Avizul Autorității Europene pentru Protecția Datelor privind propunerea de regulament al Parlamentului European și al Consiliului privind Agenția Europeană pentru Securitatea Rețelelor Informatice și a Datelor (ENISA)

(2011/C 101/04)

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 solicitarea unui aviz în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001 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],

ADOPTĂ PREZENTUL AVIZ:

I. INTRODUCERE

Descrierea propunerii

1. La 30 septembrie 2010, Comisia a adoptat o propunere de regulament al Parlamentului European și al Consiliului privind ENISA, Agenția Europeană pentru Securitatea Rețelelor Informatice și a Datelor [3].

2. ENISA a fost înființată în martie 2004, pentru o perioadă inițială de cinci ani, prin Regulamentul (CE) nr. 460/2004 [4]. În 2008, Regulamentul (CE) nr. 1007/2008 [5] a prelungit mandatul până în martie 2012.

3. În conformitate cu articolul 1 alineatul (1) din Regulamentul (CE) nr. 460/2004, agenția a fost înființată în vederea asigurării unui nivel ridicat și eficient al securității rețelelor informatice și a datelor în Uniune și pentru a contribui la buna funcționare a pieței interne.

4. Propunerea Comisiei are în vedere modernizarea agenției, consolidarea competențelor acesteia și acordarea unui nou mandat pentru o perioadă de cinci ani, care va permite continuitatea activităților agenției ulterior lunii martie 2012 [6].

5. Temeiul juridic al propunerii de regulament este articolul 114 din TFUE [7], care conferă Uniunii competența de a adopta măsuri în scopul instituirii sau asigurării funcționării pieței interne. Articolul 114 din TFUE este succesorul articolului 95 din fostul Tratat CE pe care se bazau regulamentele anterioare privind ENISA [8].

6. Expunerea de motive care însoțește propunerea menționează că prevenirea și combaterea criminalității a devenit o atribuție comună în urma intrării în vigoare a Tratatului de la Lisabona. Acesta a creat posibilitatea ca ENISA să joace un rol de platformă privind aspectele legate de securitatea rețelelor informatice și a datelor (SRD) în cadrul combaterii criminalității informatice și să efectueze schimburi de opinii și bune practici cu autoritățile din domeniul protecției informatice, aplicării legii și protecției datelor.

7. Dintre opțiunile avute la dispoziție, Comisia a ales să propună o extindere a sarcinilor ENISA și să includă autoritățile de aplicare a legii și de protecție a datelor în Grupul permanent al factorilor interesați cu drepturi depline al agenției. Noul mandat nu include atribuții operaționale, ci actualizează și reformulează atribuțiile actuale.

Consultarea AEPD

8. La 1 octombrie 2010, propunerea a fost trimisă AEPD spre consultare, în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001. AEPD apreciază faptul că a fost consultată cu privire la acest aspect și recomandă să se facă referire la această consultare în considerentele propunerii, astfel cum se procedează de obicei în cazul textelor legislative cu privire la care AEPD este consultată în conformitate cu Regulamentul (CE) nr. 45/2001.

9. Anterior adoptării propunerii, AEPD a fost consultată neoficial și a prezentat o serie de observații neoficiale. Totuși, niciuna dintre aceste observații nu a fost luată în considerare în versiunea finală a propunerii.

Evaluare generală

10. AEPD subliniază că securitatea prelucrării datelor este un element vital al protecției datelor [9]. În acest sens, autoritatea salută obiectivul propunerii de a consolida competențele agenției astfel încât să își poată îndeplini cu mai

