AVIZE

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR

Avizul Autorității Europene pentru Protecția Datelor privind Comunicarea Comisiei către Parlamentul European și Consiliu – „Politica UE de combatere a terorismului: principale realizări și viitoare provocări”

(2011/C 56/02)

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR,

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

având în vedere Carta drepturilor fundamentale a Uniunii Europene, în special articolele 7 și 8,

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

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

ADOPTĂ URMĂTORUL AVIZ:

I. INTRODUCERE

1. La 20 iulie 2010, Comisia a adoptat o Comunicare intitulată „Politica UE de combatere a terorismului: principale realizări și viitoare provocări” [3]. Comunicarea are ca scop furnizarea „elementelor-cheie ale unei evaluări politice a actualei Strategii UE de combatere a terorismului” și constituie, în același timp, un element al strategiei privind securitatea internă [4]. În comunicare sunt evaluate realizările anterioare și sunt trasate liniile politice și viitoarele provocări cu care se va confrunta politica UE de combatere a terorismului.

2. Multe dintre inițiativele menționate în comunicare au făcut deja obiectul unor avize sau observații specifice ale AEPD. Totuși, această comunicare prezintă o perspectivă de ansamblu a politicii, precum și orientări pe termen lung, ceea ce justifică un aviz specific al AEPD.

3. Prezentul aviz vizează astfel să contribuie la prezentarea unor opțiuni politice mai importante într-un domeniu în care utilizarea informațiilor cu caracter personal este o activitate în același timp esențială, foarte amplă și cu un caracter deosebit de sensibil.

4. Avizul nu prezintă observații cu privire la cea mai recentă comunicare a Comisiei în acest domeniu „Strategia de securitate internă a UE în acțiune: cinci pași către o Europă mai sigură”, adoptată la 22 noiembrie 2010 [5]. Această comunicare va fi analizată de AEPD în cadrul unui aviz separat, care va aborda încă o dată necesitatea existenței unor legături clare între diferitele documente.

5. În prezentul aviz, AEPD analizează diferitele elemente ale comunicării, formulând în același timp recomandări în vederea garantării dreptului fundamental la protecția datelor cu caracter personal în contextul politicii UE de combatere a terorismului, în special în momentul abordării viitoarelor provocări și al elaborării de noi orientări în materie de politică.

II. ANALIZA COMUNICĂRII ȘI ASPECTELE RELEVANTE PRIVIND PROTECȚIA DATELOR

6. Pornind de la structura strategiei UE de combatere a terorismului din 2005 [6], comunicarea analizează în primul rând patru componente strategice ale politicii UE de combatere a terorismului: prevenirea, protecția, urmărirea și reacția. Un capitol specific analizează apoi anumite aspecte orizontale, și anume respectarea drepturilor fundamentale, cooperarea internațională și finanțarea.

[1] JO L 281, 23.11.1995, p. 31.
[2] JO L 8, 12.1.2001, p. 1.
[3] COM(2010) 386 final.
[4] A se vedea pagina a doua a comunicării.
[5] COM(2010) 673 final.
[6] Doc. 14469/4/05 din 30 noiembrie 2005.

1. **Prevenire, protecție, urmărire, reacție și necesitatea încorporării principiilor privind protecția datelor**

7. „Prevenirea” cuprinde un număr mare de activități, variind de la prevenirea radicalizării și recrutării până la abordarea modului în care teroriștii utilizează Internetul. În acest context, comunicarea menționează printre principalele realizări Directiva-cadru a Consiliului privind combaterea terorismului, adoptată în 2002 ([1]) și modificată în 2008 ([2]).

8. „Protecția” persoanelor și a infrastructurii este, de asemenea, o temă foarte amplă, incluzând inițiative privind securitatea frontierelor, securitatea transporturilor, controlul precursorilor de explozibili, protejarea infrastructurii vitale și consolidarea lanțului de aprovizionare.

9. „Urmărirea” include colectarea de informații, cooperarea polițienească și judiciară și combaterea activităților teroriste și a finanțării acestora. Viitoarele provocări din acest sector sunt stabilirea unui cadru UE privind registrele cu numele pasagerilor ([3]), utilizarea articolului 75 din TFUE pentru dezvoltarea unui cadru privind înghețarea fondurilor și activelor financiare, precum și pentru recunoașterea reciprocă în obținerea probelor în cazurile penale.

