

I

(Rezoluții, recomandări și avize)

AVIZE

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR

Avizul Autorității Europene pentru Protecția Datelor privind inițiativa Regatului Belgiei, a Republicii Bulgaria, a Republicii Estonia, a Regatului Spaniei, a Republicii Franceze, a Republicii Italiene, a Republicii Ungare, a Republicii Polone, a Republicii Portugheze, a României, a Republicii Finlanda și a Regatului Suediei pentru o directivă a Parlamentului European și a Consiliului privind ordinul european de protecție, și privind inițiativa Regatului Belgiei, a Republicii Bulgaria, a Republicii Estonia, a Regatului Spaniei, a Republicii Austria, a Republicii Slovenia și a Regatului Suediei pentru o directivă a Parlamentului European și a Consiliului privind ordinul european de anchetă în materie penală

(2010/C 355/01)

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR,

ADOPTĂ URMĂTORUL AVIZ:

I. INTRODUCERE

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

având în vedere Carta drepturilor fundamentale a Uniunii Europene, în special articolul 8,

având în vedere Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date ⁽¹⁾,

având în vedere Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date, în special articolul 41 ⁽²⁾,

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 ⁽³⁾,

1. În ultimii ani s-au depus eforturi din ce în ce mai intense pentru îmbunătățirea cooperării judiciare în materie penală. Acest subiect, care ocupă în prezent o poziție-cheie în cadrul Programului de la Stockholm ⁽⁴⁾, este caracterizat prin natura deosebit de sensibilă a datelor cu caracter personal implicate și prin efectele pe care prelucrarea conexă a datelor ar putea să le aibă asupra persoanelor vizate.
2. Din aceste motive, Autoritatea Europeană pentru Protecția Datelor (AEPD) a acordat o atenție deosebită acestui subiect ⁽⁵⁾ și intenționează ca prin intermediul prezentului aviz să sublinieze încă o dată necesitatea protejării drepturilor fundamentale ca piatră de temelie a spațiului de libertate, securitate și justiție (SLSJ) prevăzut în Programul de la Stockholm.
3. Prezentul aviz este o reacție la două inițiative pentru adoptarea unei directive, aparținând mai multor state membre, după cum prevede articolul 76 din Tratatul privind funcționarea Uniunii Europene, respectiv:

⁽¹⁾ JO L 281, 23.11.1995, p. 31.

⁽²⁾ JO L 8, 12.1.2001, p. 1.

⁽³⁾ JO L 350, 30.12.2008, p. 60.

⁽⁴⁾ Consiliul European, Programul de la Stockholm – O Europă deschisă și sigură în serviciul cetățenilor și pentru protecția acestora (2010/C 115/01), capitolul 3, „Facilitarea vieții cetățenilor: o Europă a dreptului și a justiției”, JO C 115, 4.5.2010, p. 1; a se vedea și Avizul AEPD privind Comunicarea Comisiei către Parlamentul European și Consiliu „Un spațiu de libertate, securitate și justiție în serviciul cetățenilor”, JO C 276, 17.11.2009, p. 8.

⁽⁵⁾ În ultimii ani, AEPD a adoptat un număr important de avize și comentarii referitoare la inițiative privind spațiul de libertate, securitate și justiție care se găsesc în totalitate pe site-ul web al AEPD.

- (a) inițiativa a 12 state membre pentru o directivă a Parlamentului European și a Consiliului privind ordinul european de protecție („inițiativa OEP”), prezentată în ianuarie 2010 ⁽⁶⁾; și
- (b) inițiativa a 7 state membre pentru o directivă a Parlamentului European și a Consiliului privind ordinul european de anchetă în materie penală („inițiativa OEA”), prezentată în aprilie 2010 ⁽⁷⁾.
4. Consilierea în privința acestor inițiative se înscrie în sarcina încredințată AEPD la articolul 41 din Regulamentul (CE) nr. 45/2001 pentru consilierea instituțiilor și organelor UE asupra tuturor aspectelor privind prelucrarea de date cu caracter personal. Prin urmare, prezentul aviz formulează comentarii cu privire la inițiative în măsura în care acestea se referă la prelucrarea datelor cu caracter personal. Întrucât AEPD nu a primit nicio solicitare de consiliere, prezentul aviz este emis din proprie inițiativă ⁽⁸⁾.
5. AEPD reamintește că, în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001, Comisia are obligația să consulte AEPD atunci când adoptă o propunere legislativă referitoare la protecția drepturilor și libertăților persoanelor în ceea ce privește prelucrarea datelor cu caracter personal. În cazul unei inițiative din partea statelor membre, această obligație nu se aplică *strictu sensu*. Cu toate acestea, de la intrarea în vigoare a Tratatului de la Lisabona, procedura legislativă ordinară se aplică și în domeniul cooperării polițienești și judiciare, cu o singură excepție specifică prevăzută la articolul 76 din Tratatul privind funcționarea Uniunii Europene, respectiv o părtime din statele membre pot avea inițiativa de adoptare a unor măsuri UE. În conformitate cu Tratatul de la Lisabona, aceste inițiative sunt aliniate în cea mai mare măsură posibilă la propunerile Comisiei, iar ori de câte ori este posibil ar trebui folosite garanții procedurale. Din acest motiv, prezentele inițiative sunt însoțite de o evaluare a impactului.
6. În acest context, AEPD nu doar regretă faptul că nu a fost consultată atunci când au fost formulate inițiativele, ci recomandă, în plus, Consiliului să stabilească o procedură în cadrul căreia să aibă loc o consultare a AEPD atunci când o inițiativă introdusă de statele membre se referă la prelucrarea datelor cu caracter personal.
7. Deși cele două inițiative au obiective diferite – respectiv îmbunătățirea protecției victimelor și cooperarea transfrontalieră în materie penală prin colectarea transfrontalieră a probelor – acestea prezintă similități importante:
- (a) ambele se bazează pe principiul recunoașterii reciproce a hotărârilor și deciziilor judiciare ⁽⁹⁾;
- (b) își au originea în Programul de la Stockholm ⁽¹⁰⁾; și
- (c) prevăd schimbul de date cu caracter personal între statele membre (a se vedea punctele 10 și 13 și secțiunea II.4).

