european a optat pentru o raționalizare a modelului de supraveghere, aplicând modelul stratificat descris mai sus, în ambele medii ale sistemului care țin de primul și cel de-al treilea pilon."

59. AEPD consideră că cea mai potrivită soluție pentru această situație este introducerea unui sistem mai uniform de supraveghere, modelul deja experimentat bazat pe o structură triplă: autoritățile responsabile de protecția datelor la nivel național, AEPD la nivel central și coordonarea dintre cele două. AEPD este convinsă că înlocuirea Convenției SIV oferă oportunitatea unică de simplificare și de mai multă coerență în supraveghere, în completă armonie cu alte sisteme la scară largă (VIS, SIS II, Eurodac).

60. În cele din urmă, modelul de supraveghere coordonată ține seama, de asemenea, în mai mare măsură, de schimbările care vor fi determinate de intrarea în vigoare a Tratatului de la Lisabona și de eliminarea structurii pe piloni a UE.

61. AEPD nu își exprimă punctul de vedere cu privire la eventuala necesitate, determinată de introducerea modelului coordonat de supraveghere, a aplicării unor modificări ale instrumentului primului pilon care reglementează SIV, respectiv Regulamentul (CE) nr. 766/2008, dar AEPD atrage atenția legislatorului asupra nevoii de a analiza acest aspect și din perspectiva coerenței juridice.

Lista autorităților care beneficiază de acces la SIV

62. Articolul 7 alineatul (2) prevede obligația fiecărui stat membru de a trimite celorlalte state membre și comitetului la care se face trimitere la articolul 26 o listă a autorităților competente pe care a elaborat-o pentru a avea acces la SIV, specificând pentru fiecare autoritate datele la care poate avea acces și în ce scop.

63. AEPD atrage atenția asupra faptului că propunerea prevede numai că ar trebui să existe un schimb de informații între statele membre cu privire la autoritățile care au acces la SIV și că statele membre ar trebui să informeze comitetul menționat la articolul 26, însă nu s-a prevăzut publicarea unei asemenea liste a autorităților. Este regretabil întrucât publicarea unui asemenea liste ar ajuta la obținerea unei mai bune transparențe și ar crea un instrument practic pentru o supraveghere eficientă a sistemului, de exemplu de către autoritățile responsabile de protecția datelor.

IV. **CONCLUZII**

64. AEPD sprijină propunerea de decizie a Consiliului privind utilizarea tehnologiei informației în domeniul vamal. AEPD subliniază faptul că, datorită lucrărilor legislative în curs de desfășurare în cadrul Consiliului, observațiile sale nu se bazează pe textul final al propunerii.

65. AEPD regretă lipsa de documente explicative care ar putea oferi clarificarea și informarea necesare cu privire la obiectivele și specificitatea câtorva dintre dispozițiile propunerii.

66. AEPD pledează pentru acordarea unui atenții sporite în cadrul propunerii nevoii de garanții specifice privind protecția datelor. AEPD ia în considerare o serie de chestiuni în cazul cărora ar trebui asigurate mai bine aspectele practice ale punerii în aplicare a garanțiilor privind protecția datelor, în special în ceea ce privește aplicarea limitării scopului în privința utilizării datelor introduse în SIV. AEPD consideră această măsură drept o condiție prealabilă esențială pentru îmbunătățirea funcționării Sistemului de Informații al Vămilor.

67. AEPD pledează pentru includerea în propunere a unui model coordonat de supraveghere. Ar trebui să se ia act de faptul că AEPD are în momentul de față sarcini de supraveghere cu privire la partea din sistem care ține de primul pilon. AEPD subliniază faptul că, din motive de coerență și constanță, cea mai bună abordare este aplicarea modelului de supraveghere coordonată și în cadrul părții din sistem care ține de cel de al treilea pilon. Acest model ar asigura, de asemenea, acolo unde este necesar și adecvat, coerența cu alte instrumente juridice care reglementează instituirea și/sau utilizarea altor sisteme IT la scară largă.

68. AEPD solicită mai multe explicații cu privire la necesitatea și proporționalitatea acordării de acces pentru Eurojust și Europol. AEPD subliniază lipsa de informații explicative cu privire la această chestiune în cadrul propunerii.

69. AEPD insistă, de asemenea, asupra consolidării dispozițiilor de la articolul 8 alineatul (4) din propunere cu privire la transferul de date unor state terțe sau unor organizații internaționale. Aceasta include nevoia de a asigura un sistem uniform de evaluare a caracterului adecvării.

70. AEPD solicită introducerea unei dispoziții privind publicarea listei autorităților care au acces la SIV, pentru a crește transparența și pentru a facilita supravegherea sistemului.

Adoptat la Bruxelles, 20 aprilie 2009.

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor

Avizul Autorității Europene pentru Protecția Datelor privind propunerea de regulament al Parlamentului European și al Consiliului de modificare, în ceea ce privește farmacovigilența medicamentelor de uz uman, a Regulamentului (CE) nr. 726/2004 de stabilire a procedurilor comunitare privind autorizarea și supravegherea medicamentelor de uz uman și veterinar și de instituire a unei Agenții Europene pentru Medicamente și privind propunerea de directivă a Parlamentului European și a Consiliului de modificare, în ceea ce privește farmacovigilența, a Directivei 2001/83/CE de instituire a unui cod comunitar cu privire la medicamentele de uz uman

(2009/C 229/04)

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR,

având în vedere Tratatul de instituire a Comunității Europene, în special articolul 286,

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 [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 [2], în special articolul 41,

A ADOPTAT PREZENTUL AVIZ:

I. INTRODUCERE

Propunerile de modificare a sistemului actual de farmacovigilență

1. La 10 decembrie 2008, Comisia a adoptat două propuneri referitoare la modificarea Regulamentului (CE) nr. 726/2004 și, respectiv, a Directivei 2001/83/CE [3]. Regulamentul (CE) nr. 726/2004 al Parlamentului European și al Consiliului [4] stabilește procedurile comunitare privind autorizarea și supravegherea medicamentelor de uz uman și veterinar și instituie Agenția Europeană pentru Medicamente (denumită în continuare „EMEA"). Directiva 2001/83/CE a Parlamentului European și a Consiliului [5] conține norme privind codul comunitar cu privire la medicamentele de uz uman, în ceea ce privește procedurile specifice la nivelul statelor membre. Modificările propuse se referă la părți din ambele acte, privind farmacovigilența în ceea ce privește medicamentele pentru uz uman.

2. Farmacovigilența se definește ca știința și activitățile referitoare la depistarea, evaluarea, înțelegerea și prevenirea reacțiilor adverse ale medicamentelor [6]. Sistemul de farmacovigilență în vigoare în Europa le permite pacienților și cadrelor medicale să raporteze diverse reacții adverse la medicamente publicului și organismelor private implicate, la nivel național și european. O bază de date europeană (baza de date EudraVigilance) funcționează în cadrul EMEA ca punct de centralizare pentru gestionarea și raportarea reacțiilor adverse suspectate.

3. Farmacovigilența este considerată o adăugire necesară la sistemul comunitar de autorizare a medicamentelor, care datează din 1965, anul adoptării Directivei 65/65/CEE a Consiliului [7].

4. În conformitate cu expunerea de motive și evaluarea impactului, anexate propunerilor, sistemul actual de farmacovigilență are anumite lacune, inclusiv lipsa clarității în ceea ce privește rolurile și responsabilitățile diverselor părți implicate, proceduri complicate de raportare a reacțiilor adverse, necesitatea consolidării transparenței în ceea ce privește siguranța medicamentelor și comunicarea, precum și necesitatea de a raționaliza planificarea gestionării riscurilor în cazul medicamentelor.

