

**Al doilea aviz al Autorității Europene pentru Protecția Datelor privind propunerea de decizie-cadru a Consiliului privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală**

(2007/C 91/02)

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 <sup>(1)</sup>,

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 <sup>(2)</sup>, în special articolul 41,

ADOPTĂ PREZENTUL AVIZ:

1. În data de 19 decembrie 2005, AEPD a prezentat un aviz <sup>(3)</sup> privind propunerea Comisiei de decizie-cadru a Consiliului privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală. În acest aviz, a subliniat importanța propunerii ca instrument eficient pentru protecția datelor cu caracter personal în domeniul acoperit de Titlul VI al Tratatului UE. Acest instrument nu trebuie doar să respecte principiile protecției de date așa cum sunt enunțate în Convenția Consiliului Europei nr. 108 <sup>(4)</sup> și mai explicit în Directiva 95/46/CE, ci și să asigure un set de reguli suplimentare ținând cont de natura specifică a domeniului de aplicare a legilor. Pentru AEPD este esențial ca decizia-cadru să acopere toate prelucrările de date polițienești și judiciare, chiar dacă acestea nu sunt transmise sau făcute disponibile de către autoritățile competente ale altor state membre. Uniformitatea protecției datelor cu caracter personal este esențială, indiferent unde, de către cine sau în ce scop sunt prelucrate. AEPD a făcut mai multe propuneri pentru a îmbunătăți nivelul de protecție.
2. În data de 27 septembrie 2006, Parlamentul European a adoptat o rezoluție legislativă privind propunerea Comisiei. În linii generale, rezoluția are aceleași obiective ca avizul AEPD: sprijinirea propunerii în general și modificări care au ca scop întărirea nivelului de protecție permis de către decizia-cadru.
3. Propunerea Comisiei este în prezent discutată în cadrul Consiliului. Potrivit unor rapoarte <sup>(5)</sup>, Consiliul face progrese și modifică unele elemente esențiale ale textului propunerii. Președinția Consiliului depune eforturi sporite pentru a obține progrese și mai semnificative. Scopul este de a atinge o abordare comună asupra elementelor principale până în decembrie 2006.
4. AEPD apreciază în mod deosebit faptul că o atenție specială este acordată de Consiliu acestei importante propuneri. Cu toate acestea, este preocupată de direcțiile de dezvoltare. Textul discutat în prezent la nivelul Consiliului nu include modificările propuse de Parlamentul European și nici avizul AEPD și al Conferinței Autorităților Europene pentru Protecția Datelor. Dimpotrivă, în unele cazuri, dispozițiile din propunerea Comisiei prin care se oferă garanții cetățenilor, sunt eliminate sau atenuate substanțial. *Drept rezultat, există un risc important ca nivelul de protecție să fie inferior celui asigurat prin Directiva 95/46/CE sau chiar celui formulat mult mai general în Convenția nr. 108 a Consiliului Europei și care este obligatoriu pentru statele membre.*

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

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

<sup>(3)</sup> JO C 47, 25.2.2006, p. 27.

<sup>(4)</sup> Convenția pentru protecția persoanelor fizice privind prelucrarea automată a datelor cu caracter personal a Consiliului Europei, 28 ianuarie 1981.

<sup>(5)</sup> În mod formal, nu există documente publice accesibile, iar AEPD nu este implicată direct în munca grupului de lucru al Consiliului. Documente care reflectă situația în interiorul Consiliului pot fi găsite pe pagina de internet a Statewatch ([www.statewatch.org](http://www.statewatch.org)).

5. AEPD menționează de asemenea că recent, Comitetul pentru Libertăți Civile, Justiție și Afaceri Interne (LIBE) din Parlamentul European și-a exprimat preocuparea privind opțiunile Consiliului cu privire la această propunere de decizie-cadru.
6. Din aceste motive, AEPD adoptă acum un al doilea aviz. Acest al doilea aviz se concentrează asupra unor probleme esențiale și nu repetă toate punctele menționate în avizul AEPD din decembrie 2005, care rămân în întregime valabile.