Din aceste motive, AEPD consideră adecvată examinarea acestora împreună.

8. În acest cadru, ar trebui menționat faptul că și Comisia Europeană s-a ocupat de curând de chestiunea colectării probelor în vederea depunerii acestora la autoritățile competente din alte state membre (aspect ce reprezintă obiectul specific al inițiativei OEA). Într-adevăr, la sfârșitul anului 2009 a fost publicată o *Carte verde* ⁽¹¹⁾ – faza de consultare pentru aceasta fiind în prezent încheiată ⁽¹²⁾ – scopul Comisiei [dedus din „Planul de acțiune pentru punerea în aplicare a Programului de la Stockholm” ⁽¹³⁾] fiind acela de a înainta o propunere legislativă pentru obținerea unui regim cuprinzător privind probele în materie penală, bazat pe principiul recunoașterii reciproce, care să reglementeze toate tipurile de probe în 2011 ⁽¹⁴⁾.

⁽⁹⁾ Acest principiu, introdus în Planul de acțiune de la Viena [Planul de acțiune al Consiliului și al Comisiei referitor la modalitățile optime de punere în aplicare a dispozițiilor Tratatului de la Amsterdam privind crearea unui spațiu de libertate, securitate și justiție. Text adoptat de Consiliul Justiție și Afaceri Interne din 3 decembrie 1998, JO C 19, 23.1.1999, p. 1, punctul 45(f)], a fost formulat clar în Concluziile Consiliului European de la Tampere din 15 și 16 octombrie 1999, la punctele 33, 35-37.

⁽¹⁰⁾ O a treia inițiativă (pentru o directivă a Parlamentului European și a Consiliului privind dreptul la interpretare și traducere în cadrul procedurilor penale, 22 ianuarie 2010, 2010/0801) are aceeași origine, însă nu a fost luată în considerare aici, întrucât nu implică aspecte legate de protecția datelor cu caracter personal. A se vedea, în legătură cu același subiect, și propunerea pentru o directivă a Parlamentului European și a Consiliului privind dreptul la interpretare și traducere în cadrul procedurilor penale, 9.3.2010, COM(2010) 82 final.

⁽¹¹⁾ Carte verde privind obținerea de probe în materie penală dintr-un stat membru în altul și asigurarea admisibilității acestora, COM(2009) 624 final, 11.11.2009.

⁽¹²⁾ Răspunsurile diferite și uneori contrastante sunt examinate în prezent de Comisia Europeană și pot fi citite la: http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0004_en.htm

⁽¹³⁾ Comunicarea Comisiei către Parlamentul European, Consiliul, Comitetul Economic și Social European și Comitetul Regiunilor, Crearea unui spațiu de libertate, securitate și justiție pentru cetățenii Europei. Plan de acțiune pentru punerea în aplicare a Programului de la Stockholm, Bruxelles, 20.4.2010, COM(2010) 171 final, p. 18.

⁽¹⁴⁾ Deocamdată nu este clar cum va inter-relaționa un posibil instrument viitor cu inițiativa OEA.

⁽⁶⁾ JO C 69, 18.3.2010, p. 5.

⁽⁷⁾ JO C 165, 24.6.2010, p. 22.

⁽⁸⁾ AEPD a adoptat și în trecut avize privind inițiative ale statelor membre: a se vedea, de exemplu, Avizul AEPD din 4 aprilie 2007 privind inițiativa a 15 state membre în vederea adoptării unei decizii a Consiliului privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și criminalității transfrontaliere (JO C 169, 21.7.2007, p. 2) și Avizul AEPD din 25 aprilie 2008 privind inițiativa a 14 state membre în vederea adoptării unei decizii a Consiliului privind consolidarea Eurojust și de modificare a Deciziei 2002/187/JAI (JO C 310, 5.12.2008, p. 1).

II. COOPERAREA JUDICIARĂ ÎN MATERIE PENALĂ ȘI PRELUCRAREA DATELOR CU CARACTER PERSONAL ÎN CADRUL INIȚIATIVELOR OEP ȘI OEA

II.1. Contextul inițiativelor

9. Inițiativele menționate mai sus s-au înscris în tendința acțiunilor UE în SLSJ din ultimii ani. Din septembrie 2001 s-a înregistrat o creștere semnificativă a colectării și punerii în comun a informațiilor în cadrul Uniunii Europene (și cu țările terțe), datorată și evoluțiilor din domeniul TIC și facilitată de o serie de instrumente juridice ale UE. De asemenea, inițiativele OEP și OEA au drept scop îmbunătățirea schimbului de informații în legătură cu persoanele fizice în SLSJ.

II.2. Inițiativa OEP

10. Inițiativa OEP – care se bazează pe articolul 82 alineatul (1) litera (d) din Tratatul privind funcționarea Uniunii Europene – se concentrează asupra protecției victimelor unor fapte penale, în special a femeilor, și își propune să garanteze protecția eficientă a acestora în cadrul Uniunii Europene. Pentru a realiza acest scop, inițiativa OEP permite extinderea măsurilor de protecție enumerate la articolul 2 alineatul (2) din aceasta și adoptate în conformitate cu legislația unui stat membru („stat membru emitent”) la alt stat membru în care se mută persoana protejată („stat membru de executare”), fără a fi necesar ca victima să înceapă noi proceduri sau să furnizeze din nou probe în statul de executare.

11. Prin urmare, măsurile de protecție impuse (la cererea victimei) persoanei care reprezintă un pericol au drept scop protejarea vieții, a integrității fizice și psihice, a libertății sau integrității sexuale a victimei în cadrul UE, fără a ține seama de granițele naționale, și încearcă să prevină săvârșirea unor noi infracțiuni împotriva aceleiași victime.

12. OEP ar trebui emis, la cererea victimei din „statul (membru) emitent”, de către orice autoritate judiciară (sau echivalentă). Procesul constă în următoarele etape:

(a) „statul emitent” formulează o cerere pentru un OEP;

(b) la primirea OEP, „statul de executare” adoptă o hotărâre conform legii sale naționale pentru protejarea în continuare a persoanei vizate.