[1] JO L 281, 23.11.1995, p. 31.
[2] JO L 8, 12.1.2001, p. 1.
[3] COM(2010) 521 final.
[4] JO L 77, 13.3.2004, p. 1.
[5] JO L 293, 31.10.2008, p. 1.
[6] Pentru a preveni un vid juridic, în cazul în care procedura legislativă în cadrul Parlamentului European și al Consiliului va depăși ca durată data la care expiră mandatul actual, Comisia a adoptat, la 30 septembrie 2010, o a doua propunere de modificare a Regulamentului (CE) nr. 460/2004 prin care se intenționează exclusiv prelungirea termenului-limită al actualului mandat cu 18 luni. A se vedea COM(2010) 520 final.
[7] A se vedea supra.
[8] La 2 mai 2006, Curtea de Justiție a respins o acțiune în anulare cu privire la Regulamentul (CE) nr. 460/2004 anterior, care contesta temeiul juridic al acestuia (cauza C-217/04).
[9] Cerințele de securitate sunt cuprinse în articolele 22 și 35 din Regulamentul (CE) nr. 45/2001, articolele 16 și 17 din Directiva 95/46/CE și articolele 4 și 5 din Directiva 2002/58/CE.

mare eficacitate sarcinile și responsabilitățile curente și, în același timp, să își extindă domeniul de activitate. De asemenea, AEPD salută includerea autorităților de protecție a datelor și a organelor de aplicare a legii ca factori interesați cu drepturi depline. AEPD consideră că prelungirea mandatului ENISA reprezintă o modalitate de a încuraja la nivel european gestionarea profesionistă și eficientă a măsurilor de securitate pentru sistemele informatice.

11. Evaluarea generală a propunerii este pozitivă. Cu toate acestea, în ceea ce privește mai multe aspecte, propunerea de regulament este neclară sau incompletă, ceea ce cauzează motive de îngrijorare din perspectiva protecției datelor. Aceste aspecte vor fi explicate și discutate în capitolul următor al prezentului aviz.

II. **OBSERVAȚII ȘI RECOMANDĂRI**

Sarcinile extinse care vor fi îndeplinite de ENISA nu sunt suficient de clare

12. Sarcinile extinse ale agenției care au legătură cu implicarea organelor de aplicare a legii și autorităților de protecție a datelor sunt formulate în termeni foarte generali în articolul 3 al propunerii. Expunerea de motive este mai explicită în acest sens. Aceasta face referire la interconectarea ENISA cu organele de aplicare a legii în materie de criminalitate informatică și la efectuarea de către agenție a unor sarcini fără caracter operațional în combaterea criminalității informatice. Totuși, aceste sarcini nu au fost incluse sau au fost menționate doar în termeni foarte generali la articolul 3.

13. Pentru a evita orice incertitudine juridică, propunerea de regulament ar trebui să fie clară și lipsită de ambiguități în privința sarcinilor ENISA. Astfel cum s-a precizat, securitatea prelucrării datelor reprezintă un aspect vital al protecției datelor. ENISA va avea un rol din ce în ce mai important în acest domeniu. Trebuie să fie clar pentru cetățeni, instituții și organe ce tip de activități poate desfășura ENISA. Această dimensiune este cu atât mai importantă în cazul în care sarcinile extinse ale ENISA includ prelucrarea de date cu caracter personal (a se vedea punctele 17-20 de mai jos).

14. Articolul 3 alineatul (1) litera (k) din propunere prevede că agenția efectuează orice altă sarcină care îi este conferită printr-un alt act legislativ al Uniunii. AEPD își exprimă preocuparea cu privire la această clauză deschisă, deoarece creează o potențială lacună care ar putea afecta coerența instrumentului juridic și ar putea conduce la o „denaturare a funcțiilor" agenției.

15. Una dintre sarcinile menționate la articolul 3 alineatul (1) litera (k) din propunere este inclusă în Directiva 2002/58/CE ([1]). Aceasta prevede că agenția trebuie să fie consultată de către Comisie cu privire la orice măsuri tehnice de punere în aplicare referitoare la notificări, în contextul încălcării securității datelor. AEPD recomandă descrierea în mai mare detaliu a acestei activități, cu limitarea concomitentă a acesteia la domeniul securității. Având în vedere potențialul impact pe care ENISA l-ar putea avea asupra evoluției politicii în acest domeniu, această activitate ar trebui să ocupe o poziție mai clară și mai proeminentă în cadrul propunerii de regulament.