5. Intenția generală a celor două propuneri este să remedieze aceste lacune și să îmbunătățească și să consolideze sistemul comunitar de farmacovigilență, scopul principal fiind acela de a asigura o mai bună protecție a sănătății publice, asigurând funcționarea adecvată a pieței interne și simplificând normele și procedurile existente [8].

Datele cu caracter personal în farmacovigilență și consultarea AEPD

6. Funcționarea generală a actualului sistem de farmacovigilență se bazează pe prelucrarea datelor cu caracter personal. Aceste date sunt incluse în rapoartele privind reacțiile adverse la medicamente și pot fi considerate date referitoare la sănătate („date privind sănătatea") ale persoanelor vizate, întrucât prezintă informații privind utilizarea medicamentelor și problemele de sănătate asociate. Prelucrarea acestor date face obiectul unor norme stricte privind protecția datelor, prevăzute în articolul 10 din Regulamentul (CE) nr. 45/2001 și articolul 8 din Directiva 95/46/CE [9]. Importanța protejării acestor date a fost subliniată recent în mod repetat de Curtea Europeană a Drepturilor Omului în contextul

[1] JO L 281, 23.11.1995, p. 31.
[2] JO L 8, 12.1.2001, p. 1.
[3] COM(2008) 664 final și COM(2008) 665 final.
[4] JO L 136, 30.4.2004, p. 1.
[5] JO L 311, 28.11.2001, p. 67.
[6] A se vedea expunerea de motive la ambele propuneri, de la pagina 3.
[7] JO 22, 9.2.1965, p. 369.
[8] A se vedea expunerea de motive de la pagina 2.
[9] A se vedea Avizul AEPD din 2 decembrie 2008 privind propunerea de directivă privind drepturile pacienților în cadrul asistenței medicale transfrontaliere, punctele 15-17, disponibil la adresa http://www.edps.europa.eu, în ceea ce privește definiția datelor privind sănătatea.

articolului 8 din Convenția Europeană a Drepturilor Omului: „Protecția datelor cu caracter personal, în special a datelor medicale, este de o deosebită importanță pentru ca o persoană să beneficieze de dreptul său de respectare a vieții private și a vieții de familie, astfel cum este garantat la articolul 8 din convenție" ([10]).

7. Cu toate acestea, nu se face nicio trimitere la protecția datelor în actualul text al Regulamentului (CE) nr. 726/2004 și al Directivei 2001/83/CE, cu excepția unei trimiteri specifice în regulament, care va fi discutată la punctele 21 și următoarele.

8. Autoritatea Europeană pentru Protecția Datelor (AEPD) regretă că aspectele privind protecția datelor nu au fost luate în considerare în modificările propuse și că nu a fost consultată în mod oficial cu privire la ambele propuneri de modificare, conform articolului 28 alineatul (2) din Regulamentul (CE) nr. 45/2001. Avizul de față se întemeiază pe articolul 41 alineatul (2) din același regulament. AEPD recomandă includerea unei trimiteri la prezentul aviz în preambulul ambelor propuneri.

9. AEPD constată că, deși protecția datelor nu este luată în considerare în mod suficient în cadrul juridic actual privind farmacovigilența și în propuneri, aplicarea practică a sistemului comunitar central EudraVigilance este problematică din perspectiva protecției datelor. În acest sens, EMEA a notificat sistemul actual EudraVigilance către AEPD în iunie 2008, privind o verificare prealabilă în baza articolului 27 din Regulamentul (CE) nr. 45/2001.

10. Prezentul aviz și concluziile AEPD privind verificarea prealabilă (publicare prevăzută în cursul acestui an) se vor suprapune parțial. Cu toate acestea, obiectivul celor două acte este diferit: prezentul aviz se concentrează pe cadrul juridic general care sprijină sistemul, astfel cum decurge din Regulamentul (CE) nr. 726/2004 și Directiva 2001/83/CE și modificările propuse, iar verificarea prealabilă conține o analiză detaliată cu privire la protecția datelor, care se concentrează pe modul de elaborare ulterioară a normelor actuale în acte ulterioare (de exemplu decizii și orientări), eliberate de EMEA sau de Comisie și de EMEA împreună, și pe modul de funcționare în practică a bazei de date EudraVigilance.

11. Pentru început, prezentul aviz va explica, simplificat, sistemul de farmacovigilență european, astfel cum decurge din Regulamentul (CE) nr. 726/2004 și Directiva 2001/83/CE în stadiul actual. Ulterior, se va analiza necesitatea prelucrării datelor cu caracter personal în contextul farmacovigilenței. În final, se vor discuta propunerile Comisiei de îmbunătățire a cadrului juridic actual și a celui avut în vedere, și se vor face recomandări cu privire la asigurarea și îmbunătățirea normelor de protecție a datelor.

([10]) A se vedea CEDO 17 iulie 2008, I v. Finlanda (nr. cererii 20511/03), punctul 38 și CEDO 25 noiembrie 2008, Armonas v. Lihuania (nr. cererii 36919/02), punctul 40.

II. SISTEMUL DE FARMACOVIGILENȚĂ AL UE: PRELUCRAREA DATELOR CU CARACTER PERSONAL ȘI CONSIDERENTE PRIVIND PROTECȚIA DATELOR

Părțile implicate în colectarea și diseminarea informațiilor

12. Mai multe părți sunt implicate în colectarea și difuzarea informațiilor privind efectele adverse ale medicamentelor în Uniunea Europeană. La nivel național, cele două părți importante sunt titularii de autorizații de introducere pe piață (societăți autorizate să comercializeze medicamente) și autoritățile naționale competente (autoritățile răspunzătoare de autorizarea de introducere pe piață). Autoritățile naționale competente autorizează produsele prin proceduri naționale, care includ „procedura de recunoaștere reciprocă" și „procedura descentralizată" ([11]). Comisia Europeană poate, de asemenea, deveni autoritate competentă pentru produsele autorizate prin așa-numita „procedură centralizată". O parte importantă la nivel european este EMEA. Una dintre sarcinile acestei agenții este asigurarea difuzării informațiilor privind reacțiile adverse ale medicamentelor autorizate în Comunitate, prin intermediul unei baze de date, baza de date menționată anterior, EudraVigilance.

Colectarea și stocarea datelor cu caracter personal la nivel național

13. Directiva 2001/83/CE vorbește în termeni generali despre responsabilitatea statelor membre de a opera un sistem de farmacovigilență în care să fie colectate informații „utile în supravegherea medicamentelor" (articolul 102). În baza articolelor 103 și 104 din Directiva 2001/83/CE [a se vedea și articolele 23 și 24 din Regulamentul (CE) nr. 726/2004], titularii de autorizații de introducere pe piață trebuie să dețină propriile sisteme de farmacovigilență pentru a-și asuma responsabilitatea pentru produsele de pe piață și pentru a asigura luarea de acțiuni corespunzătoare, după caz. Informațiile sunt colectate direct de la cadrele medicale sau de la pacienți. Titularul de autorizație de introducere pe piață trebuie să raporteze electronic autorității competente toate informațiile relevante pentru raportul beneficii/riscuri cu privire la un anumit medicament.