10. „Reacția” se referă la capacitatea de a gestiona urmările unui atac terorist și include asistența acordată victimelor terorismului.

11. Toate aceste domenii prezintă legături puternice cu inițiativele cu privire la care AEPD și-a exprimat deja o poziție: programul de la Stockholm, măsurile restrictive și înghețarea bunurilor, reținerea datelor, scannerele de securitate, precursorii de arme, identificarea biometrică, decizia de la Prüm, registrele cu numele pasagerilor, acordul TFTP, sistemul de informații Schengen, sistemul de informații Visa, gestionarea integrată a frontierelor, strategia UE de gestionare a informațiilor și schimbul transfrontalier de probe.

12. Domeniul „prevenirii” și cel al „protecției” sunt cele mai sensibile din perspectiva protecției datelor, din mai multe motive.

13. În primul rând, aceste domenii sunt, prin definiție, bazate pe evaluări prospective ale riscurilor, care în cele mai multe cazuri determină o prelucrare preventivă și amplă a unor cantități foarte mari de informații cu caracter personal cu privire la cetățeni care nu sunt suspecți (cum ar fi, de exemplu, verificarea internetului, frontierele electronice și scannerele de securitate).

14. În al doilea rând, comunicarea are în vedere intensificarea parteneriatelor între autoritățile de aplicare a legii și întreprinderile private (precum furnizorii de servicii internet, instituțiile financiare și întreprinderile din domeniul transporturilor) în vederea comunicării reciproce a informațiilor relevante și, uneori, pentru „a delega” acestora din urmă anumite părți ale sarcinilor de aplicare a legii. Aceasta duce la sporirea utilizării de către autoritățile publice în sprijinul aplicării legii a datelor cu caracter personal, colectate de întreprinderi private în scopuri comerciale.

15. Multe dintre aceste inițiative au fost luate, de multe ori ca reacție rapidă la incidente teroriste, în absența unei analize aprofundate a posibilelor duplicări sau suprapuneri cu măsurile deja existente. În unele cazuri, chiar după mai mulți ani de la intrarea în vigoare, nu s-a stabilit încă în ce măsură invadarea vieții private a cetățenilor în urma acestor măsuri a fost cu adevărat necesară.

16. În plus, există probabilitatea ca utilizarea „cu caracter preventiv” a datelor cu caracter personal să ducă la discriminare. Analiza preventivă a informațiilor ar presupune colectarea și prelucrarea de date cu caracter personal în legătură cu categorii largi de persoane (de exemplu, toți pasagerii, toți utilizatorii internetului), indiferent de vreo suspiciune specifică referitoare la acestea. Analiza acestor date, în special dacă este cuplată cu tehnici de extragere a datelor – poate avea ca rezultat etichetarea unor persoane nevinovate drept suspecte deoarece profilul (vârsta, sexul, religia etc.) și/sau tiparele acestora (de exemplu, în ceea ce privește deplasările, utilizarea internetului etc.) corespund celor ale persoanelor care au sau sunt suspectate a avea legături cu terorismul. Prin urmare, în special în acest context, utilizarea ilegală sau neadecvată a informațiilor (uneori sensibile) cu caracter personal, cuplată cu puterile coercitive ample ale autorităților de aplicare a legii, poate duce la discriminarea și stigmatizarea unor persoane și/sau grupuri specifice de persoane.

17. Din această perspectivă, garantarea unui nivel al protecției datelor reprezintă și o modalitate de a contribui la combaterea rasismului, xenofobiei și discriminării ceea ce, potrivit comunicării, „poate contribui la prevenirea radicalizării și a recrutării în scopuri teroriste”.