16. AEPD recomandă, de asemenea, includerea unei trimiteri la Directiva 1999/5/CE ([2]) în considerentul 21, având în vedere sarcina specială a ENISA menționată la articolul 3 alineatul (1) litera (c) din actuala propunere de a sprijini statele membre și instituțiile și organismele europene în eforturile acestora de colectare, analiză și difuzare a informațiilor privind securitatea rețelelor informatice și a datelor. Aceasta ar trebui să contribuie la activitățile de promovare desfășurate de ENISA în favoarea celor mai bune practici și tehnici SRD (securitatea rețelelor informatice și a datelor), deoarece va ilustra mai bine posibilele interacțiuni constructive între agenție și organismele de standardizare.

Trebuie să se clarifice dacă agenția va prelucra date cu caracter personal

17. Propunerea nu specifică dacă sarcinile atribuite agenției ar putea include prelucrarea de date cu caracter personal. Prin urmare, propunerea nu conține un temei juridic specific pentru prelucrarea de date cu caracter personal, în sensul articolului 5 din Regulamentul (CE) nr. 45/2001.

18. Cu toate acestea, unele dintre sarcinile atribuite agenției ar putea implica (cel puțin într-o anumită măsură) prelucrarea de date cu caracter personal. De exemplu, nu se poate exclude faptul că analiza incidentelor de securitate și a cazurilor de încălcare a securității datelor sau executarea de funcții fără caracter operațional în cadrul combaterii criminalității informatice ar putea implica activități de colectare și analiză a datelor cu caracter personal.

19. Considerentul 9 al propunerii face referire la dispozițiile din Directiva 2002/21/CE ([3]) care prevăd că, dacă este cazul, agenția este notificată de autoritățile naționale de reglementare în cazul încălcării securității. AEPD recomandă ca propunerea să specifice în mai mare detaliu ce notificări trebuie să fie trimise agenției și cum trebuie să răspundă ENISA la acestea. De asemenea, propunerea ar trebui să abordeze implicațiile în termeni de prelucrare a datelor cu caracter personal care ar putea surveni în urma analizei acestor notificări (dacă este cazul).

([1]) Directiva 2002/58/CE a Parlamentului European și al Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) JO L 201, 31.7.2002, p. 37.

([2]) Directiva 1999/5/CE a Parlamentului European și a Consiliului din 9 martie 1999 privind echipamentele hertziene și echipamentele terminale de telecomunicații și recunoașterea reciprocă a conformității acestora, JO L 91, 7.4.1999, p. 10, în special articolul 3 alineatul (3) litera (c).

([3]) Directiva 2002/21/CE a Parlamentului European și a Consiliului din 7 martie 2002 privind un cadru de reglementare comun pentru rețelele și serviciile de comunicații electronice (Directivă-cadru, JO L 108, 24.4.2002, p. 33).

20. AEPD invită legislatorul să clarifice dacă și care dinte activitățile ENISA enumerate la articolul 3 vor include prelucrarea de date cu caracter personal.

Ar trebui să fie specificate norme de securitate internă pentru ENISA

21. Deși ENISA are un rol important în discuțiile privind securitatea rețelelor informatice și a datelor în Europa, propunerea nu face aproape nicio mențiune cu privire la instituirea unor măsuri de securitate pentru agenția însăși (asociate sau nu prelucrării de date cu caracter personal).

22. În opinia AEPD, agenția se va afla într-o poziție chiar mai bună pentru promovarea bunelor practici în legătură cu securitatea prelucrării datelor dacă astfel de măsuri de securitate ar fi aplicate cu rigurozitate la nivel intern de către agenția însăși. Aceasta va contribui la recunoașterea agenției nu doar ca centru de expertiză, ci și ca punct de referință pentru punerea în aplicare concretă a celor mai bune tehnici disponibile (*best available techniques*, BAT) în domeniul securității. Eforturile pentru excelență în cadrul punerii în aplicare a practicilor de securitate ar trebui, prin urmare, să fie încorporate în regulamentul care stabilește procedurile de lucru ale agenției. Prin urmare, AEPD sugerează ca în propunere să se adauge o dispoziție în acest sens, de exemplu, printr-o cerință ca agenția să aplice cele mai bune tehnici disponibile, ceea ce înseamnă cele mai eficace și avansate proceduri de securitate și metode de funcționare ale acestora.