14. Directiva 2001/83/CE nu e foarte clară în privința tipului de informații referitoare la efecte adverse care ar trebui colectate la nivel național, modalităților de stocare sau de comunicare. Articolele 104 și 106 se referă numai la „rapoartele" care trebuie elaborate. Norme mai detaliate privind aceste rapoarte se regăsesc în orientările elaborate de Comisie, după consultarea EMEA, a statelor membre și a părților interesate, în baza articolului 106. În Orientările privind farmacovigilența în ceea ce privește medicamentele

([11]) A se vedea evaluarea impactului, de la pagina 10.

de uz uman (în continuare „orientările"), se face referire la așa-numitele „Rapoarte de siguranță individuale de caz" (în continuare „ICSR"), rapoarte privind efectele adverse ale medicamentelor cu privire la un anumit pacient ([12]). Conform orientărilor, un element minim necesar de informație pentru crearea unui ICSR este „un pacient identificabil" ([13]). Se prevede că pacientul poate fi identificat prin inițiale, numărul de pacient, data nașterii, greutatea, înălțimea și sexul, numărul de înregistrare în spital, informații privind antecedentele medicale ale pacientului, informații privind părinții pacientului ([14]).

15. Prin sublinierea posibilității de identificare a pacientului, prelucrarea informației cade în mod clar sub incidența normelor privind protecția datelor, astfel cum sunt prevăzute în Directiva 95/46/CE. Într-adevăr, deși numele pacientului nu este menționat, prin corelarea tuturor informațiilor disponibile (de exemplu, spital, data nașterii, inițiale) și în condiții specifice (de exemplu, în comunități închise sau spații reduse), este posibilă identificarea acestuia. Astfel, informația prelucrată în contextul farmacovigilenței ar trebui, în principiu, considerată ca referindu-se la o persoană fizică identificabilă în sensul articolului 2 litera (a) din Directiva 95/46/CE ([15]). Deși nu se clarifică nici în regulament nici în directivă, această chestiune se regăsește în orientări, unde se prevede că „informația ar trebui să fie cât mai completă cu putință, luând în considerare legislația UE privind protecția datelor" ([16]).

16. Trebuie subliniat că, în ciuda orientărilor, raportarea efectelor adverse la nivel național este departe de a fi uniformă. Această chestiune va fi aprofundată la punctele 24 și 25 de mai jos.

Baza de date EudraVigilance

17. Baza de date EudraVigilance, operată de EMEA, joacă un rol esențial în sistemul european de farmacovigilență. După cum am menționat, EudraVigilance este un sistem centralizat de prelucrare a datelor în rețea și de gestiune, utilizat pentru raportarea și evaluarea presupuselor reacțiilor adverse pe durata producerii de medicamente și după eliberarea de autorizații de comercializare a acestora în comunitate și în țările care fac parte din Spațiul Economic European. Temeiul juridic pentru baza de date EudraVigilance este articolul 57 alineatul (1) litera (d) din Regulamentul (CE) nr. 726/2004.

18. Actuala bază de date EudraVigilance este formată din două compartimente, (1) informația provenită din teste clinice (care au loc înainte de comercializarea medicamentului, numită și perioada de „preautorizare") și (2) informația provenită din rapoarte cu privire la efectele adverse (colectate ulterior, numită și perioada „postautorizare"). Prezentul aviz se concentrează pe perioada „postautorizare", întrucât modificările propuse se concentrează pe aceasta.

19. Baza de date EudraVigilance cuprinde date privind pacienți, obținute pe baza ICSR. EMEA primește ICSR de la autoritățile naționale competente [a se vedea articolul 102 din Directiva 2001/83/CE și articolul 22 din Regulamentul (CE) nr. 726/2004] și în unele cazuri direct de la titularii de autorizații de introducere pe piață [a se vedea articolul 104 din Directiva 2001/83/CE și articolul 24 din Regulamentul (CE) nr. 726/2004].

20. Prezentul aviz se concentrează pe prelucrarea datelor cu caracter personal privind pacienții. Trebuie subliniat, totuși, că baza de date EudraVigilance cuprinde informații cu caracter personal care se referă și la persoanele care lucrează pentru autoritățile naționale competente sau titularii autorizațiilor de introducere pe piață, dacă transmit informații bazei de date. Sistemul păstrează numele complet, adresa, datele de contact, detalii din documentele de identificare ale acestor persoane. O altă categorie de informații cu caracter personal o reprezintă datele referitoare la așa-numitele persoane calificate răspunzătoare de farmacovigilență, numite de titularii de autorizații de introducere pe piață în conformitate cu articolul 103 din Directiva 2001/83/CE. Evident, drepturile și obligațiile prevăzute în Regulamentul (CE) nr. 45/2001 se aplică în totalitate prelucrării acestor informații.

Accesul la baza de date EudraVigilance

21. Articolul 57 alineatul (1) litera (d) din Regulamentul (CE) nr. 726/2004 prevede că baza de date ar trebui să fie accesibilă în permanență tuturor statelor membre. Cadrele medicale, titularii autorizațiilor de introducere pe piață și publicul trebuie, deci, să dispună de niveluri de acces adecvate la această bază de date, protecția datelor cu caracter personal fiind garantată. După cum s-a menționat la punctul 7, aceasta este singura dispoziție din regulament și din Directiva 2001/83/CE care face trimitere la protecția datelor.

22. Articolul 57 alineatul (1) litera (d) a condus la următorul regim de acces. În momentul primirii de către EMEA a unui ICSR, aceasta îl transmite direct portalului EudraVigilance, accesibil de către EMEA, autoritățile naționale competente și Comisie. După validarea ICSR (verificarea autenticității și a unicității) de către EMEA, informația din ICSR este transmisă bazei de date propriu-zise. EMEA, autoritățile naționale competente și Comisia au drepturi depline de acces la baza de date, iar titularii de autorizații de

([12]) A se vedea volumul 9A din Regulamentul medicamentelor în Uniunea Europeană: Orientări privind farmacovigilența în ceea ce privește medicamentele de uz uman, la adresa: http://ec.europa.eu/enterprise/pharmaceuticals/eudralex/vol-9/pdf/vol9a_09-2008.pdf

([13]) A se vedea orientările de la pagina 57.

([14]) A se vedea nota de subsol nr. 13.

([15]) Articolul 2 alineatul (a) din Directiva 95/46/CE definește „datele cu caracter personal" ca fiind „orice informație cu referire la o persoană fizică identificată sau identificabilă (persoana vizată)"; o persoană identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un număr de identificare sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, psihice, economice, culturale sau sociale". Considerentul (26) specifică: „[...] pentru a determina dacă o persoană este identificabilă este oportun să se ia în considerare toate mijloacele care pot fi utilizate în mod rezonabil fie de operator, fie de orice altă persoană pentru a identifica persoana vizată. Pentru o analiză aprofundată, a se vedea Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, Avizul nr. 4/2007 privind conceptul datelor cu caracter personal (documentul GL 136), adoptat la 20 iunie 2007, disponibil la adresa http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm Cele de mai sus sunt valabile și pentru Regulamentul (CE) nr. 45/2001.

([16]) A se vedea nota de subsol nr. 13.

introducere pe piață au acces la baza de date numai în anumite condiții, și anume numai la datele pe care le-au transmis ei înșiși EMEA. Informațiile cumulate despre ICSR sunt ulterior afișate pe site-ul internet EudraVigilance, accesibil publicului larg, inclusiv cadrelor medicale.

23. La 19 decembrie 2008, EMEA a publicat un proiect de politică de acces pe site-ul propriu, pentru consultare publică ([17]). Documentul arată cum intenționează EMEA să pună în aplicare articolul 57 alineatul (1) litera (d) din Regulamentul (CE) nr. 726/2004. AEPD va aborda din nou acest subiect începând cu punctul 48.

Slăbiciunile sistemului actual și lipsa garanțiilor de protecție a datelor

24. Evaluarea de impact a Comisiei demonstrează o serie de slăbiciuni ale sistemului actual de farmacovigilență al UE, considerat complex și neclar. Sistemul complicat de colectare, stocare și schimb de date între diversele părți la nivel național și european este considerat una dintre principalele lacune. Situația este complicată și de faptul că există disparități între modalitățile de punere în aplicare a Directivei 2001/83/CE în statele membre ([18]). O consecință este faptul că autoritățile naționale competente și EMEA sunt confruntate frecvent cu rapoarte de cazuri de reacții adverse incomplete sau în duplicat ([19]).