2. **O abordare coerentă bazată pe principiul necesității**

18. O observație generală importantă se referă la necesitatea de a asigura consecvența și relațiile clare între toate comunicările și inițiativele în domeniul afacerilor interne și, în special în domeniul securității interne. De exemplu, chiar dacă strategia UE de combatere a terorismului este strâns legată de strategia de gestionare a informațiilor, strategia privind Carta drepturilor fundamentale și modelul european al schimburilor de informații, relațiile dintre toate aceste documente nu sunt abordate explicit și de

([1]) 2002/475/JAI (JO L 164, 22.6.2002, p. 3).
([2]) 2008/919/JAI (JO L 330, 9.12.2008, p. 21).
([3]) Astfel cum s-a anunțat și în planul de acțiune al Comisiei privind punerea în aplicare a programului de la Stockholm COM(2010) 171 final din 20 aprilie 2010.

manieră cuprinzătoare. Această problemă a devenit evidentă odată cu adoptarea, la 22 noiembrie 2010, a „Strategiei de securitate internă a UE în acțiune: cinci pași către o Europă mai sigură” ([1]).

19. Prin urmare, AEPD recomandă instituțiilor UE să se asigure că politicile și inițiativele în domeniul afacerilor interne și securității interne sunt concepute și puse în aplicare de așa manieră încât să asigure o abordare coerentă și legături clare între acestea, creând sinergii adecvate și pozitive și evitând duplicarea activităților și eforturilor.

20. AEPD recomandă, de asemenea, ca principiul necesității să fie analizat în mod explicit în fiecare propunere din acest domeniu. Aceasta ar trebui să se realizeze atât prin analizarea posibilelor suprapuneri cu instrumentele deja existente, cât și prin limitarea colectării și schimbului de date cu caracter personal la ceea ce este cu adevărat necesar pentru scopul urmărit.

21. De exemplu, în cazul Acordului cu SUA privind Programul de urmărire a finanțării activităților teroriste (TFTP II), AEPD a întrebat în ce măsură acordul era cu adevărat necesar în vederea obținerii rezultatelor care s-ar fi putut obține prin utilizarea unor instrumente mai puțin invazive pentru viața privată, precum cele deja prevăzute de cadrul UE și internațional existent ([2]). În același aviz, AEPD a pus sub semnul întrebării necesitatea de a trimite date cu caracter personal în vrac în detrimentul unei modalități mai orientate.

22. Comunicarea menționează printre provocări „aceea de a asigura că aceste instrumente răspund unor nevoi reale (în materie de aplicare a legii) asigurând totodată respectarea deplină a dreptului la viață privată și a normelor privind protecția datelor”. AEPD salută această recunoaștere explicită și invită instituțiile UE să evalueze cu atenție în ce măsură instrumentele deja instituite, precum și cele avute în vedere răspund nevoilor reale în materie de aplicare a legii, evitând în același timp suprapunerea măsurilor sau restricțiile inutile ale vieții private. Din această perspectivă, instrumentele existente ar trebui să dovedească, în cadrul examinărilor periodice, că reprezintă mijloace eficace de combatere a terorismului.

23. AEPD a susținut în numeroase avize și observații nevoia ca toate instrumentele existente de schimb de informații să fie examinate înainte de a fi propuse altele noi, în special în recentul aviz cu privire la „Prezentarea generală asupra modului de gestionare a informațiilor în spațiul de libertate, securitate și justiție” ([3]). Într-adevăr, evaluarea eficacității măsurilor existente ținând seama în același timp de impactul noilor măsuri avute în vedere asupra vieții private este esențială și ar trebui să aibă un rol important în cadrul acțiunii Uniunii Europene în acest domeniu, în conformitate cu abordarea adoptată în programul de la Stockholm.

24. Suprapunerile și lipsa de eficacitate ar trebui să conducă la adaptări ale opțiunilor politice sau chiar la consolidarea sau eliminarea sistemelor existente de colectare și prelucrare a datelor.

25. AEPD recomandă acordarea unei atenții speciale propunerilor care au ca rezultat colectări generale de date cu caracter personal cu privire la toți cetățenii și nu doar cu privire la suspecți. Ar trebui să se analizeze și să se justifice în mod specific și acele cazuri în care prelucrarea datelor cu caracter personal este prevăzută în alte scopuri decât cele pentru care au fost colectate inițial, de exemplu în cazul accesului în scopuri legate de aplicarea legii la datele cu caracter personal stocate în sistemul Eurodac.