23. Această abordare va permite agenției să formuleze recomandări privind adecvarea practică a anumitor tehnici pentru oferirea garanțiilor de securitate necesare. În plus, în punerea în aplicare a acestor BAT ar trebui să se acorde prioritate acelor tehnici care permit asigurarea securității și minimizează în același timp impactul asupra confidențialității. Ar trebui să fie selectate tehnicile care sunt mai compatibile cu conceptul „confidențialității prin concepție".

24. Chiar cu o abordare mai puțin ambițioasă, AEPD recomandă, cel puțin, ca regulamentul să conțină următoarele cerințe: (i) crearea unei politici de securitate internă în urma unei evaluări cuprinzătoare a riscurilor și luând în considerare standardele internaționale și bunele practici din statele membre, (ii) numirea unui ofițer de securitate responsabil cu punerea în aplicare a politicii, care să dispună de resursele și autoritatea adecvată, (iii) aprobarea acestei politici în urma unei examinări aprofundate a riscurilor reziduale și a metodelor de control propuse de Consiliul de administrație și (iv) o revizuire periodică a politicii, cu specificarea clară a frecvenței alese și a obiectivelor revizuirii.

Canalele de cooperare cu autoritățile de protecție a datelor (inclusiv AEPD) și Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal ar trebui să fie mai bine definite

25. Astfel cum s-a menționat deja, AEPD salută prelungirea mandatului agenției și consideră că autoritățile de protecție a datelor pot avea numeroase beneficii datorită existenței agenției (iar agenția poate beneficia de expertiza acestor autorități). Având în vedere convergența naturală și logică între securitate și protecția datelor, agenția și autoritățile de protecție a datelor sunt invitate la o colaborare cu adevărat strânsă.

26. Considerentele 24 și 25 conțin o trimitere la propunerea de directivă a UE privind criminalitatea informatică și menționează că agenția ar trebui să stabilească legături cu organele de aplicare a legii și cu autoritățile de protecție a datelor în ceea ce privește aspectele legate de securitatea informațiilor în cadrul combaterii criminalității informatice ([1]).

27. Propunerea ar trebui să prezinte, de asemenea, canale și mecanisme concrete de colaborare care vor (i) asigura *consecvența* activităților agenției cu cele ale autorităților de protecție a datelor și (ii) vor permite *cooperarea strânsă* între agenție și autoritățile de protecție a datelor.

28. În ceea ce privește *consecvența*, considerentul 27 se referă explicit la faptul că sarcinile agenției nu ar trebui să intre în conflict cu autoritățile de protecție a datelor din statele membre. AEPD salută această mențiune, însă observă că nu se face referire la AEPD și la Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal. AEPD recomandă legislatorului să includă în propunere și o dispoziție similară privind lipsa interferenței în ceea ce privește aceste două entități. Aceasta va crea un mediu de lucru mai clar pentru toate părțile și ar trebui să creeze un cadru pentru canalele și mecanismele de colaborare care vor permite agenției să ofere asistență diferitelor autorități de protecție a datelor și Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal.

29. De asemenea, în ceea ce privește *cooperarea strânsă*, AEPD salută includerea unei reprezentări a autorităților de protecție a datelor în cadrul Grupului permanent al factorilor interesați care va oferi consiliere agenției în legătură cu desfășurarea activităților acesteia. AEPD recomandă să se menționeze explicit că această reprezentare din partea autorităților naționale de protecție a datelor ar trebui să se facă pe baza numirii de către agenție, la propunerea Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal. De asemenea, ar fi de apreciat dacă s-ar introduce o mențiune care să prevadă prezența AEPD, ca atare, la acele reuniuni în cadrul cărora se intenționează discutarea unor aspecte care sunt relevante pentru cooperarea cu AEPD. În plus, AEPD recomandă ca agenția (la recomandarea Grupului permanent al factorilor interesați și cu aprobarea Consiliului de administrație) să instituie grupuri de lucru *ad hoc* pentru diversele teme în cadrul cărora protecția datelor și securitatea se suprapun, în scopul creării unui cadru pentru acest efort de cooperare strânsă.