#### *Probleme generale*

7. În domeniul libertății, securității și justiției aflat în plină dezvoltare, schimbul de informații polițienești și judiciare între statele membre devine din ce în ce mai important. Mai multe instrumente juridice sunt propuse sau au fost adoptate pentru a facilita acest schimb de informații. AEPD subliniază încă o dată că, în acest context, un cadru juridic stabil este necesar pentru a asigura respectarea drepturilor fundamentale ale cetățenilor. Prezenta (propunere de) decizie-cadru este legată în mod direct de propunerile care facilitează schimbul de informații.
8. Cu toate că recunoaște importanța adoptării cât mai grabnice a deciziei-cadru de către Consiliu, AEPD atenționează că rapiditatea luării deciziei nu trebuie să conducă la o reducere a standardelor de protecție. Textul dezbătut în prezent la nivelul Consiliului provoacă îndoieli în privința faptului că rezultatul va fi îndeajuns de solid pentru a oferi cetățenilor un nivel de protecție eficient. În situația de față, consecința obiectivului de rapiditate pare a fi că dispozițiile eventual controversate sunt eliminate sau atenuate. Lipsa unui timp suficient pentru a ajunge la un consens în privința dispozițiilor eventual controversate, poate avea ca rezultat compromiterea calității deciziei-cadru.
9. În aceste circumstanțe, AEPD recomandă Consiliului să acorde mai mult timp negocierilor pentru a atinge un rezultat care să asigure un grad de protecție adecvat.

#### *Aplicabilitatea pentru prelucrările interne*

10. Această problemă a fost un element esențial al avizului din decembrie 2005 și a fost dezbătută ulterior cu mare atenție. Regulile generale privind protecția datelor trebuie să se aplice tuturor datelor în domeniul cooperării polițienești și judiciare, și nu trebuie să se limiteze la schimburile transfrontaliere între statele membre. Un domeniu de aplicare mai limitat nu ar putea oferi o protecție adecvată, așa cum se cere prin articolul 30 alineatul (1) litera b) din Tratatul UE. Acest punct a fost subliniat în mai multe ocazii, de asemenea de către alte părți interesate în afară de AEPD.
11. În avizul din decembrie 2005, AEPD a stabilit că limitarea la schimbul de date cu alte state membre ar face domeniul de aplicare al deciziei-cadru deosebit de nesigur și de instabil, fapt care ar fi contrar obiectivului său principal. La data colectării sau prelucrării datelor cu caracter personal, nu se cunoaște faptul dacă aceste date vor fi sau nu relevante ulterior pentru schimbul cu autoritățile competente din alte state membre.
12. Din acest motiv, un domeniu de aplicare mai limitat este nefuncțional și, dacă ar fi introdus, ar cere distincții dificile și precise în bazele de date ale autorităților de aplicare a legilor, având ca rezultat complicații și cheltuieli suplimentare pentru aceste autorități și fiind mai mult în detrimentul siguranței juridice a persoanelor fizice.
13. Două exemple pot fi date pentru a ilustra aceste consecințe. În primul rând, complicații și cheltuieli suplimentare ar rezulta din faptul că dosarele penale sunt în mare număr compuse din date provenind de la autorități diferite. Consecința unui domeniu de aplicare limitat ar fi că părți ale acestor dosare compuse — părțile care conțin date provenind de la autorități din alte state membre — ar fi protejate în decizia-cadru, iar alte părți nu ar fi. În al doilea rând, siguranța juridică a persoanelor ar avea de suferit, deoarece — în cazul unui domeniu de aplicare mai limitat — datele provenind din țări terțe, dar neschimbate între statele membre, nu ar fi acoperite de decizia-cadru. Se subînțelege că prelucrarea acestor date ar atrage riscuri specifice pentru persoanele vizate, cum ar fi de exemplu faptul că nu există o obligație juridică de a examina exactitatea acestor date. Un bun exemplu ar fi utilizarea listelor „no-fly” în scopul aplicării legii în statele membre.