26. Comunicarea subliniază, de asemenea, că una dintre provocările viitoare va fi aceea de a elabora o politică eficace de cercetare în domeniul securității, ceea ce va contribui la un nivel ridicat de securitate. AEPD susține afirmația din comunicare, potrivit căreia cercetarea eficace în materie de securitate ar trebui să consolideze legăturile dintre diferiții actori. În această perspectivă, este vital ca expertiza în domeniul protecției datelor să fie integrată în cercetarea în domeniul securității în una dintre primele etape, astfel încât să ghideze opțiunile politice și să asigure încorporarea în cea mai mare măsură posibilă a confidențialității în noile tehnologii orientate către securitate, conform principiului „confidențialitate prin concept”.

3. **În privința utilizării măsurilor restrictive (înghețarea bunurilor)**

27. În ceea ce privește utilizarea măsurilor restrictive (înghețarea bunurilor) luate împotriva anumitor țări și persoane suspectate de terorism, jurisprudența Curții de Justiție a confirmat în mod repetat și consecvent că respectarea drepturilor fundamentale în combaterea terorismului este esențială în vederea asigurării atât a respectării drepturilor cetățenilor, cât și a legalității măsurilor luate.

28. AEPD și-a adus deja contribuția în acest domeniu, prin avize și observații ([4]), subliniind, pe de o parte, îmbunătățirile aduse procedurilor și solicitând, pe de altă parte, îmbunătățiri suplimentare, în special în privința dreptului

([1]) A se vedea punctul 4 al prezentului aviz.
([2]) Avizul AEPD din 22 iunie 2010.
([3]) Aviz AEPD din 30 septembrie 2010.

([4]) Avizul din 28 iulie 2009 privind propunerea de regulament al Consiliului de modificare a Regulamentului (CE) nr. 881/2002 de instituire a unor măsuri restrictive specifice împotriva anumitor persoane și entități care au legătură cu Osama ben Laden, cu rețeaua Al-Qaida și cu talibanii (JO C 276, 17.11.2009, p. 1). Avizul din 16 decembrie 2009 privind diverse propuneri legislative de impunere a unor măsuri restrictive în ceea ce privește Somalia, Zimbabwe, Republica Populară Democrată Coreeană și Guineea (JO C 73, 23.3.2010, p. 1). A se vedea, de asemenea, scrisoarea AEPD din 20 iulie 2010 privind trei propuneri legislative referitoare la anumite măsuri restrictive, respectiv referitoare la dl Milosevic și persoanele asociate cu acesta, în sprijinul mandatului Tribunalului Internațional pentru Fosta Iugoslavie și în ceea ce privește Eritreea. Toarte avizele și observațiile AEPD sunt disponibile pe site-ul internet al AEPD, http://www.AEPD.europa.eu

la informare și de acces la datele cu caracter personal, definirea clară a restricționării acestor drepturi și disponibilitatea căilor judiciare efective de atac și a supravegherii independente.

29. Necesitatea unor îmbunătățiri suplimentare ale procedurii și sistemelor de protecție disponibile persoanelor incluse pe o listă a fost recent confirmată de Tribunalul General în așa-numita cauză „Kadi II" ([1]). În special, Curtea a subliniat necesitatea ca persoanele incluse pe listă să fie informate în detaliu cu privire la motivele pentru care au fost incluse. Aceasta se apropie foarte mult de drepturile în temeiul legislației privind protecția datelor de a avea acces la propriile date cu caracter personal și de a putea dispune rectificarea acestora, în special atunci când sunt incorecte sau neactualizate. Aceste drepturi, menționate explicit de articolul 8 al Cartei drepturilor fundamentale, constituie elemente esențiale ale protecției datelor și ar putea face obiectul limitărilor doar în măsura în care aceste limitări sunt necesare, previzibile și stabilite prin lege.