([1]) Propunere de Directivă a Parlamentului European și a Consiliului privind atacurile împotriva sistemelor informatice și de abrogare a Deciziei-cadru 2005/222/JAI a Consiliului, COM(2010) 517 final.

30. În cele din urmă, pentru a evita orice posibilă neînțelegere, AEPD recomandă utilizarea termenului „autorități de protecție a datelor" în locul termenului „autorități de protecție a confidențialității", precum și să se clarifice care sunt acele autorități prin includerea unei trimiteri la articolul 28 din Directiva 95/46/CE și la AEPD, astfel cum se prevede în capitolul V al Regulamentului (CE) nr. 45/2001.

Nu este clar ce beneficiari pot solicita asistență din partea ENISA

31. AEPD remarcă o inconsecvență în propunerea de regulament cu privire la cine poate solicita asistență din partea ENISA. Din considerentele 7, 15, 16, 18 și 36 ale propunerii, reiese că ENISA are capacitatea de a acorda asistență organismelor statelor membre și Uniunii în ansamblu. Cu toate acestea, articolul 2 alineatul (1) face referire doar la Comisie și la statele membre, în timp ce articolul 14 restricționează capacitatea de a prezenta solicitări de asistență la: (i) Parlamentul European, (ii) Consiliu, (iii) Comisie și (iv) orice organism competent numit de un stat membru, fără să fie menționate unele dintre instituțiile, organismele, agențiile și oficiile Uniunii.

32. Articolul 3 al propunerii este mai specific și prevede diferite tipuri de asistență, în funcție de tipul de beneficiari: (i) colectarea și analiza informațiilor privind securitatea datelor (în cazul statelor membre și instituțiilor și organismelor europene), (ii) analiza situației securității rețelelor informatice și a datelor în Europa (în cazul statelor membre și instituțiilor europene), (iii) promovarea utilizării bunelor practici în domeniul gestionării riscurilor și securității (în Uniune și în statele membre), (iv) dezvoltarea detectării în materie de securitate a rețelelor informatice și a datelor (în instituțiile și organismele europene) și (v) colaborarea în cadrul dialogului și cooperării cu țările terțe (în cazul Uniunii).

33. AEPD invită legislatorul să remedieze această inconsecvență și să procedeze la alinierea dispozițiilor susmenționate. În acest sens, AEPD recomandă ca articolul 14 să fie modificat în așa fel încât să includă într-adevăr toate instituțiile, organismele, oficiile și agențiile Uniunii și să precizeze cu claritate ce tip de asistență poate fi solicitat de către diferitele entități din Uniune (în cazul în care legislatorul intenționează o astfel de diferențiere). În același sens, se recomandă ca anumite entități publice și private să poată solicita asistență din partea agenției dacă sprijinul solicitat are un potențial clar din perspectivă europeană și este compatibil cu obiectivele agenției.

Funcțiile Consiliului de administrație

34. Expunerea de motive prevede competențe sporite ale Consiliului de administrație în ceea ce privește rolul său de supraveghere. AEPD salută acest rol consolidat și recomandă includerea mai multor aspecte privind protecția datelor printre funcțiile Consiliului de administrație. În plus, AEPD recomandă ca regulamentul să specifice fără ambiguitate cine are următoarele drepturi: (i) de a institui măsuri pentru aplicarea Regulamentului (CE) nr. 45/2001 de către agenție, inclusiv măsurile care privesc numirea unui responsabil cu protecția datelor, (ii) de a aproba politica de securitate și revizuirile periodice ulterioare și (iii) de a stabili protocolul de cooperare cu autoritățile de protecție a datelor și organele de aplicare a legii.

Aplicabilitatea Regulamentului (CE) nr. 45/2001

35. Deși Regulamentul (CE) nr. 45/2001 include deja o cerință în acest sens, AEPD propune includerea în articolul 27 a numirii responsabilului cu protecția datelor, deoarece această măsură are o importanță deosebită și ar trebui însoțită de instituirea cu promptitudine a normelor de punere în aplicare cu privire la sfera competențelor și sarcinilor care îi vor fi atribuite responsabilului cu protecția datelor în conformitate cu articolul 24 alineatul (8) din Regulamentul (CE) nr. 45/2001. Mai concret, articolul 27 ar putea avea următorul conținut:

1. Informațiile prelucrate de agenție în conformitate cu prezentul regulament fac obiectul Regulamentului (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. Consiliul de administrație instituie măsuri pentru aplicarea Regulamentului (CE) nr. 45/2001 de către agenție, inclusiv măsurile referitoare la responsabilul cu protecția datelor din cadrul agenției.

36. În cazul în care este necesar un temei juridic pentru prelucrarea datelor cu caracter personal, astfel cum s-a discutat la punctele 17-20 de mai sus, acesta ar trebui să prevadă și specificarea mecanismelor de protecție, limitărilor și condițiilor necesare și adecvate în care va avea loc această prelucrare.

III. **CONCLUZII**

37. Evaluarea generală a propunerii este pozitivă, iar AEPD salută prelungirea mandatului agenției și extinderea sarcinilor acesteia prin includerea autorităților de protecție a datelor și a organelor de aplicare a legii în grupul factorilor interesați cu drepturi depline. AEPD consideră că prin continuitatea activității agenției se va încuraja la nivel european gestionarea profesionistă și eficientă a măsurilor de securitate pentru sistemele informatice.

38. AEPD recomandă ca, pentru evitarea oricăror incertitudini juridice, propunerea să fie clarificată în privința extinderii sarcinilor agenției și, în special, a celor legate de implicarea organelor de aplicare a legii și a autorităților de protecție a datelor. De asemenea, AEPD atrage atenția asupra potențialei lacune create de includerea în propunere a unei dispoziții care permite adăugarea unor noi sarcini ale agenției prin orice act legislativ al Uniunii fără nicio restricție suplimentară.

39. AEPD invită legislatorul să clarifice dacă și care dintre activitățile ENISA vor include prelucrarea de date cu caracter personal.

40. AEPD recomandă includerea unor dispoziții privind stabilirea unei politici de securitate pentru agenția însăși, în vederea consolidării rolului agenției ca factor favorizant al excelenței în materie de practici de securitate și ca promotor al principiului confidențialității prin concepție, prin integrarea utilizării celor mai bune tehnici disponibile în materie de securitate cu privire la drepturile de protecție a datelor cu caracter personal.

41. Canalele de cooperare cu autoritățile de protecție a datelor, inclusiv AEPD și Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, ar trebui să fie mai bine definite, în scopul asigurării consecvenței și cooperării strânse.

42. AEPD invită legislatorul să soluționeze unele inconsecvențe în ceea ce privește restricțiile exprimate în articolul 14 cu privire la capacitatea de a solicita asistență din partea agenției. În special, AEPD recomandă să se renunțe la aceste restricții, urmând ca toate instituțiile, organismele, agențiile și oficiile Uniunii să aibă dreptul de a solicita asistență din partea agenției.

43. În cele din urmă, AEPD recomandă includerea în capacitățile extinse ale Consiliului de administrație a anumitor aspecte concrete care ar putea spori asigurarea că în interiorul agenției sunt urmate bunele practici cu privire la securitate și protecția datelor. Printre altele, se propune includerea numirii unui responsabil cu protecția datelor și aprobarea măsurilor având ca scop aplicarea corectă a Regulamentului (CE) nr. 45/2001.

Adoptat la Bruxelles, 20 decembrie 2010.

Giovanni BUTTARELLI

Adjunct al Autorității Europene pentru Protecția Datelor