13. Pentru realizarea acestui obiectiv este necesară instituirea unor măsuri administrative. Parțial, aceste măsuri vor viza

schimbul de informații cu caracter personal între statele membre „emitente” și statele membre „de executare” în legătură cu persoana vizată („victima”) și persoana care reprezintă un pericol. Schimbul de date cu caracter personal este prevăzut în următoarele dispoziții:

(a) la articolul 6 se prevede că OEP însuși cuprinde mai multe informații cu caracter personal, după cum se specifică la punctele (a), (e), (f), (g) și (h) și în anexa I;

(b) obligațiile autorității competente din statul de executare prevăzute la articolul 8 alineatul (1) necesită prelucrarea datelor cu caracter personal, în special obligația de a notifica orice încălcare a măsurii de protecție [articolul 8 alineatul (1) litera (d) și anexa II];

(c) obligațiile autorității competente din statul membru de executare și statul membru emitent în caz de modificare, expirare sau revocare a ordinului de protecție și/sau a măsurilor de protecție (articolul 14).

14. Informațiile menționate la alineatul anterior se înscriu în mod clar în domeniul de aplicare a datelor cu caracter personal, definit pe larg în legislația privind protecția datelor drept „orice informații privind o persoană fizică identificată sau identificabilă”⁽¹⁵⁾ și explicat în continuare de Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal. Inițiativa OEP se referă la informațiile referitoare la o persoană fizică (victima sau persoana care reprezintă un pericol) sau informațiile folosite sau care ar putea fi folosite pentru a evalua, a trata într-un anumit mod sau a influența situația unei persoane (în special persoana care reprezintă un pericol)⁽¹⁶⁾.

II.3. Inițiativa OEA

15. Inițiativa OEA – care se bazează pe articolul 82 alineatul (1) litera (a) din Tratatul privind funcționarea Uniunii Europene – impune statelor membre să colecteze, să stocheze și să transmită probe chiar dacă acest lucru nu este încă disponibil în jurisdicția națională. Prin urmare, inițiativa depășește principiul disponibilității prezentat în Programul de la Haga din 2004 ca abordare inovatoare pentru

⁽¹⁵⁾ A se vedea articolul 2 litera (a) din Decizia-cadru 2008/977/JAI a Consiliului privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală, precum și articolul 2 litera (a) din Directiva 95/46/CE și articolul 2 litera (a) din Regulamentul (CE) nr. 45/2001.

⁽¹⁶⁾ A se vedea Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, Avizul 4/2007 privind conceptul de date cu caracter personal, GL 136, adoptat la 20 iunie 2007, p. 10.

schimbul transfrontalier de informații privind aplicarea legii⁽¹⁷⁾. De asemenea, inițiativa depășește Decizia-cadru 2008/978/JAI din 18 decembrie 2008 privind mandatul european de obținere a probelor, care este aplicabilă doar pentru probe (date) care există deja⁽¹⁸⁾.

16. OEA trebuie emis pentru aplicarea uneia sau mai multor măsuri de anchetă specifice, în statul de executare, în vederea obținerii de probe (care probabil nu există în momentul emiterii ordinului) și transferului acestora (articolul 12). OEA se aplică aproape tuturor măsurilor de anchetă (a se vedea considerentele 6 și 7 ale inițiativei).
17. Obiectivul inițiativei OEA este de a crea un instrument unic, eficient și flexibil pentru a obține probe aflate într-un alt stat membru în cadrul procedurilor penale, în locul unui instrument juridic mai complex folosit în prezent de autoritățile judiciare (pe baza asistenței judiciare reciproce, pe de o parte, și a recunoașterii reciproce, pe de altă parte)⁽¹⁹⁾.
18. În mod clar, probele colectate prin intermediul unui OEA (a se vedea și anexa A la inițiativă) pot conține date cu caracter personal, după cum este cazul informațiilor privind conturile bancare (articolul 23), al informațiilor privind tranzacțiile bancare (articolul 24) și al monitorizării tranzacțiilor bancare (articolul 25), sau ar putea să includă comunicarea datelor cu caracter personal (așa cum se întâmplă în cazul videoconferințelor sau teleconferințelor prevăzute la articolele 21 și 22).
19. Din aceste motive, inițiativa OEA are un impact semnificativ asupra dreptului la protecția datelor cu caracter personal. Ținând seama, de asemenea, că data pentru punerea în aplicare a Deciziei-cadru 2008/978/JAI nu a expirat încă (și prin urmare este dificil de evaluat eficiența instrumentului și necesitatea unor măsuri juridice suplimentare)⁽²⁰⁾, AEPD reamintește necesitatea unei verificări

⁽¹⁷⁾ Principiul consacrat în Programul de la Haga. Consolidarea libertății, securității și justiției în Uniunea Europeană, punctul 2.1, înseamnă „că, pe întregul teritoriu al Uniunii, un oficial însărcinat cu aplicarea legii dintr-un stat membru care are nevoie de anumite informații pentru a-și îndeplini obligațiile poate obține respectivele informații dintr-un alt stat membru, iar agenția de aplicare a legii din celălalt stat membru care deține informațiile trebuie să i le pună la dispoziție în scopul declarat, ținând seama de cerința anchetelor în curs din statul respectiv”. În această privință, a se vedea Avizul AEPD privind propunerea de decizie a Consiliului privind schimbul de informații conform principiului disponibilității [COM(2005) 490 final], JO C 116, 17.5.2006, p. 8.

⁽¹⁸⁾ Decizia-cadru 2008/978/JAI a Consiliului din 18 decembrie 2008 privind mandatul european de obținere a probelor în scopul obținerii de obiecte, documente și date în vederea utilizării acestora în cadrul procedurilor în materie penală, JO L 350, 30.12.2008, p. 72.

⁽¹⁹⁾ În prezent există două instrumente de recunoaștere reciprocă aplicabile obținerii probelor: Decizia-cadru 2003/577/JAI a Consiliului din 22 iulie 2003 privind executarea în Uniunea Europeană a ordinelor de înghețare a bunurilor sau a probelor (JO L 196, 2.8.2003, p. 45) și Decizia-cadru 2008/978/JAI, citată la nota de subsol 18.

⁽²⁰⁾ Articolul 23 alineatul (1) din Decizia-cadru 2008/978/JAI prevede că „Statele membre adoptă măsurile necesare pentru a se conforma dispozițiilor prezentei decizii-cadru până la 19 ianuarie 2011”.

periodice, ținând seama de principiile de protecție a datelor, a eficienței și proporționalității măsurilor juridice adoptate în SLSJ⁽²¹⁾. Prin urmare, AEPD recomandă adăugarea la inițiativa OEA a unei clauze privind evaluarea prin care să li se impună statelor membre să raporteze în mod regulat cu privire la aplicarea instrumentului, iar Comisiei să sintetizeze aceste rapoarte și, dacă este cazul, să formuleze propuneri de modificare corespunzătoare.

II.4. Prelucrarea datelor cu caracter personal prevăzută în inițiativele OEA și OEP

20. După cum s-a explicat mai sus la punctele 13, 14 și 18, este clar că, în temeiul directivelor propuse, datele cu caracter personal vor fi prelucrate și vor face obiectul schimbului între autoritățile competente din diferitele state membre. În această situație, persoana vizată este protejată prin dreptul fundamental la protecția datelor, recunoscut la articolul 16 din Tratatul privind funcționarea Uniunii Europene și la articolul 8 din Carta drepturilor fundamentale a Uniunii Europene.
 21. În ciuda acestui fapt, în „Declarația detaliată” care însoțește inițiativa OEP, „riscul de a aduce atingere drepturilor fundamentale” este identificat ca fiind egal cu „0” (zero)⁽²²⁾, iar în analiza de impact cuprinsă în „Declarația detaliată” care însoțește inițiativa EIO, aspectele legate de protecția datelor nu sunt luate în considerare⁽²³⁾.
 22. AEPD regretă aceste concluzii și subliniază importanța protecției datelor în contextele speciale în care sunt prelucrate date cu caracter personal, respectiv:
 - (a) domeniul vast al cooperării judiciare în materie penală;
 - (b) datele sunt adesea sensibile și de obicei sunt obținute de către autoritățile polițienești și judiciare ca urmare a unei anchete;
 - (c) conținutul posibil al datelor, în special în legătură cu inițiativa OEA, care ar trebui să se extindă la orice tip de probe; și
- ⁽²¹⁾ De asemenea, punctul 1.2.3 din Programul de la Stockholm impune ca inițiativele legislative noi să fie înaintate după verificarea respectării principiului proporționalității.
- ⁽²²⁾ Declarația detaliată care permite evaluarea conformității cu principiul subsidiarității și al proporționalității în conformitate cu articolul 5 din Protocolul (nr. 2) la Tratatul de la Lisabona din 6 ianuarie 2010.
- ⁽²³⁾ Declarația detaliată din 23 iunie 2010, Dosarul interinstituțional: 2010/0817 (COD) se referă în mod explicit doar la dreptul la libertate și securitate și la dreptul la o bună administrare (a se vedea p. 25 și p. 41).

- (d) posibila comunicare a probelor în afara UE, în conformitate cu articolul 13 din Decizia-cadru 2008/977/JAI privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală ⁽²⁴⁾.
23. În acest context, operațiunile de prelucrare a datelor au un impact deosebit și ar putea afecta semnificativ drepturile fundamentale ale persoanei vizate, inclusiv dreptul la protecția datelor cu caracter personal.
24. Ținând seama de aspectele de mai sus, AEPD se întreabă de ce inițiativele nici nu abordează protecția datelor cu caracter personal (în afara faptului că se referă la obligațiile de confidențialitate impuse actorilor implicați într-o anchetă prin articolul 18 din inițiativa OEA), nici nu fac trimitere în mod explicit la Decizia-cadru 2008/977/JAI. Într-adevăr, această decizie-cadru ar fi aplicabilă operațiunilor de prelucrate avute în vedere în cele două inițiative [a se vedea articolul 1 alineatul (2) litera (a)].
25. Din acest motiv, AEPD salută faptul că în timpul activităților pregătitoare din cadrul Consiliului în legătură cu inițiativa OEP a fost introdusă o trimitere la Decizia-cadru 2008/977/JAI ⁽²⁵⁾ și are încredere că Parlamentul European va confirma această modificare a inițiativelor originale ⁽²⁶⁾.
26. AEPD regretă faptul că un considerent similar nu a fost încă introdus și în inițiativa OEA, care implică un schimb mult mai intens de date cu caracter personal. În acest context, AEPD salută sugestia făcută de Comisia Europeană, comentând asupra inițiativei OEA, că ar trebui introdusă o trimitere (atât în considerente, cât și în corpul propunerii) la aplicabilitatea Deciziei-cadru 2008/977/JAI ⁽²⁷⁾.

⁽²⁴⁾ În plus: Decizia-cadru 2008/977/JAI.

⁽²⁵⁾ A se vedea considerentul 27 din ultimul proiect al inițiativei OEP (28 mai 2010, documentul Consiliului nr. 10384/2010): „Datele cu caracter personal prelucrate în cadrul punerii în aplicare a prezentei decizii-cadru ar trebui să fie protejate în conformitate cu 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 și în conformitate cu principiile stabilite în Convenția Consiliului Europei din 28 ianuarie 1981 pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, pe care toate statele membre au ratificat-o”.

⁽²⁶⁾ În acest sens, a se vedea amendamentul 21 inclus în proiectul de raport referitor la inițiativa pentru o directivă a Parlamentului European și a Consiliului privind ordinul european de protecție [00002/2010 – C7-0006/2010 – 2010/0802(COD)], 20.5.2010, Comisia pentru libertăți civile, justiție și afaceri interne – Comisia pentru drepturile femeii și egalitatea între sexe, Raportori: Teresa Jiménez-Becerril Barrio, Carmen Romero López, la http://www.europarl.europa.eu/meetdocs/2009_2014/documents/femm/prj/817/817530/817530ro.pdf

⁽²⁷⁾ A se vedea comentariile Comisiei privind ordinul european de anchetă în materie penală, 24.8.2010, JUST/B/1/AA-et D(2010) 6815, p. 9 și 38, la http://ec.europa.eu/justice/news/intro/doc/comment_2010_08_24_en.pdf

27. Prin urmare și fără a aduce atingere secțiunii III de mai jos, ambele inițiative ar trebui să includă o dispoziție specifică menită să clarifice că Decizia-cadru 2008/977/JAI se aplică prelucrării de date prevăzute în inițiative.