14. AEPD subliniază încă o dată faptul că este nevoie de un nivel ridicat de protecție a datelor în domeniul cooperării polițienești și judiciare, domeniu în care prelucrarea datelor cu caracter personal presupune, prin natura sa, riscuri specifice pentru cetățeni așa cum, *inter alia*, s-a recunoscut în articolul 30 alineatul (1) litera (b) din Tratatul UE. Mai mult decât atât, discrepanțe mari între protecția datelor în primul și al treilea pilon ar afecta nu numai drepturile cetățenilor la protecția datelor cu caracter personal, ci și eficiența cadrului de aplicare a legilor, respectiv încrederea reciprocă între statele membre.
15. Propunerea servește ambelor obiective. Trebuie să asigure garanții pentru cetățeni împotriva utilizării necorespunzătoare a datelor lor cu caracter personal. Pentru cetățeni, nu are importanță dacă datele referitoare la aceștia sunt prelucrate în contextul unui schimb între statele membre sau într-un context exclusiv intern. Mai mult decât atât, ar trebui să contribuie la încrederea reciprocă între statele membre, ca o condiție pentru un schimb reușit de informații. Dacă la prelucrarea datelor se aplică standardele generale, ar rezulta o mai ușoară acceptare a schimbului de date între statele membre.
16. AEPD atenționează că limitarea domeniului de aplicare a deciziei-cadru în contextul unui schimb de date nu ar contribui în totalitate la întărirea încrederii reciproce între autoritățile statelor membre. Mai mult decât atât, un text limitat nu protejează cetățenii într-un mod adecvat. În asemenea circumstanțe, decizia-cadru nu ar mai prezenta o garanție adecvată pentru cetățeni împotriva eventualelor abuzuri asupra datelor lor, din partea autorităților publice. Potrivit AEPD, această „funcție de protecție” a legislației este esențială, cel puțin pentru a asigura faptul că Uniunea Europeană respectă drepturile fundamentale în conformitate cu articolul 6 din Tratatul UE.
17. În încheiere, există un argument strategic în favoarea deciziei-cadru aplicabilă tuturor prelucrărilor. După cum arată recente negocieri cu Statele Unite pentru un nou acord privind prelucrarea și transferul datelor pasagerilor curselor aeriene <sup>(1)</sup>, o legislație UE stabilă, protejând cetățenii în orice situații în interiorul UE, va consolida poziția UE în negocierile cu țări terțe. În absența unei legislații stabile, ar fi mai degrabă dificil să se insiste asupra unui nivel adecvat de protecție în țări terțe, ca o precondiție pentru transferul de date cu caracter personal.

#### *Alte preocupări*

18. *Sublinierea calității datelor.* Articolul 4 din propunerea Comisiei include nu numai principiile esențiale de calitate a datelor din Directiva 95/46/CE, ci și pentru unele dintre acestea, asigură reguli speciale. Face distincție între diferitele tipuri de persoane vizate (suspecți, persoane condamnate, victime, martori etc.). Datele referitoare la acestea trebuie tratate diferit, cu garanțiile specifice, în special în privința persoanelor nesuspecte. Articolul 4 conține în continuare obligațiile pentru statele membre de a distinge datele conform gradului lor de exactitate și de temeinicie. Aceasta este o dispoziție importantă deoarece autoritățile care aplică legile utilizează de asemenea date bazate pe presupuneri și nu neapărat pe fapte. AEPD consideră aceste dispoziții ca garanții esențiale care nu trebuie suprimate din propunere sau făcute facultative.
19. *Prelucrarea datelor și limitarea scopurilor.* În avizul din decembrie 2005, AEPD a analizat necesitatea de adoptare a unor dispoziții juridice mai bune privind utilizarea ulterioară a datelor care au fost colectate de către o autoritate, pentru un anumit scop. În prezent, preocupările AEPD privind articolul 5 sunt legate în principal de punctul de vedere că în timp ce, pe de o parte, prelucrarea (ulterioară) a datelor pentru scopuri mai largi trebuie să fie acordată, pe de altă parte, legislația trebuie să asigure condiții precise pentru această prelucrare, pentru a proteja persoanele vizate. AEPD atenționează împotriva soluțiilor care lasă problema la discreția legislațiilor naționale sau care nu limitează condițiile pentru prelucrarea ulterioară în conformitate cu Directiva 95/46/CE și cu Convenția nr. 108 a Consiliului European <sup>(2)</sup>. În privința prelucrării categoriilor speciale de date: aceasta a fost dezbătută în Directiva 95/46/CE și în Convenția nr. 108, într-o interdicție generală cu excepții <sup>(3)</sup>. AEPD este preocupată de faptul că, în decizia-cadru, interdicția generală va fi suprimată și că — acționând astfel — excepția devine regulă. O asemenea soluție nu ar fi incompatibilă cu Directiva 95/46/CE, dar nu va fi conformă cu Convenția 108.