25. Aceasta se datorează faptului că, deși orientările sus-menționate conțin o descriere a conținutului ICSR, statele membre decid modalitățile de punere în aplicare la nivel național. Aceasta include atât mijloacele de comunicare utilizate pentru raportarea de către titularii autorizației de introducere pe piață către autoritățile naționale competente, cât și informația efectivă cuprinsă în rapoarte (nu se folosește un formular model pentru raportare în Europa). De asemenea, unele autorități naționale competente pot aplica criterii calitative specifice pentru admisibilitatea rapoartelor (în funcție de conținut, de gradul de completare etc.), în vreme ce în alte state aceste criterii nu s-ar aplica. Este evident că abordarea la nivel național privind raportarea și evaluarea calității ICSR are un impact direct asupra modului de raportare ulterioară către EMEA, prin baza de date EudraVigilance.

26. AEPD ar dori să sublinieze că slăbiciunile sus-menționate nu au ca rezultat numai inconveniente practice, dar reprezintă un pericol considerabil la adresa protecției datelor cu privire la sănătate ale cetățenilor. Deși, după cum am arătat în alineatele anterioare, prelucrarea datelor cu privire la sănătate are loc în etape diferite ale procesului de farmacovigilență, nu există în prezent dispoziții privind protecția acestor date. Singura excepție este trimiterea generală la protecția datelor din articolul 57 alineatul (1) litera (d) din Regulamentul (CE) nr. 726/2004, care nu se referă decât la ultima etapă a prelucrării datelor, și anume la accesibilitatea datelor cuprinse în baza de date EudraVigilance. Mai mult, lipsa clarității cu privire la rolurile și responsabilităților diverselor părți implicate în prelucrare, precum și lipsa de norme specifice de prelucrare este o amenințare la adresa confidențialității, a integrității și responsabilității datelor personale prelucrate.

27. Prin urmare, AEPD dorește să sublinieze că absența unei analize cuprinzătoare privind protecția datelor, reflectată în cadrul juridic care stă la baza sistemului de farmacovigilență în UE, trebuie văzută ca o slăbiciune a actualului sistem. Această slăbiciune ar trebui remediată prin modificarea legislației actuale.

III. FARMACOVIGILENȚA ȘI NECESITATEA DATELOR CU CARACTER PERSONAL

28. Ca preocupare preliminară și generală, AEPD dorește să ridice problema necesității efective a prelucrării datelor privind sănătatea ale persoanelor fizice identificabile în toate etapele sistemului de farmacovigilență (la nivel național și european).

29. După cum am explicat anterior, în ICSR pacientul nu este menționat cu numele și nu este identificat ca atare. Cu toate acestea, pacientul poate fi identificat în anumite cazuri, prin combinarea informațiilor disparate din ICSR. Conform orientărilor, în unele cazuri, se acordă un număr specific pentru fiecare pacient, ceea ce presupune că sistemul, în întregul său, permite trasabilitatea persoanei implicate. Cu toate acestea, nici directiva, nici regulamentul nu fac trimitere la trasabilitatea persoanelor ca parte a obiectivului sistemului de farmacovigilență.

30. AEPD invită, astfel, legiuitorul să clarifice dacă se dorește ca trasabilitatea să servească drept obiectiv al farmacovigilenței în diferitele etape ale prelucrării și în mod special în cadrul bazei de date EudraVigilance.

31. În acest sens, este utilă o comparare cu regimul propus privind donarea și transplantul de organe ([20]). În contextul transplantului de organe, trasabilitatea unui organ către donator, precum și către beneficiarul organului, este de o deosebită importanță, în special în cazul unor evenimente sau reacții adverse grave.

([17]) A se vedea proiectul EudraVigilance privind politicile de acces pentru medicamentele de uz uman, din 19 decembrie 2008, la adresa http://www.emea.europa.eu/pdfs/human/phv/18743906en.pdf

([18]) A se vedea evaluarea impactului de la pagina 17.

([19]) A se vedea nota de subsol nr. 18.

([20]) A se vedea propunerea Comisiei de directivă a Parlamentului European și a Consiliului privind standardele de calitate și siguranță referitoare la organele umane destinate transplantului, COM(2008) 818 final. A se vedea Avizul AEPD din 5 martie 2009, la adresa http://www.edps.europa.eu

32. Cu toate acestea, în contextul farmacovigilenței, AEPD nu are dovezi suficiente pentru a concluziona că trasabilitatea este efectiv necesară în orice moment. Farmacovigilența se referă la raportarea efectelor adverse ale medicamentelor utilizate de un număr (în cea mai mare parte) necunoscut de oameni și care vor fi utilizate de un număr (în cea mai mare parte) necunoscut de oameni. Există, deci, – cel puțin în perioada „postautorizare" – o legătură mai puțin automată și individuală între informațiile privind efectele adverse și persoana vizată, ca în cazul informației privind organele și persoanele implicate în transplantului unui organ specific. Este evident că pacienții care au utilizat un anumit medicament și care au raportat efecte adverse au interesul să cunoască rezultatul oricărei evaluări ulterioare. Aceasta nu înseamnă că informațiile raportate ar trebui în fiecare caz conectate la persoana specifică prin întregul proces de farmacovigilență. În multe cazuri ar trebui să fie suficientă conectarea informației privind efectele adverse la medicamentul în sine, ceea ce permite părților implicate, probabil prin intermediul cadrelor medicale, să informeze pacienții în general cu privire la consecințele luării unui anumit medicament.

33. Dacă se dorește, totuși, asigurarea trasabilității, AEPD reamintește analiza pe care a realizat-o în avizul privind propunerea Comisiei de directivă privind standardele de calitate și siguranță referitoare la organele umane destinate transplantului. În acel aviz, a explicat relația dintre trasabilitate, identificabilitate, anonimitate și confidențialitate a datelor. Identificabilitatea este un termen crucial în legislația privind protecția datelor ([21]). Normele privind protecția datelor se aplică datelor referitoare la persoane care sunt identificate sau identificabile ([22]). Trasabilitatea datelor către o anumită persoană se substituie identificabilității. În legislația privind protecția datelor, anonimitatea este antonimul identificabilității și, deci, al trasabilității. Datele sunt considerate anonime numai dacă este imposibilă identificarea persoanei (sau traseul către persoana) la care se referă datele. Noțiunea de „anonimitate" este diferită de cum o înțelegem în viața de zi cu zi, adică o persoană nu poate fi identificată din aceste date, ca atare, pentru că, de exemplu, numele său a fost șters. În aceste situații, ne referim mai degrabă la confidențialitatea datelor, adică informația este accesibilă (în totalitate) numai celor autorizați să aibă acces. Cu toate că trasabilitatea și anonimitatea nu pot coexista, trasabilitatea și confidențialitatea pot.

34. Pe lângă trasabilitate, un alt motiv pentru identificabilitatea pacienților pe durata întregului proces de farmacovigilență ar putea fi buna funcționare a sistemului. AEPD înțelege că, atunci când informația se referă la o persoană identificabilă și, deci, unică, este mai ușor pentru autoritățile competente relevante (adică autoritățile naționale competente și EMEA) să monitorizeze și să controleze conținutul unui ICSR (să verifice duplicate). Deși AEPD înțelege necesitatea unui astfel de mecanism de control, nu este convinsă că simpla necesitate ar putea justifica identificabilitatea datelor în toate etapele procesului de farmacovigilență și în special în baza de date EudraVigilance. Printr-o mai bună structurare și coordonare a sistemului de raportare, de exemplu printr-un sistem descentralizat, astfel cum se discută mai jos, la punctul 42 și următoarele, duplicarea s-ar putea evita încă de la nivelul național.