III. NORME SPECIFICE NECESARE ÎN VEDEREA COOPERĂRII JUDICIARE ÎN MATERIE PENALĂ, ÎN PLUS FAȚĂ DE CADRUL JURIDIC PENTRU PROTECȚIA DATELOR EXISTENT

28. Ambele inițiative ridică din nou problema fundamentală a aplicării incomplete și inconsecvente a principiilor privind protecția datelor în domeniul cooperării judiciare în materie penală ⁽²⁸⁾.
29. AEPD este conștientă de importanța îmbunătățirii eficienței cooperării judiciare între statele membre și în domeniile reglementate de inițiativele OEP și OEA ⁽²⁹⁾. În plus, AEPD înțelege avantajele și nevoia de punere în comun a informațiilor, însă dorește să sublinieze că prelucrarea acestor date trebuie să fie în conformitate – *inter alia* ⁽³⁰⁾ – cu normele UE privind protecția datelor. Acest aspect este și mai evident ținând seama de Tratatul de la Lisabona, care introduce articolul 16 din Tratatul privind funcționarea Uniunii Europene și conferă caracter obligatoriu articolului 8 din Carta Drepturilor Fundamentale a Uniunii Europene.
30. Situațiile care implică schimbul transfrontalier de informații în cadrul UE merită o atenție specială întrucât prelucrarea datelor cu caracter personal în mai multe jurisdicții sporește riscurile la adresa drepturilor și intereselor persoanelor fizice implicate. Datele cu caracter personal vor fi prelucrate în mai multe jurisdicții în care cerințele legale, precum și cadrul tehnic, nu sunt neapărat aceleași.
31. În plus, acest lucru generează incertitudinea juridică a persoanelor vizate: pot fi implicate părți din alte state membre, s-ar putea aplica legile naționale ale diverselor state membre, care ar putea fi diferite de legile cu care sunt obișnuite persoanele vizate sau s-ar putea aplica într-un sistem juridic care nu îi este familiar persoanei vizate. De aceea sunt necesare eforturi mai intense pentru a asigura conformitatea cu cerințele ce rezultă din legislația UE privind protecția datelor ⁽³¹⁾.

⁽²⁸⁾ A se vedea și secțiunea V din aviz.

⁽²⁹⁾ A se vedea, *inter alia*, aprobarea nevoii de a îmbunătăți accesul la justiție, cooperarea între autoritățile judiciare europene și eficiența sistemului judiciar în sine în Avizul AEPD „Către o strategie europeană în domeniul e-justiției”, JO C 128, 6.6.2009, p. 13, punctele 9 și 21.

⁽³⁰⁾ În legătură cu aspectul privind respectarea normelor procedurale penale din statele membre, în special în domeniul Propunerii OEA, se poate face trimitere la considerațiile și îngrijorările exprimate în răspunsurile transmise Comisiei Europene în timpul consultării publice asupra Cărții verzi (a se vedea notele de subsol 11 și 12).

⁽³¹⁾ A se vedea, de asemenea, Consiliul, Programul de la Haga: Consolidarea libertății, a securității și a justiției în Uniunea Europeană (2005/C 53/01), JO C 53, 3.3.2005, p. 1, 7 și următoarele.

32. Din punctul de vedere al AEPD, clarificarea aplicabilității Deciziei-cadru 2008/977/JAI, astfel cum a fost propusă la punctul 27, reprezintă doar o primă etapă.
33. Provocările specifice pentru asigurarea unei protecții eficiente în domeniul cooperării judiciare în materie penală, coroborate cu Decizia-cadru 2008/977/JAI care nu este pe deplin satisfăcătoare (a se vedea punctele 52-56) ar putea necesita introducerea unor dispoziții specifice privind protecția datelor atunci când instrumentele juridice specifice ale UE impun schimbul de date cu caracter personal.

IV. PROVOCĂRI PENTRU PROTECȚIA EFICIENTĂ A DATELOR ÎN CADRUL COOPERĂRII ÎN MATERIE PENALĂ: RECOMANDĂRI PRIVIND INIȚIATIVELE OEP ȘI OEA

IV.1. Observații introductive

34. Protecția eficientă a datelor cu caracter personal (după cum se subliniază la punctul 29) nu este importantă doar pentru persoanele vizate, ci contribuie și la succesul cooperării judiciare. În realitate, disponibilitatea de a schimba astfel de date cu autoritățile altor state membre va fi mai mare dacă o autoritate este asigurată de nivelul de protecție, acuratețe și fiabilitate a datelor cu caracter personal din celălalt stat membru⁽³²⁾. Pe scurt, stabilirea unui standard comun (ridicat) pentru protecția datelor în acest domeniu sensibil va promova încrederea reciprocă între statele membre și va consolida cooperarea judiciară pe baza recunoașterii reciproce, îmbunătățind calitatea datelor în cadrul schimbului de informații.
35. În acest context specific, AEPD recomandă includerea unor garanții specifice pentru protecția datelor în cadrul inițiativelor OEP și OEA, pe lângă trimiterea generală la Decizia-cadru 2008/977/JAI (propusă la alineatul 27).
36. Unele dintre aceste garanții au o natură mai generală și trebuie să fie incluse în ambele inițiative, în special garanțiile care au ca scop îmbunătățirea acurateței datelor, precum și a securității și confidențialității. Alte garanții se referă la dispozițiile specifice incluse fie în inițiativa OEP, fie în inițiativa OEA.

IV.2. Garanții mai generale

Acuratețea

37. În situațiile prevăzute de inițiative în care datele fac obiectul schimbului între statele membre, ar trebui să se pună un

⁽³²⁾ A se vedea Avizul AEPD privind propunerea pentru o decizie-cadru a Consiliului privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală [COM(2005) 475 final], JO C 47, 25.2.2006, p. 27, punctele 5-7.

accent specific asupra asigurării acurateței informațiilor. În această privință, AEPD salută faptul că inițiativa OEP prevede la articolul 14 obligații clare pentru autoritatea competentă din statul emitent de informare a autorității competente din statul de executare cu privire la orice modificare sau la expirarea sau revocarea ordinului de protecție.