<sup>(1)</sup> Acordul între Uniunea Europeană și Statele Unite ale Americii privind prelucrarea și transferul datelor de înregistrare a numerelor pasagerilor (PNR) de către companii aeriene către Departamentul de Securitate Națională a Statelor Unite, JOL 298, p. 29.

<sup>(2)</sup> Vezi: articolul 13, în legătură cu articolul 6 alineatul (1) litera (b) din Directiva 95/46/CE, și articolul 9, în legătură cu articolul 5 litera (b) din Convenția 108.

<sup>(3)</sup> Vezi: articolul 8 din Directiva 95/46/CE și articolul 6 din Convenția 108.

20. Schimbul de date cu alte autorități și părți private. Propunerea Comisiei conține limitări și garanții specifice pentru schimbul de informații cu alte autorități, în afară de autoritățile polițienești și judiciare, cu părți private sau autorități ale țărilor terțe. AEPD subliniază importanța acestor dispoziții speciale pentru următoarele motive. În primul rând, schimbul de informații cu aceste „terțe părți” atrage după sine riscuri specifice (violarea securității, prelucrarea ulterioară în alte scopuri etc.). În al doilea rând, implicarea părților terțe în domeniul aplicării legilor și în prelucrarea informațiilor de aplicare a legilor devine tot mai mult un truism. Directiva 2006/24/CE privind stocarea datelor <sup>(1)</sup>, acordul privind datele PNR cu Statele Unite și așa-numitul caz Swift <sup>(2)</sup> sunt exemple relevante. În al treilea rând, hotărârea PNR a Curții Europene de Justiție din 30 mai 2006 <sup>(3)</sup> ridică serioase semne de întrebare privind protecția datelor cu caracter personal colectate de către părți private în scopuri comerciale și prelucrate ulterior în scopuri de aplicare a legilor.
21. În privința transferului către și de la o altă parte — publică sau privată — în interiorul UE, este important ca propunerea să trateze problema într-un mod precis și să ofere soluții compatibile cu Directiva 95/46/CE. Aceste soluții trebuie să asigure că rezultatele structurii pilonilor — în special incertitudinea privind delimitarea ambilor piloni în privința schimbului de date cu caracter personal între autoritățile de aplicare a legii și alte părți — nu va afecta negativ eficacitatea protecției.
22. În privința transferului de date către sau de la țări terțe, propunerea Comisiei asigură o decizie competentă din partea Comisiei. Dacă aceasta nu ar fi acceptată în Consiliu, rezultatul ar fi că fiecare stat membru va decide asupra competenței pe cont propriu sau, chiar mai rău, va transfera datele fără a examina nivelul de protecție într-o țară terță. Absența unui sistem armonizat pentru schimbul de date cu caracter personal cu țările terțe va putea de asemenea să:
- afecteze încrederea între autoritățile statelor membre deoarece o autoritate poate fi mai puțin motivată să comunice informații unei autorități dintr-un alt stat membru, dacă acest stat membru ar putea comunica informațiile autorităților unei țări terțe, în absența unor garanții clare,
  - provoace reveniri la punctul de plecare. Dacă autoritatea statului membru nu poate primi informații directe de la un alt stat membru din cauza protecției datelor de către Decizia-cadru, aceasta poate solicita asistență de la o autoritate dintr-o țară terță,
  - permită fenomenul de „forum shopping” pentru autoritățile din țări terțe: aceste autorități pot solicita informații în statele membre, beneficiind de cele mai reduse cerințe juridice pentru transferuri.
- AEPD consideră esențial ca mecanismul care asigură standardele comune și coordonează deciziile competente să fie pus în aplicare, de asemenea pentru a fi compatibil cu Convenția nr. 108 a Consiliului Europei (în special articolul 12 din aceasta) <sup>(4)</sup>. Textul deciziei-cadru trebuie să prevadă un asemenea mecanism.
23. AEPD înțelege că mai multe state membre contestă bazele juridice pentru includerea unei dispoziții privind schimbul de date cu caracter personal cu țări terțe, în cazurile în care aceste date nu sunt permise de la, sau făcute accesibile de către autoritatea competentă a unui alt stat membru. Potrivit AEPD, contestarea bazelor juridice este neîntemeiată. Exemplele prezentate în avizul din decembrie 2005, precum și argumentele menționate în paragraful precedent demonstrează legătura directă a acestor schimburi cu țări terțe, cu cooperarea polițienească și judiciară în conformitate cu articolul 29 din Tratatul UE. Dispoziția privind schimbul de date cu caracter personal cu țări terțe, trebuie considerată ca o dispoziție suplimentară și necesară pentru atingerea obiectivelor articolului 29 UE în legătură cu articolul 6 UE, în special pentru o cooperare mai strânsă a forțelor polițienești prin respectarea drepturilor fundamentale.