35. AEPD recunoaște că, în circumstanțe deosebite, este imposibil să se asigure anonimitatea datelor. Este, de exemplu, cazul unor medicamente utilizate de un grup foarte limitat de persoane. În aceste cazuri specifice, ar trebui elaborate garanții speciale de protecție pentru a corespunde obligațiilor consacrate în legislația privind protecția datelor.

36. În concluzie, AEPD are dubii serioase cu privire la necesitatea, în toate etapele procesului de farmacovigilență, a trasabilității sau utilizării datelor privind pacienți care pot fi identificați. AEPD este conștientă de faptul că nu poate fi posibilă excluderea prelucrării datelor care pot fi identificate în fiecare etapă, în special la nivel național, unde colectarea efectivă de informații privind efectele adverse are loc. Cu toate acestea, normele privind protecția datelor prevăd că prelucrarea datelor privind sănătatea să aibă loc numai atunci când este strict necesar. Utilizarea de date care pot fi identificate ar trebui, deci, redusă la minimum și interzisă sau oprită în stadiu incipient, după posibilități, în cazurile în care nu este considerată necesară. Prin urmare, AEPD invită legiuitorul să reevalueze necesitatea utilizării acestor informații la nivel european și național.

37. Se observă că, în cazurile în care există o nevoie reală de prelucrare a datelor care pot fi identificate sau atunci când nu se poate asigura anonimitatea acestora (a se vedea punctul 35 de mai sus), ar trebui explorate posibilitățile tehnice de identificare indirectă a persoanelor vizate, de exemplu prin pseudonime ([23]).

38. Prin urmare, AEPD recomandă introducerea, în Regulamentul (CE) nr. 726/2004 și în Directiva 2001/83/CE a unui nou articol care să prevadă că dispozițiile din Regulamentul (CE) nr. 726/2004 și din Directiva 2001/83/CE nu aduc atingere drepturilor și obligațiilor ce decurg din dispozițiile Regulamentului (CE) nr. 45/2001 și Directivei 95/46/CE, cu trimitere specifică la articolul 10 al Regulamentului (CE) nr. 45/2001 și la articolul 8 al Directivei 95/46/CE. Ar mai trebui adăugat și faptul că datele

([21]) A se vedea Avizul AEPD, punctele 11-28.

([22]) A se vedea articolul 2 alineatul (a) din Directiva 95/46/CE și articolul 3 alineatul (a) din Regulamentul (CE) nr. 45/2001, precum și explicația de la nota de subsol 13.

([23]) Adoptarea unui pseudonim este un proces la care se poate recurge pentru a ascunde identitatea persoanei vizate, putând totuși identifica datele. Există diverse posibilități tehnice, de exemplu păstrarea în siguranță a listelor de corespondență dintre identitatea reală și pseudonim, utilizarea de algoritmi criptografici bidirecționali etc.

privind sănătatea care pot fi identificate vor fi prelucrate numai dacă este strict necesar, iar părțile implicate ar trebui să evalueze această necesitate în toate etapele procesului de farmacovigilență.

IV. **ANALIZA DETALIATĂ A PROPUNERII**

39. Cu toate că protecția datelor nu este luată în considerare în modificările propuse, o analiză mai detaliată a propunerii este utilă deoarece arată că unele dintre modificările avute în vedere cresc impactul și riscurile ulterioare în ceea ce privește protecția datelor.

40. Intenția generală a celor două propuneri este să îmbunătățească consecvența cu normele, să clarifice responsabilitățile, să simplifice sistemul de reportare și să consolideze baza de date EudraVigilance ([24]).

Clarificarea responsabilităților

41. Comisia a încercat în mod evident să clarifice responsabilitățile, propunând modificarea dispozițiilor actuale, astfel încât legislația să indice mai explicit care sunt responsabilitățile fiecărei părți. Bineînțeles, clarificarea misiunilor fiecărei părți și a obligațiilor acestora referitoare la raportarea efectelor adverse mărește transparența sistemului și, prin urmare, din punctul de vedere al protecției datelor, reprezintă o evoluție pozitivă. În termeni generali, pacienții ar trebui să poată înțelege, din legislație, cum, când și de către cine le sunt prelucrate datele cu caracter personal. Cu toate acestea, clarificarea propusă a sarcinilor și responsabilităților ar trebui să fie legată în mod explicit de cele consacrate în legislația privind protecția datelor.

Simplificarea procesului de raportare

42. Simplificarea sistemului de raportare ar trebui să se realizeze prin utilizarea de portaluri web naționale privind siguranța medicamentelor, conectate la portalul web european privind siguranța medicamentelor [a se vedea noul articol propus 106 din Directiva 2001/83/CE, precum și articolul 26 din Regulamentul (CE) nr. 726/2004]. Portalurile web naționale vor cuprinde formulare publice pentru raportarea reacțiilor adverse suspectate de către cadrele medicale și pacienți [a se vedea noul articol propus 106 alineatul (3) din Directiva 2001/83/CE, precum și articolul 25 din Regulamentul (CE) nr. 726/2004]. De asemenea, portalul web european va cuprinde informații privind metodele de raportare, inclusiv modele de formular pentru raportarea online de către pacienți și cadrele medicale.

43. AEPD dorește să sublinieze că, deși utilizarea acestor portaluri web și a modelelor de formular va crește eficacitatea sistemului de raportare, concomitent, vor crește riscurile la adresa protecției datelor în cadrul sistemului. AEPD invită legiuitorul să alinieze evoluția acestui sistem de raportare la dispozițiile legislației privind protecția datelor. Aceasta presupune, după cum s-a menționat, că necesitatea prelucrării datelor cu caracter personal ar trebui evaluată în mod corespunzător, în ceea ce privește fiecare etapă a procesului. Aceasta ar trebui să se reflecte în organizarea raportării la nivel național și în transmiterea informațiilor către EMEA și baza de date EudraVigilance. Într-un sens mai larg, AEPD recomandă cu fermitate elaborarea de formulare uniforme la nivel național, care ar preveni practicile divergente care dau naștere unor niveluri diferite de protecție a datelor.

44. Sistemul avut în vedere pare să presupună că pacienții pot raporta direct EMEA sau, poate, direct bazei de date EudraVigilance. Acest lucru ar însemna că, prin aplicația actuală a bazei de date EudraVigilance, informația va fi introdusă în portalul EMEA, după cum s-a explicat la punctele 21-22 de mai sus și va fi accesibilă Comisiei și autorităților naționale competente.

45. În general, AEPD sprijină cu fermitate un sistem descentralizat de raportare. Comunicarea către portalul european ar trebui coordonată prin utilizarea portalurilor naționale, care sunt în răspunderea autorităților naționale competente. Ar trebui să se recurgă la raportarea indirectă de către pacienți, adică prin intermediul cadrelor medicale (prin portal sau altfel) și nu la raportarea directă de către pacienți, îndeosebi către baza de date EudraVigilance.

46. În orice caz, orice sistem de raportare prin portal web presupune norme stricte de securitate. În acest sens, AEPD ar dori să reamintească trimiterea la Avizul privind propunerea de directivă privind drepturile pacienților în cadrul asistenței medicale transfrontaliere, în special partea privind securitatea datelor din statele membre și protecția vieții private în aplicațiile e-sănătate ([25]). În acel aviz, AEPD a subliniat deja că viața privată și securitatea ar trebui să facă parte din concepția și punerea în aplicare a oricărei aplicații e-sănătate [principiul „viață privată prin concepție" (privacy by design)] ([26]). Același considerent se aplică portalurilor web avute în vedere.