38. AEPD ia notă, de asemenea, de faptul că necesitatea asigurării traducerilor ar putea afecta acuratețea informațiilor, în special din cauza faptului că inițiativele se referă la instrumente juridice specifice care ar putea avea un înțeles diferit în diferite limbi și în sisteme juridice diferite. În acest context, deși salută faptul că inițiativa OEP abordează problema traducerilor (articolul 16), AEPD propune includerea unei dispoziții similare și în cadrul inițiativei OEA.

Securitate, conștientizare și răspundere

39. Intensificarea cooperării transfrontaliere care ar putea rezulta în urma adoptării celor două inițiative presupune o analiză atentă a aspectelor de securitate ale transmiterii transfrontaliere a datelor cu caracter personal în legătură cu executarea unor OEP sau OEA⁽³³⁾. Acest lucru este necesar nu doar pentru respectarea standardelor de securitate ale prelucrării datelor cu caracter personal impuse prin articolul 22 din Decizia-cadru 2008/977/JAI, ci și pentru asigurarea caracterului secret al anchetelor și a confidențialității procedurilor penale în cauză, care este reglementată de articolul 18 din inițiativa OEA și, ca regulă generală în ceea ce privește datele cu caracter personal rezultate din schimbul transfrontalier, de articolul 21 din Decizia-cadru 2008/977/JAI.
40. AEPD subliniază necesitatea unor sisteme de telecomunicații sigure în cadrul procedurilor de transmitere. Prin urmare, AEPD salută dispoziția privind utilizarea Rețelei Judiciare Europene⁽³⁴⁾ ca instrument pentru a asigura prezentarea corectă a OEP și OEA autorităților naționale competente, prevenind sau minimizând astfel riscul implicării unor autorități necorespunzătoare în schimbul de date cu caracter personal [a se vedea articolul 7 alineatele (2) și (3) din inițiativa OEP și articolul 6 alineatele (3) și (4) din inițiativa OEA].

41. Prin urmare, inițiativele ar trebui să includă dispoziții care să impună statelor membre să se asigure că:

⁽³³⁾ Pentru aspecte mai generale, a se vedea Comunicarea Comisiei către Consiliu, Parlamentul European și Comitetul Economic și Social European, Către o strategie europeană în domeniul e-justiției, Bruxelles, 30.5.2008, COM(2008)329 final, p. 8: „Autoritățile judiciare trebuie să poată realiza schimbul de date confidențiale în deplină securitate”.

⁽³⁴⁾ Decizia 2008/976/JAI a Consiliului din 16 decembrie 2008 privind Rețeaua Judiciară Europeană (JO L 348, 24.12.2008, p. 130).

- (a) autoritățile competente dispun de resurse adecvate pentru aplicarea directivelor propuse;
- (b) funcționarii competenți respectă standardele profesionale și sunt supuși unor proceduri interne corespunzătoare care asigură, în special, protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, echitatea procedurilor și respectarea corespunzătoare a dispozițiilor privind confidențialitatea și secretul profesional (incluse la articolul 18 din inițiativa OEA).
42. În plus, AEPD recomandă introducerea unor dispoziții care să asigure respectarea principiilor materiale de protecție a datelor în cazul prelucrării datelor cu caracter personal și existența mecanismelor interne necesare pentru a demonstra conformitatea față de părțile interesate externe. Aceste dispoziții ar putea fi instrumentele necesare pentru a trage la răspundere operatorii de date [conform „principiului responsabilității”, care este discutat în contextul revizuirii actuale a cadrului pentru protecția datelor ⁽³⁵⁾]. AEPD le cere acestora să ia măsurile necesare pentru asigurarea conformității. Aceste dispoziții ar trebui să includă:
- (a) sistemele de autentificare care permit doar persoanelor autorizate să aibă acces la ambele baze de date ce conțin date cu caracter personal sau la locațiile în care se află probe;
- (b) urmărirea accesărilor datelor cu caracter personal și a operațiunilor efectuate în legătură cu aceste date;
- (c) punerea în aplicare a controlului de audit.

IV.3. Garanții în cadrul inițiativei OEA

43. Ținând seama de caracteristicile deosebit de intruzive ale anumitor măsuri de anchetă, AEPD invită la un proces de reflecție aprofundat asupra admisibilității probelor colectate în alte scopuri decât prevenirea, anchetarea, depistarea sau urmărirea infracțiunilor sau aplicarea sancțiunilor penale și exercitarea dreptului la apărare. Ar trebui să se țină seama în mod deosebit de utilizarea probelor obținute în baza articolului 11 alineatul (1) litera (d) din Decizia-cadru 2008/977/JAI ⁽³⁶⁾.

⁽³⁵⁾ A se vedea Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal și Grupul de lucru pentru poliție și justiție, Viitorul confidențialității, p. 20 și următoarele.

⁽³⁶⁾ Această dispoziție recunoaște utilizarea probelor și în „orice alt scop doar cu consimțământul prealabil al statului membru care transmite sau cu consimțământul persoanei vizate, în conformitate cu legislația națională”.

44. Prin urmare, în inițiativa OEA ar trebui inclusă o excepție de la aplicarea dispoziției cuprinse în articolul 11 alineatul (1) litera (d), care să prevadă faptul că dovezile colectate în baza OEA nu pot fi folosite în alte scopuri decât prevenirea, anchetarea, depistarea sau urmărirea infracțiunilor sau aplicarea sancțiunilor penale și exercitarea dreptului la apărare.