<sup>(1)</sup> Directiva 2006/24/CE a Parlamentului European și a Consiliului din 15 martie 2006 privind stocarea datelor generate sau prelucrate în legătură cu dispoziția serviciului de comunicare electronică accesibil publicului sau a rețelelor de comunicare publice și modificând Directiva 2002/58/CE, JO L 105, p. 54.

<sup>(2)</sup> Vezi Avizul 10/2006 din 22 noiembrie 2006 privind articolul 29 al Grupului de Lucru pentru Protecția Datelor privind prelucrarea datelor cu caracter personal de către Societatea pentru Telecomunicații Financiare Interbancare Internațională (SWIFT).

<sup>(3)</sup> Hotărârea în cazurile C-317/04 și C-318/04.

<sup>(4)</sup> Vezi de asemenea mai precis: articolul 2 din Protocolul Suplimentar (ratificat de mai multe state membre), care corespunde articolelor 25-26 din Directiva 95/46/CE.

24. *Drepturile persoanelor vizate.* Persoanele vizate au dreptul să fie informate despre prelucrarea datelor cu caracter personal care le privesc direct. Acest drept este legat de principiul prelucrării corecte și legale a datelor cu caracter personal, care, în sine, este respectat de către decizia-cadru și este protejat de Convenția nr. 108 a Consiliului Europei, în special în articolele 5 litera (a) și 8. Un element esențial al acestui drept este că informația trebuie comunicată de către operatorul de date *ex officio*. Deoarece persoanele vizate nu cunosc și nu pot cunoaște, în mod normal, faptul că informațiile referitoare la ele au fost prelucrate, ar fi contrar naturii acestui drept să se necesite o cerere de la persoanele vizate. Bineînțeles, dreptul de informare face obiectul unor excepții și este clar că aceste excepții pot juca un rol important în domeniul aplicării legilor, deoarece informațiile privind investigațiile penale ar putea prejudicia investigația însăși. Totuși, orice soluție care face dreptul de informare dependent de o cerere din partea persoanelor vizate, nu poate fi acceptată și nu este compatibilă cu Convenția nr. 108 a Consiliului Europei.
25. AEPD subliniază faptul că *poziția autorităților pentru protecția datelor* trebuie să fie compatibilă cu poziția oferită acestora de Directiva 95/46/CE. Această poziție este cea mai importantă în domeniul cooperării polițienești și judiciare. Cooperarea între autoritățile de aplicare a legii pentru a combate în mod eficient terorismul și alte infracțiuni serioase necesită prelucrarea frecventă de date cu caracter personal confidențiale și necesită excepții de la drepturile persoanelor vizate (vezi, de exemplu punctul precedent, privind dreptul de informare).
26. AEPD subliniază în primul rând necesitatea supravegherii și inspecției efective de către autorități a prelucrării datelor cu caracter personal în cadrul domeniului de aplicare a acestei decizii-cadru, în special când datele cu caracter personal sunt schimbate între statele membre în domeniul cooperării polițienești. În al doilea rând, trebuie asigurat rolul consultativ al autorităților, atât în cadrul jurisdicției naționale cât și în cel al rețelei instituționalizate al autorităților de protecție a datelor, grupul de lucru al autorităților (cunoscut în directivă ca „Articolul 29 — Grupul de lucru”). Intervenția autorităților de protecție a datelor este necesară, în vederea întăririi armonizării protecției sub acest instrument cu protecția menționată în Directiva 95/46/CE, pentru a asigura compatibilitatea cu obligațiile juridice și pentru a atinge armonizarea între statele membre, de asemenea la nivel practic.
27. Articolul 24 din propunerea Comisiei conține reguli detaliate privind *securitatea*, comparabile cu regulile incluse în Convenția Europol. AEPD atenționează asupra suprimării acestor reguli din propunere. Un nivel armonizat de securitate este un instrument important pentru întărirea încrederii atât a persoanelor vizate, cât și între autoritățile statelor membre.
28. În avizul din decembrie 2005, AEPD recomandă că garanțiile specifice trebuie aplicate prin luarea în considerare a *prelucrării unor categorii specifice de date*, cum ar fi datele biometrice și codul ADN. În domeniul aplicării legilor, utilizarea acestor categorii de date devine din ce în ce mai importantă, chiar dacă această utilizare poate atrage după sine riscuri speciale pentru persoanele vizate. Sunt necesare reguli comune. AEPD regretă că această recomandare nu a fost luată în considerare de către Consiliu, sau cel puțin nu vizibil. AEPD recomandă Comisiei și Consiliului să adopte o propunere în această materie, indiferent dacă se raportează sau nu la principiul de disponibilitate.

#### Concluzii

29. AEPD recomandă Consiliului să acorde mai mult timp dezbaterilor pentru a ajunge la un rezultat care să asigure o protecție adecvată. Cu toate că AEPD recunoaște importanța adoptării deciziei-cadru de către Consiliu într-un termen scurt, atenționează că rapiditatea luării deciziei nu trebuie să conducă la o reducere a standardelor de protecție.
30. Armonizarea protecției este esențială, indiferent unde, de către cine și în ce scop sunt prelucrate datele cu caracter personal. AEPD recomandă Consiliului să respecte nivelul de protecție care să nu fie inferior celui asigurat de Directiva 95/46/CE sau chiar celui formulat în linii generale în Convenția nr. 108 a Consiliului Europei și care este obligatoriu pentru statele membre.
31. Regulile generale privind protecția datelor trebuie să se aplice tuturor datelor în domeniul cooperării polițienești și judiciare și să nu se limiteze la un schimb transfrontalier între statele membre. Prezentul aviz conține argumente care arată că un domeniu de aplicare mai limitat este nefuncțional și care, în cazul în care ar fi introdus, ar conduce la complicații și cheltuieli suplimentare pentru autorități și ar deteriora siguranța juridică a persoanelor fizice.

32. Alte preocupări ale AEPD sunt:

- Dispozițiile speciale privind calitatea datelor din propunerea Comisiei nu trebuie suprimate din propunere, sau făcute facultative,
- Dispozițiile privind utilizarea ulterioară a datelor și privind categoriile speciale de date trebuie să fie compatibile cu Directiva 95/46/CE și conforme cu Convenția nr. 108 a Consiliului Europei,
- Dispozițiile speciale privind schimbul de date cu alte părți, în afara autorităților de aplicare a legii, în interiorul UE, nu trebuie suprimate din propunere sau limitate în domeniul de aplicare. În privința schimbului de date cu țări terțe, *cel puțin* mecanismul care asigură standardele comune și deciziile coordonate privind competența, trebuie pus în aplicare, de asemenea în compatibilitate cu Convenția nr. 108 a Consiliului Europei. Textul deciziei-cadru trebuie să asigure un astfel de mecanism,
- Soluțiile care promovează dependența dreptului de informare de o cerere a persoanei vizate, nu sunt acceptabile și nici compatibile cu Convenția nr. 108 a Consiliului Europei,
- Poziția autorităților de protecție a datelor trebuie să fie armonizată cu poziția asigurată în Directiva 95/46/CE,
- Regulile detaliate privind securitatea, comparabile cu regulile incluse în Convenția Europol, nu trebuie suprimate din propunere,
- Comisia și Consiliul trebuie să adopte o propunere privind prelucrarea categoriilor speciale de date, cum ar fi datele biometrice și codul ADN, indiferent dacă sunt sau nu în raport cu principiul disponibilității.

Adoptat la Bruxelles, 29 noiembrie 2006.

Peter HUSTINX  
Autoritatea Europeană pentru Protecția  
Datelor

---