47. Prin urmare, AEPD recomandă includerea în noile articole 25 și 26 din Regulamentul (CE) nr. 726/2004 și în articolul 106 din Directiva 2001/83/CE, care se referă la elaborarea unui sistem de raportare a efectelor adverse prin utilizarea de portaluri web, a unei obligații de incorporare a măsurilor adecvate privind protecția vieții private și securitatea. Principiile confidențialității , integrității, responsabilizării și disponibilității datelor ar putea fi menționate ca principale obiective de securitate, care ar trebui garantate la același nivel în toate statele membre. Utilizarea de norme și

([24]) A se vedea expunerea de motive de la paginile 2-3.

([25]) A se vedea Avizul AEPD menționat la nota de subsol 7 la propunerea de directivă privind drepturile pacienților în cadrul asistenței medicale transfrontaliere, punctele 32-34.

([26]) A se vedea punctul 32 din aviz.

mijloace tehnice adecvate, cum ar fi criptarea și autentificarea digitală a semnăturii, ar putea fi incluse.

Consolidarea bazei de date EudraVigilance: îmbunătățirea accesului

48. Noul articol 24 din Regulamentul (CE) nr. 726/2004 se referă la baza de date EudraVigilance. Articolul clarifică faptul că orice consolidare a bazei de date presupune o utilizare intensificată a bazei de date de către diversele părți implicate, în ceea ce privește furnizarea și accesarea informației în și din baza de date. Două alineate ale articolului 24 sunt importante în acest sens.

49. Alineatul (2) al articolului 24 se referă la accesibilitatea bazei de date. Acesta înlocuiește articolul 57 alineatul (1) litera (d) din Regulamentul (CE) nr. 726/2004, discutat anterior ca unică dispoziție actuală referitoare la protecția datelor. Trimiterea la protecția datelor este păstrată, dar numărul părților care îi fac obiectul a fost redus. Acolo unde textul actual prevede că se vor acorda niveluri corespunzătoare de acces la baza de date cadrelor medicale, titularilor de autorizații de introducere pe piață și publicului, datele cu caracter personal fiind protejate, Comisia propune în prezent eliminarea titularilor de autorizații menționați anterior de pe listă și acordarea de acces acestora „în măsura în care este necesar pentru ca ei să respecte obligațiile privind farmacovigilența", fără nicio mențiune la protecția datelor. Motivele nu sunt clare.

50. Al treilea alineat al articolului 24 prevede normele privind accesul la ICSR. Publicul poate solicita accesul, care poate fi acordat în termen de 90 de zile, „cu excepția cazului în care transmiterea datelor confidențiale ar putea compromite anonimatul persoanelor care fac obiectul rapoartelor". AEPD sprijină ideea care a stat la baza acestei dispoziții, și anume că numai datele anonime pot fi făcute publice. Cu toate acestea, AEPD dorește să sublinieze, după cum s-a mai explicat, că anonimitatea trebuie înțeleasă ca fiind deplina imposibilitate de a identifica persoana care a raportat efectul advers (a se vedea și punctul 33).

51. Accesibilitatea sistemului EudraVigilance ar trebui, în general, să fie reevaluată în lumina normelor privind protecția datelor. Acest lucru afectează direct elaborarea politicilor de acces publicate de EMEA în decembrie 2008, menționate la punctul 23 de mai sus ([27]). În cazul în care informațiile din baza de date EudraVigilance se referă în mod necesar la persoane fizice care pot fi identificate, accesul la acele date trebuie să fie cât mai restrictiv posibil.

52. AEPD recomandă, în consecință, includerea în articolul 24 alineatul (2) propus din Regulamentul (CE) nr. 726/2004 a unei teze potrivit căreia accesibilitatea bazei de date EudraVigilance va fi reglementată conform drepturilor și obligațiilor ce decurg din legislația comunitară în materie de protecție a datelor.

Drepturile persoanelor vizate

53. AEPD dorește să sublinieze că, din momentul prelucrării datelor care pot fi identificate, partea responsabilă de prelucrare trebuie să se conformeze tuturor cerințelor legislației comunitare în materie de protecție a datelor. Aceasta presupune, *inter alia*, că persoana implicată este bine informată cu privire la utilizarea datelor și la entitatea care le va prelucra și cu privire la orice informații suplimentare necesare potrivit articolului 11 din Regulamentul (CE) nr. 45/2001 și/sau articolul 10 din Directiva 95/46/CE. Persoana în cauză ar trebui, deci, să-și poată invoca drepturile la nivel național și european, cum ar fi dreptul la acces [articolul 12 din Directiva 95/46/CE și articolul 13 din Regulamentul (CE) nr. 45/2001], dreptul la opoziție [articolul 18 din Regulamentul (CE) nr. 45/2001 și articolul 14 din Directiva 95/46/CE] etc.

54. Prin urmare, AEPD recomandă adăugarea unui alineat la articolul 101 propus din Directiva 2001/83/CE conform căruia, în cazul prelucrării datelor cu caracter personal, persoana va fi informată în mod corespunzător conform articolului 10 din Directiva 95/46/CE.

55. Accesul la informațiile proprii ale unei persoane, informații cuprinse în baza de date EudraVigilance, nu este abordat în legislația actuală și propusă. Trebuie subliniat că, în cazurile în care se consideră necesară stocarea de date cu caracter personal în baza de date, așa cum am menționat, pacientul în cauză ar trebui să aibă dreptul să invoce dreptul său de acces la datele cu caracter personal care îl vizează în conformitate cu articolul 13 din Regulamentul (CE) nr. 45/2001. Prin urmare, AEPD recomandă adăugarea unui alineat la articolul 24 propus conform căruia se vor aplica măsuri de asigurare a dreptului persoanei vizate de a exercita dreptul de acces la datele cu caracter personal referitoare la aceasta, conform articolului 13 din Regulamentul (CE) nr. 45/2001.

V. **CONCLUZII ȘI RECOMANDĂRI**

56. AEPD este de părere că lipsa unei evaluări corespunzătoare a implicațiilor privind protecția datelor în farmacovigilență constituie una dintre slăbiciunile cadrului juridic actual, astfel cum este prevăzut în Regulamentul (CE) nr. 726/2004 și în Directiva 2001/83/CE. Modificarea actuală a Regulamentului (CE) nr. 726/2004 și a Directivei 2001/83/CE ar trebui considerată o oportunitate de a introduce protecția datelor ca element de sine stătător și important al farmacovigilenței.

57. Un aspect general care trebuie abordat este necesitatea efectivă a prelucrării datelor cu caracter personal privind sănătatea în toate etapele procesului de farmacovigilență. După cum a arătat în prezentul aviz, AEPD are îndoieli serioase cu privire la această nevoie și invită legiuitorul să o reevalueze în diversele etape ale procesului. Este clar că scopul farmacovigilenței poate fi atins, în multe cazuri, prin

([27]) A se vedea, de asemenea, nota de subsol 15.

schimbul de informații referitoare la efecte adverse, schimb anonim în sensul legislației privind protecția datelor. Duplicarea raportării se poate evita prin aplicarea unor proceduri de raportare a datelor bine structurate, la nivel național.

58. Amendamentele propuse au în vedere un sistem de raportare simplificat și consolidarea bazei de date EudraVigilance. AEPD a explicat că aceste modificări măresc riscurile pentru protecția datelor, în special în privința raportării directe a pacienților către EMEA sau baza de date EudraVigilance. În acest sens, AEPD sprijină cu fermitate un sistem descentralizat și indirect de raportare prin care comunicarea către portalul web european este coordonată prin utilizarea portalurilor web naționale. De asemenea, AEPD subliniază că viața privată și securitatea ar trebui să facă parte din concepția și punerea în aplicare a unui sistem de raportare prin utilizarea de portaluri web [principiul „viață privată prin concepție" (privacy by design)].

59. AEPD subliniază că din momentul prelucrării datelor privind sănătatea referitoare la persoane fizice identificate sau care pot fi identificate, persoana responsabilă de prelucrare trebuie să se conformeze tuturor cerințelor legislației comunitare în materie de protecție a datelor.

60. Mai precis, AEPD recomandă:

— includerea unei trimiteri la acest aviz în preambulul ambelor propuneri;

— introducerea unui considerent atât în Regulamentul (CE) nr. 726/2004, cât și în Directiva 2001/83/CE, privind importanța protecției datelor în contextul farmacovigilenței, cu trimiteri la legislația comunitară aplicabilă;

— introducerea în Regulamentul (CE) nr. 726/2004 și în Directiva 2001/83/CE a unui nou articol cu caracter general care să prevadă că:

— dispozițiile din Regulamentul (CE) nr. 726/2004 și din Directiva 2001/83/CE nu aduc atingere drepturilor și obligațiilor ce decurg din dispozițiile Regulamentului (CE) nr. 45/2001 și Directivei 95/46/CE, cu trimitere specifică la articolul 10 al Regulamentului (CE) nr. 45/2001 și la articolul 8 al Directivei 95/46/CE;

— datele privind sănătatea care pot fi identificate vor fi prelucrate numai dacă este strict necesar iar părțile implicate ar trebui să evalueze această necesitate în toate etapele procesului de farmacovigilență;

— includerea în articolul 24 alineatul (2) propus din Regulamentul (CE) nr. 726/2004 a unei teze potrivit căreia accesibilitatea bazei de date EudraVigilance va fi reglementată conform drepturilor și obligațiilor ce decurg din legislația comunitară în materie de protecție a datelor;

— adăugarea unui alineat la articolul 24 propus conform căruia se vor aplica măsuri de asigurare a dreptului persoanei vizate de a exercita dreptul de acces la datele cu caracter personal referitoare la aceasta, conform articolului 13 din Regulamentul (CE) nr. 45/2001;

— adăugarea unui alineat la articolul 101 propus din Directiva 2001/83/CE conform căruia, în cazul prelucrării datelor cu caracter personal, persoana va fi informată în mod corespunzător conform articolului 10 din Directiva 95/46/CE;

— includerea în noile articole propuse 25 și 26 din Regulamentul (CE) nr. 726/2004 și în articolul 106 din Directiva 2001/83/CE, care se referă la elaborarea unui sistem de raportare a efectelor adverse prin utilizarea de portaluri web, a unei obligații de incorporare a măsurilor adecvate privind protecția vieții private și securitatea, la același nivel în toate statele membre, luând în considerare principiile de bază ale confidențialității, integrității, responsabilizării și disponibilității datelor.

Adoptat la Bruxelles, 22 aprilie 2009.

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor

IV

(Informări)

INFORMĂRI PROVENIND DE LA INSTITUȚIILE ȘI ORGANELE UNIUNII EUROPENE

COMISIE

Rata de schimb a monedei euro [1]

22 septembrie 2009

(2009/C 229/05)

1 euro =

	Moneda	Rata de schimb		Moneda	Rata de schimb
USD	dolar american	1,4780	AUD	dolar australian	1,6922
JPY	yen japonez	135,09	CAD	dolar canadian	1,5787
DKK	coroana daneză	7,4422	HKD	dolar Hong Kong	11,4552
GBP	lira sterlină	0,90470	NZD	dolar neozeelandez	2,0484
SEK	coroana suedeză	10,0940	SGD	dolar Singapore	2,0863
CHF	franc elvețian	1,5149	KRW	won sud-coreean	1 779,06
ISK	coroana islandeză		ZAR	rand sud-african	10,9943
NOK	coroana norvegiană	8,6280	CNY	yuan renminbi chinezesc	10,0902
BGN	leva bulgărească	1,9558	HRK	kuna croată	7,2943
CZK	coroana cehă	25,131	IDR	rupia indoneziană	14 316,85
EEK	coroana estoniană	15,6466	MYR	ringgit Malaiezia	5,1434
HUF	forint maghiar	271,42	PHP	peso Filipine	70,238
LTL	litas lituanian	3,4528	RUB	rubla rusească	44,5532
LVL	lats leton	0,7055	THB	baht thailandez	49,687
PLN	zlot polonez	4,1613	BRL	real brazilian	2,6726
RON	leu românesc nou	4,2475	MXN	peso mexican	19,6500
TRY	lira turcească	2,1882	INR	rupie indiană	70,8900

[1] *Sursă*: rata de schimb de referință publicată de către Banca Centrală Europeană.

INFORMĂRI PROVENIND DE LA STATELE MEMBRE

Actualizare a listei punctelor de trecere a frontierei menționate la articolul 2 alineatul (8) din Regulamentul (CE) nr. 562/2006 al Parlamentului European și al Consiliului de instituire a unui cod comunitar privind regimul de trecere a frontierelor de către persoane (Codul frontierelor Schengen) (JO C 316, 28.12.2007, p. 1, JO C 134, 31.5.2008, p. 16, JO C 177, 12.7.2008, p. 9, JO C 200, 6.8.2008, p. 10, JO C 331, 31.12.2008, p. 13, JO C 3, 8.1.2009, p. 10, JO C 37, 14.2.2009, p. 10, JO C 64, 19.3.2009, p. 20, JO C 99, 30.4.2009, p. 7)

(2009/C 229/06)

Publicarea listei cu punctele de trecere a frontierei prevăzute la articolul 2 alineatul (8) din Regulamentul (CE) nr. 562/2006 al Parlamentului European și al Consiliului din 15 martie 2006 de instituire a unui cod comunitar privind regimul de trecere a frontierelor de către persoane (Codul frontierelor Schengen) are la bază informațiile comunicate Comisiei de către statele membre în conformitate cu articolul 34 din Codul frontierelor Schengen.

În afară de publicarea în Jurnalul Oficial, o actualizare lunară este disponibilă pe site-ul internet al Direcției Generale Justiție, Libertate și Securitate.

UNGARIA

Înlocuirea listei publicate în JO C 316, 28.12.2007, p. 1.

UNGARIA–CROAȚIA

Frontiere terestre

1. Barcs–Terezino Polje
2. Beremend–Baranjsko Petrovo Selo
3. Berzence–Gola
4. Drávaszabolcs–Donji Miholjac
5. Drávaszabolcs (râu, la cerere) (*)
6. Gyékényes–Koprivnica (cale ferată)
7. Letenye–Goričan I
8. Letenye–Goričan II (autostradă)
9. Magyarboly–Beli Manastir (cale ferată)
10. Mohács (râu)
11. Murakeresztúr–Kotoriba (cale ferată)
12. Udvar–Dubosevica

(*) 07.00-19.00.

UNGARIA–SERBIA

Frontiere terestre

1. Bácsalmás–Bajmok (**)
2. Hercegszántó–Bački Breg
3. Kelebia–Subotica (cale ferată)
4. Mohács (râu)
5. Röszke–Horgoš (autostradă)
6. Röszke–Horgoš (cale ferată)
7. Szeged (râu) (**)
8. Tiszasziget–Đjala (Gyála) (**)
9. Tompa–Kelebija

(**) A se vedea nota de subsol (*).