IV.4. Garanții în cadrul inițiativei OEP

45. În legătură cu inițiativa OEP, AEPD recunoaște că datele cu caracter personal care fac obiectul schimbului între autoritățile competente și care sunt enumerate în anexa I la inițiativă (atât în legătură cu victima, cât și cu persoana care reprezintă un pericol) sunt adecvate, relevante și nu sunt excesive în raport cu scopul pentru care sunt colectate și prelucrate ulterior.
46. Cu toate acestea, din inițiativă – în special din articolul 8 alineatul (1) litera (b) – nu reiese suficient de clar ce date cu caracter personal privind victima vor fi comunicate persoanei care reprezintă un pericol de către autoritatea competentă a statului de executare.
47. AEPD consideră că este adecvat să se ia în considerare împrejurările și conținutul măsurilor de protecție formulate de către autoritatea judiciară din statul membru emitent înainte de a informa persoana care reprezintă un pericol. Prin urmare, aceasta din urmă ar trebui să primească doar acele informații cu caracter personal ale victimei (care ar putea include, în anumite cazuri, și datele de contact) care sunt strict relevante pentru executarea deplină a măsurii de protecție.
48. AEPD este conștientă de faptul că furnizarea informațiilor de contact (de exemplu numere de telefon, adresa victimei, precum și alte locuri frecventate de obicei, precum locul de muncă sau școala copiilor) poate, de fapt, să pună în pericol sănătatea fizică și psihică a victimei, precum și dreptul acesteia la viață privată și la protecția datelor cu caracter personal. Pe de altă parte, indicarea adreselor relevante poate fi necesară în unele cazuri pentru a preveni persoana care reprezintă un pericol asupra locurilor în care îi este interzis să se deplaseze. Această măsură are ca scop asigurarea respectării ordinului și prevenirea potențialelor sancțiuni pentru încălcarea acestuia. În plus, în funcție de împrejurări, identificarea locului (locurilor) în care persoanei care reprezintă un pericol îi este interzis să se deplaseze poate fi necesară pentru a nu limita inutil libertatea de mișcare a acesteia.

49. Ținând seama de aceste aspecte, AEPD subliniază importanța acestui subiect și recomandă ca inițiativa OEP să precizeze în mod clar că, în funcție de împrejurările cazului, persoanei care reprezintă un pericol ar trebui să i se transmită doar acele date cu caracter personal ale

victimei (care pot include, în unele cazuri, și datele de contact) care sunt strict relevante pentru exercitarea deplină a măsurii de protecție⁽³⁷⁾.

50. În sfârșit, AEPD solicită clarificarea expresiei „mijloace electronice” incluse la considerentul 10 al inițiativei OEP. Ar trebui să se explice, în special, dacă datele cu caracter personal sunt prelucrate folosind „mijloace electronice” și, în acest caz, ce garanții sunt puse la dispoziție.

V. NORME PRIVIND PROTECȚIA DATELOR ȘI COOPERAREA JUDICIARĂ ÎN MATERIE PENALĂ: ÎNGRIJORĂRI LEGATE DE INIȚIATIVELE OEP ȘI OEA

51. Decizia-cadru 2008/977/JAI se aplică tuturor schimburilor de date cu caracter personal din cadrul inițiativelor OEP și OEA.

52. Deși AEPD a recunoscut că Decizia-cadru 2008/977/JAI – atunci când este aplicată de către statele membre – reprezintă un pas important către protecția datelor în cadrul cooperării polițienești și judiciare⁽³⁸⁾, decizia-cadru în sine nu este pe deplin satisfăcătoare⁽³⁹⁾. Principala îngrijorare rămasă nerezolvată se referă la sfera limitată de aplicare a acesteia. Decizia-cadru se limitează la schimburile de date cu caracter personal din domeniul cooperării polițienești și judiciare între autoritățile și sistemele din diferite state membre și de la nivelul Uniunii Europene⁽⁴⁰⁾.

53. Chiar dacă această îngrijorare nu poate fi soluționată în contextul inițiativelor OEP și OEA, AEPD insistă asupra evidențierii faptului că absența unui standard comun (ridicat) de protecție a datelor în cadrul cooperării judiciare ar putea să implice că, atunci când instrumentează un dosar penal cuprinzând informații care provin din alte state membre (inclusiv, de exemplu, probe colectate pe baza unui OEA), o autoritate judiciară de la nivel național sau al UE ar fi nevoită să aplice norme diferite de prelucrare a datelor: normele naționale autonome (care trebuie să

respecte Convenția nr. 108 a Consiliului Europei) pentru datele care provin din statul membru respectiv și normele de aplicare a Deciziei-cadru 2008/977/JAI pentru datele care provin din alte state membre. Astfel, „informații” diferite s-ar putea încadra în regimuri juridice diferite.

54. Consecințele aplicării unui standard „dublu” de protecție a datelor pentru fiecare dosar penal cu elemente transfrontaliere sunt relevante în practica de fiecare zi (de exemplu, păstrarea informațiilor prevăzute de legile aplicabile ale fiecăruia dintre organismele care transmit date; restricții de prelucrare suplimentară cerute de fiecare organism care transmite date; în cazul unei cereri din partea unei țări terțe, fiecare organism care transmite date și-a da acordul în conformitate cu propria evaluare a adecvării și/sau cu angajamentele internaționale; și diferențele în ceea ce privește reglementarea dreptului de acces de către persoana vizată). În plus, protecția și drepturile cetățenilor ar putea varia și pot fi supuse unor derogări ample diferite în funcție de statul membru în care are loc prelucrarea⁽⁴¹⁾.

55. Prin urmare, AEPD profită de această ocazie pentru a reitera opiniile sale privind necesitatea unui cadru juridic cuprinzător pentru protecția datelor care să cuprindă toate competențele UE, inclusiv poliția și justiția, și care să se aplice atât datelor cu caracter personal transmise sau puse la dispoziție de către autoritățile competente ale altor state membre, cât și prelucrărilor interne din SLSJ⁽⁴²⁾.

56. În final, AEPD observă că normele de protecție a datelor ar trebui să se aplice tuturor sectoarelor și utilizării datelor în toate scopurile⁽⁴³⁾. Desigur, ar trebui să fie posibile excepții justificate în mod legal și formulate cu claritate, în special în ceea ce privește datele cu caracter personal prelucrate în scopul aplicării legii⁽⁴⁴⁾. Lacunele în protecția datelor cu caracter personal contravin cadrului juridic curent (reinnoit) al Uniunii Europene. Articolul 3 alineatul (2) din Directiva 95/46/CE – care exclude din domeniul de aplicare al

⁽³⁷⁾ Acesta pare a fi sensul amendamentelor 13 și 55 la Proiectul de raport referitor la inițiativa pentru o directivă a Parlamentului European și a Consiliului privind ordinul european de protecție [00002/2010 – C7-0006/2010 – 2010/0802(COD)], 20.5.2010, Comisia pentru libertăți civile, justiție și afaceri interne – Comisia pentru drepturile femeii și egalitatea de gen.