30. În această perspectivă, AEPD împărtășește punctul de vedere adoptat în comunicare, potrivit căruia una dintre viitoarele provocări în domeniul politicii de combatere a terorismului va fi utilizarea articolului 75 din TFUE. Acest nou temei juridic, introdus de Tratatul de la Lisabona, permite în mod specific instituirea măsurilor de înghețare a bunurilor împotriva persoanelor fizice sau juridice. AEPD recomandă ca acest temei juridic să fie utilizat și pentru stabilirea unui cadru privind înghețarea bunurilor care să respecte pe deplin drepturile fundamentale. AEPD este dispusă să contribuie în continuare la dezvoltarea procedurilor și instrumentelor legislative relevante și așteaptă să fie consultată în mod corespunzător și din timp atunci când Comisia, în temeiul Programului său de lucru 2011, va elabora reglementări specifice în acest domeniu ([2]).

31. Într-o perspectivă mai largă, există necesitatea de a stabili un cadru pentru protecția datelor care să se aplice și politicii externe și de securitate comune. Într-adevăr, articolul 16 din TFUE oferă un temei juridic pentru stabilirea normelor de protecție a datelor și în domeniul politicii externe și de securitate comune. Temeiul juridic diferit și procedura prevăzută în articolul 39 din TUE se vor aplica doar atunci când datele cu caracter personal sunt prelucrate în acest domeniu de către statele membre. Cu toate acestea, chiar dacă Tratatul de la Lisabona solicită stabilirea acestor norme de protecție a datelor și oferă instrumentele de stabilire a acestora, în momentul de față nu este prevăzută nicio inițiativă în recenta Comunicare privind „O abordare globală a protecției datelor cu caracter personal în Uniunea Europeană" ([3]). În acest context, AEPD invită Comisia să prezinte o propunere de stabilire a unui cadru de protecție a datelor în domeniul politicii externe și de securitate comune.

([1]) Hotărârea din 30 septembrie 2010 în cauza T-85/09 *Kadi/Comisia*, a se vedea în special punctele 157 și 177.

([2]) Programul de lucru al Comisiei 2011 [COM(2010) 623 din 27 octombrie 2010] menționează în anexa II (Listă indicativă a posibilelor inițiative care sunt în curs de analizare) un „regulament de stabilire a unei proceduri pentru înghețarea fondurilor persoanelor suspectate de activități teroriste pe teritoriul UE".

([3]) Comunicarea Comisiei (2010) 609 din 4 noiembrie 2010.

4. **Respectarea drepturilor fundamentale și cooperarea internațională**

32. Capitolul dedicat respectării drepturilor fundamentale subliniază că UE ar trebui să aibă un comportament exemplar cu privire la Carta drepturilor fundamentale, care ar trebui să reprezinte busola tuturor politicilor UE. AEPD salută această abordare.

33. AEPD sprijină, de asemenea, afirmația că respectarea drepturilor fundamentale nu este doar o cerință legală, ci și o condiție esențială pentru încrederea reciprocă între autoritățile naționale și în rândul publicului în general.

34. În acest context, AEPD recomandă o abordare proactivă și acțiuni concrete pentru atingerea acestui obiectiv, precum și ca o modalitate de punere eficace în aplicare a Cartei drepturilor fundamentale a UE ([4]).

35. Evaluările privind impactul asupra vieții private (EIVP) și consultarea din timp a autorităților competente din domeniul protecției datelor ar trebui să fie asigurate pentru toate inițiativele care au un impact asupra protecției datelor cu caracter personal, indiferent de inițiatorul acestora și de domeniul în care sunt propuse.

36. În capitolul privind cooperarea internațională, Comunicarea subliniază și necesitatea creării „condițiilor juridice și ale cadrului politic necesare pentru o cooperare consolidată cu partenerii externi ai UE în domeniul combaterii terorismului".

37. În acest sens, AEPD reamintește nevoia de a asigura existența, în momentul schimburilor de date cu caracter personal cu țări terțe și organizații internaționale, a unor mecanisme adecvate de protecție în vederea asigurării respectării drepturilor cetățenilor privind protecția datelor și în contextul cooperării internaționale.

38. Aceasta include, de asemenea, promovarea protecției datelor în cooperare cu țările terțe și organizațiile internaționale, în vederea asigurării îndeplinirii standardelor UE. De asemenea, se asigură astfel compatibilitatea cu intenția Comisiei de a dezvolta standarde juridice și tehnice înalte ale protecției datelor în țările terțe și la nivel internațional și de a consolida cooperarea cu țările terțe ([5]).