UNGARIA–ROMÂNIA

Frontiere terestre

1. Ágerdőmajor (Tiborszállás)–Carei (cale ferată)
2. Ártánd–Borș
3. Battonya–Turnu
4. Biharkeresztes–Episcopia Bihorului (cale ferată)

5. Csengersima–Petea
6. Gyula–Vărșand
7. Kiszombor–Cenad
8. Kötegyán–Salonta (cale ferată)
9. Létavértes–Săcuieni (***)
10. Lőkösháza–Curtici (cale ferată)
11. Méhkerék–Salonta
12. Nagylak–Nădlac
13. Nyírábrány–Valea lui Mihai (cale ferată)
14. Nyírábrány–Valea lui Mihai
15. Vállaj–Urziceni

(***) 06.00-22.00.

UNGARIA–UCRAINA

Frontiere terestre

1. Barabás–Kosino (****)
2. Beregsurány–Luzhanka
3. Eperjeske–Salovka (cale ferată)
4. Lónya–Dzvinkove (*****)
5. Tiszabecs–Vylok
6. Záhony–Čop (cale ferată)
7. Záhony–Čop

(****) A se vedea nota de subsol (*).
(*****) 08.00-16.00.

Frontiere aeriene

Aeroporturi internaționale:

1. Budapest Nemzetközi Repülőtér
2. Debrecen Repülőtér
3. Sármellék

Aerodromuri (deschise numai la cerere):

1. Békéscsaba
2. Budaörs
3. Fertőszentmiklós
4. Győr–Pér
5. Kecskemét
6. Nyíregyháza
7. Pápa
8. Pécs–Pogány
9. Siófok–Balatonkiliti
10. Szeged
11. Szolnok

V

(Anunțuri)

PROCEDURI REFERITOARE LA PUNEREA ÎN APLICARE A POLITICII COMERCIALE COMUNE

COMISIE

Aviz privind măsurile antidumping asupra importurilor de nitrat de amoniu originar din Rusia

(2009/C 229/07)

Ca urmare a unei cereri înaintate de JSC Kirovo-Chepetsky Khimichesky Kombinat, Tribunalul de Primă Instanță al Comunităților Europene, prin hotărârea sa din 10 septembrie 2008 în cauza T-348/05, a anulat Regulamentul (CE) nr. 945/2005 ([1]) al Consiliului din 21 iunie 2005 de modificare a (i) Regulamentului (CE) nr. 658/2002 ([2]) de instituire a unui drept antidumping definitiv la importurile de nitrat de amoniu originar din Rusia și a (ii) Regulamentului (CE) nr. 132/2001 ([3]) privind instituirea unui drept antidumping definitiv și perceperea cu titlu definitiv a dreptului provizoriu instituit la importurile de nitrat de amoniu originar din, printre altele, Ucraina. Ca urmare a unei cereri de interpretare a hotărârii mai sus-menționate, Tribunalul de Primă Instanță a declarat în continuare, prin hotărârea sa din 9 iulie 2009, că partea operațională a hotărârii din 10 septembrie 2008 se interpretează în sensul că Regulamentul (CE) nr. 945/2005 din 21 iunie 2005 este anulat în ceea ce privește JSC Kirovo-Chepetsky Khimichesky Kombinat.

În consecință, taxele antidumping definitive plătite în temeiul Regulamentului (CE) nr. 658/2002 al Consiliului pentru importurile de produse fabricate și exportate către Uniunea Europeană de JSC Kirovo-Chepetsky Khimichesky Kombinat, cu excepția taxelor antidumping percepute la importul produselor care se încadrează la codurile NC 3102 30 90 și 3102 40 90 se rambursează sau se remit. Rambursarea sau remiterea se solicită de la autoritățile vamale naționale în conformitate cu legislația vamală aplicabilă.

([1]) JO L 160, 23.6.2005, p. 1.
([2]) JO L 102, 18.4.2002, p. 1.
([3]) JO L 23, 25.1.2001, p. 1.

Prețul abonamentului în 2009
(fără TVA, inclusiv cheltuieli de transport pentru expediere simplă)

Jurnalul Oficial al UE, seriile L+C, numai versiunea tipărită	22 de limbi oficiale ale UE	1 000 EUR pe an (*)
Jurnalul Oficial al UE, seriile L+C, numai versiunea tipărită	22 de limbi oficiale ale UE	100 EUR pe lună (*)
Jurnalul Oficial al UE, seriile L+C, versiunea tipărită + CD-ROM, ediție anuală (cumulat)	22 de limbi oficiale ale UE	1 200 EUR pe an
Jurnalul Oficial al UE, seria L, numai versiunea tipărită	22 de limbi oficiale ale UE	700 EUR pe an
Jurnalul Oficial al UE, seria L, numai versiunea tipărită	22 de limbi oficiale ale UE	70 EUR pe lună
Jurnalul Oficial al UE, seria C, numai versiunea tipărită	22 de limbi oficiale ale UE	400 EUR pe an
Jurnalul Oficial al UE, seria C, numai versiunea tipărită	22 de limbi oficiale ale UE	40 EUR pe lună
Jurnalul Oficial al UE, seriile L+C, CD-ROM, ediție lunară (cumulat)	22 de limbi oficiale ale UE	500 EUR pe an
Supliment la Jurnalul Oficial (seria S – Anunțuri de achiziții publice), CD-ROM, ediție bisăptămânală	Multilingv: 23 de limbi oficiale ale UE	360 EUR pe an (= 30 EUR pe lună)
Jurnalul Oficial al UE, seria C – Anunțuri de concurs	Limbă (limbi) în funcție de concurs	50 EUR pe an

(*) Preț cu amănuntul:
- până la 32 de pagini: 6 EUR
- de la 33 la 64 de pagini: 12 EUR
- peste 64 de pagini: preț fixat după caz

Abonamentul la *Jurnalul Oficial al Uniunii Europene*, care apare în limbile oficiale ale Uniunii Europene, este disponibil în 22 de versiuni lingvistice. Cuprinde seriile L (Legislație) și C (Comunicări și informări).

Pentru fiecare versiune lingvistică se încheie un abonament separat.

În conformitate cu Regulamentul (CE) nr. 920/2005 al Consiliului, publicat în Jurnalul Oficial L 156 din 18 iunie 2005, care prevede că, temporar, instituțiile Uniunii Europene nu au obligația de a redacta toate actele în irlandeză și nici de a le publica în această limbă, Jurnalele Oficiale publicate în limba irlandeză se comercializează separat.

Abonamentul la Suplimentul Jurnalului Oficial (seria S – Anunțuri de achiziții publice) cuprinde toate cele 23 de versiuni lingvistice oficiale într-un singur CD-ROM multilingv.

La cerere, abonamentul la *Jurnalul Oficial al Uniunii Europene* conferă dreptul de a primi diverse anexe ale Jurnalului Oficial. Abonaților li se semnalează apariția anexelor printr-un „Anunț pentru cititori” inclus în *Jurnalul Oficial al Uniunii Europene*.

Distribuire și abonamente

Publicațiile destinate vânzării, editate de Oficiul pentru Publicații, pot fi procurate prin agențiile noastre de vânzări.

Lista agențiilor de vânzări este disponibilă la adresa:

http://publications.europa.eu/others/agents/index_ro.htm

EUR-Lex (http://eur-lex.europa.eu) oferă un acces direct și gratuit la dreptul Uniunii Europene. Acest site permite consultarea *Jurnalului Oficial al Uniunii Europene*, inclusiv a tratatelor, a legislației, a jurisprudenței și a actelor pregătitoare ale legislației.

Pentru mai multe informații despre Uniunea Europeană, consultați: http://europa.eu

Oficiul pentru Publicații al Uniunii Europene
2985 Luxemburg
LUXEMBURG

RO