⁽³⁸⁾ A se vedea Avizul AEPD privind Comunicarea Comisiei către Parlamentul European, Consiliul și Comitetul Economic și Social European „Către o strategie europeană în domeniul e-justiției” (2009/C 128/02), JO C 128, 6.6.2009, p. 13, punctul 17.

⁽³⁹⁾ A se vedea cele trei avize AEPD referitoare la propunerea de decizie-cadru a Consiliului privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală [COM(2005) 475 final], JO C 47, 25.2.2006, p. 27, JO C 91, 26.4.2007, p. 9, JO C 139, 23.6.2007, p. 1. A se vedea și Avizul AEPD privind Comunicarea Comisiei către Parlamentul European și Consiliul „Un spațiu de libertate, securitate și justiție în serviciul cetățenilor”, JO C 276, 17.11.2009, p. 8, punctele 19, 29 și 30.

⁽⁴⁰⁾ A se vedea articolul 2 din Decizia-cadru 2008/977/JAI.

⁽⁴¹⁾ A se vedea al treilea Aviz AEPD privind propunerea de decizie-cadru a Consiliului privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală (JO C 139, 23.6.2007, p. 41), menționat la nota de subsol 39, punctul 46.

⁽⁴²⁾ Această poziție a AEPD este susținută în mod clar de Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal și Grupul de lucru pentru poliție și justiție, Viitorul confidențialității. Contribuție comună la Consultarea Comisiei Europene privind cadrul legal pentru dreptul fundamental la protecția datelor cu caracter personal, GL 168, adoptată la 1 decembrie 2009, p. 4, p. 7 și următoarele și 24 și următoarele.

⁽⁴³⁾ A se vedea Comunicarea Comisiei către Parlamentul European și Consiliul, „Un spațiu de libertate, securitate și justiție în serviciul cetățenilor”, Bruxelles, 10.6.2009, COM(2009) 262 final, p. 30: „Uniunea trebuie să se echipeze cu un regim complet de protejare a datelor personale, care să cuprindă ansamblul competențelor Uniunii”.

⁽⁴⁴⁾ O astfel de abordare ar corespunde și scopului Declarației 21 anexate la Tratatul de la Lisabona privind protecția datelor cu caracter personal în domeniul cooperării judiciare în materie penală și al cooperării polițienești.

directivei cooperarea polițienească și judiciară – nu corespunde filozofiei cuprinse la articolul 16 din Tratatul privind înființarea Uniunii Europene. În plus, aceste lacune nu sunt acoperite într-o măsură suficientă de Convenția nr. 108 a Consiliului Europei ⁽⁴⁵⁾, pe care toate statele membre sunt obligate să o respecte.

VI. CONCLUZII ȘI RECOMANDĂRI

57. În privința ambelor inițiative, OEP și OEA, AEPD recomandă:

- includerea unor dispoziții specifice care să prevadă că instrumentele se aplică fără a aduce atingere Deciziei-cadru 2008/977/JAI a Consiliului din 27 noiembrie 2008 privind protecția datelor cu caracter personal în cadrul cooperării polițienești și judiciare în materie penală;
- includerea unor dispoziții care impun statelor membre să se asigure că:
 - autoritățile competente dispun de resursele necesare pentru aplicarea directivelor propuse;
 - funcționarii competenți respectă standardele profesionale și sunt supuși unor proceduri interne corespunzătoare care asigură în special protecția persoanelor în legătură cu prelucrarea datelor cu caracter personal, echitatea procedurilor și respectarea corespunzătoare a dispozițiilor privind confidențialitatea și secretul profesional;
 - sistemele de autentificare permit doar persoanelor autorizate să aibă acces la ambele baze de date ce conțin date cu caracter personal sau locațiile în care se află probe;
 - se monitorizează accesările și modul în care se desfășoară operațiunile;
 - sunt puse în aplicare controale de audit.

58. În privința inițiativei OEP, AEPD recomandă:

- să se precizeze în mod clar că, în funcție de împrejurările cazului, persoanei care reprezintă un pericol ar trebui să i se transmită doar acele date cu caracter

personal ale victimei (care, în anumite cazuri, pot include și datele de contact) care sunt strict relevante pentru executarea deplină a măsurii de protecție;

- să fie clarificată expresia „mijloace electronice” cuprinsă în considerentul 10 al inițiativei OEP.

59. În ceea ce privește inițiativa OEA, AEPD recomandă:

- introducerea unei dispoziții privind traducerile, similară celei incluse la articolul 16 din inițiativa OEA;
- introducerea unei dispoziții care să împiedice utilizarea probelor în alte scopuri decât prevenirea, anchetarea, depistarea sau urmărirea infracțiunii sau aplicarea sancțiunilor penale și exercitarea dreptului de apărare, ca excepție de la articolul 11 alineatul (1) litera (d) din Decizia-cadru 2008/977/JAI;
- adăugarea la inițiativa OEA a unei clauze de evaluare, prin care statelor membre să li se impună să raporteze în mod regulat cu privire la aplicarea instrumentului, iar Comisiei să sintetizeze aceste rapoarte și, dacă este cazul, să formuleze propuneri corespunzătoare pentru modificări.

60. În plus și la nivel mai general, AEPD:

- recomandă Consiliului să stabilească o procedură în cadrul căreia să aibă loc consultarea AEPD, în cazul în care o inițiativă introdusă de statele membre este legată de prelucrarea datelor cu caracter personal;
- reiterează necesitatea unui cadru juridic cuprinzător pentru protecția datelor, care să reglementeze toate domeniile de competență ale UE, inclusiv poliția și justiția, care să se aplice atât datelor cu caracter personal transmise sau puse la dispoziție de către autoritățile competente ale altor state membre, cât și prelucrărilor interne în SLSJ.

Adoptat la Bruxelles, 5 octombrie 2010.

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor

⁽⁴⁵⁾ Convenția pentru protecția persoanelor fizice în privința prelucrării automate a datelor cu caracter personal a Consiliului Europei, 28 ianuarie 1981, nr. 108.