([4]) A se vedea Comunicarea Comisiei (2010) 573 din 19 octombrie 2010 privind o Strategie pentru punerea în aplicare efectivă a Cartei drepturilor fundamentale de către Uniunea Europeană.

([5]) A se vedea Comunicarea (2010) 609 privind „O abordare globală a protecției datelor cu caracter personal în Uniunea Europeană", paginile 16 și 17.

39. O oportunitate clară pentru acțiunea Uniunii Europene în acest domeniu este oferită de măsurile restrictive (de înghețare a bunurilor), în cazul cărora cooperarea intensă cu țările terțe și cu Organizația Națiunilor Unite nu ar trebui să reducă nivelul ridicat de protecție a drepturilor fundamentale oferit de sistemul juridic al UE.

III. **CONCLUZII**

40. AEPD salută atenția acordată în comunicare drepturilor fundamentale și protecției datelor și recomandă continuarea îmbunătățirilor concrete în domeniul politicii de combatere a terorismului.

41. AEPD recomandă sprijinirea prin inițiative concrete a respectării drepturilor fundamentale în acest domeniu, în special a dreptului de protecție a datelor cu caracter personal, care reprezintă un sprijin necesar pentru promovarea certitudinii juridice, a încrederii și cooperării în domeniul combaterii terorismului, precum și o condiție legală necesară pentru dezvoltarea sistemelor avute în vedere.

42. AEPD sprijină, de asemenea, abordarea potrivit căreia în acest domeniu ar trebui să fie preferată elaborarea sistematică a politicilor elaborării politicilor în funcție de incidente, în special atunci când incidentele duc la crearea de noi sisteme de colectare și schimb de date fără o evaluare adecvată a alternativelor existente.

43. În această perspectivă, AEPD recomandă instituțiilor UE să se asigure că politicile și inițiativele din domeniul afacerilor interne și securității interne sunt concepute și puse în aplicare de așa manieră încât să asigure o abordare consecventă și legături clare între acestea, creând sinergii adecvate și pozitive și evitând duplicare activităților și eforturilor.

44. În acest context, AEPD recomandă legislatorului UE să consolideze rolul protecției datelor, asumându-și acțiuni (și termene limită) specifice, precum:

— evaluarea eficacității măsurilor existente, cu analizarea concomitentă a impactului acestora asupra vieții private, este esențială și ar trebui să reprezinte un rol important acțiunii Uniunii Europene în acest domeniu;

— atunci când se are în vedere luarea unor noi măsuri, analizarea posibilei suprapuneri cu instrumentele deja existente, luarea în considerare a eficacității acestora și limitarea colectării și schimbului de date la ceea ce este cu adevărat necesar pentru scopul urmărit;

— propunerea instituirii unui cadru de protecție a datelor care să se aplice și politicii externe și de securitate comune;

— propunerea unei abordări cuprinzătoare și globale în ceea ce privește asigurarea, în domeniul măsurilor restrictive (de înghețare a bunurilor), atât a eficacității acțiunii de aplicare a legii, cât și a respectării drepturilor fundamentale, pe baza articolului 75 din TFUE;

— plasarea protecției datelor în centrul dezbaterii privind măsurile din acest domeniu, prin asigurarea, de exemplu, a efectuării de evaluări ale impactului asupra vieții private și protecției datelor, precum și a consultării oportune a autorităților competente în materie de protecție a datelor în momentul înaintării propunerilor relevante în acest domeniu;

— asigurarea valorificării expertizei în domeniul protecției datelor în cadrul cercetării în materie de securitate într-o etapă incipientă a acestei cercetări, astfel încât această expertiză să imprime direcția opțiunilor politice, iar confidențialitatea să fie încorporată în cea mai mare măsură posibilă în noile tehnologii orientate către securitate;

— asigurarea mecanismelor adecvate de protecție în momentul prelucrării datelor cu caracter personal în contextul cooperării internaționale, promovând în același timp dezvoltarea și punerea în aplicare a principiilor de protecție a datelor de către țările terțe și organizațiile internaționale.

Adoptat la Bruxelles, 24 noiembrie 2010.

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor