I

*(Resolucije, priporočila in mnenja)*

# MNENJA

# EVROPSKI NADZORNIK ZA VARSTVO PODATKOV

## Mnenje Evropskega nadzornika za varstvo podatkov o predlogu uredbe Sveta o stališču Unije v Skupnem odboru za carinsko sodelovanje EU-ZDA glede medsebojnega priznavanja programa o pooblaščenih gospodarskih subjektih v Evropski uniji in programa carinsko-trgovinskega partnerstva proti terorizmu v Združenih državah Amerike

(2012/C 160/01)

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV JE –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 16 Pogodbe,

ob upoštevanju Listine Evropske unije o temeljnih pravicah ter zlasti členov 7 in 8 Listine,

ob upoštevanju Direktive Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ([1]),

ob upoštevanju Uredbe (ES) št. 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov ([2]) ter zlasti člena 41 Uredbe –

SPREJEL NASLEDNJE MNENJE:

### I. UVOD

#### I.1 Posvetovanje z Evropskim nadzornikom za varstvo podatkov (ENVP) in namen mnenja

1. Komisija je 5. januarja 2011 sprejela predlog uredbe Sveta o stališču Unije v Skupnem odboru za carinsko sodelovanje EU-ZDA glede medsebojnega priznavanja programa o pooblaščenih gospodarskih subjektih v Evropski uniji in programa carinsko-trgovinskega partnerstva proti terorizmu v Združenih državah Amerike ([3]) (v nadaljnjem besedilu: predlog). Istega dne je predlog poslala ENVP.

2. ENVP, s katerim je bilo pred tem opravljeno neformalno posvetovanje, je Komisiji poslal več neuradnih pripomb. Namen tega mnenja je dopolniti te pripombe z vidika sedanjega predloga in javno predstaviti stališča ENVP.

3. ENVP priznava, da obdelava osebnih podatkov ni v ospredju predloga. Večina obdelanih informacij ne bo vključevala osebnih podatkov, kot so opredeljeni v zakonodaji o varstvu podatkov ([4]). Vendar je treba zakonodajo o varstvu podatkov upoštevati tudi v tistih primerih, v katerih to velja, kot bo pojasnjeno v nadaljevanju.

([1]) UL L 281, 23.11.1995, str. 31.
([2]) UL L 8, 12.1.2001, str. 1.
([3]) COM(2011) 937 konč.
([4]) Kot je navedeno v točkah 8 in 9 tega mnenja.

### I.2 **Ozadje predloga**

4. Namen predloga je vzpostaviti medsebojno priznavanje programov trgovinskega partnerstva EU in ZDA – in sicer programa o pooblaščenih gospodarskih subjektih (AEO) v EU in programa carinsko-trgovinskega partnerstva proti terorizmu (C-TPAT) v ZDA – za spodbujanje trgovine med subjekti, ki vlagajo v varnost dobavne verige in so člani enega od teh programov.

5. Carinski odnosi med Evropsko unijo in ZDA temeljijo na Sporazumu o carinskem sodelovanju in medsebojni pomoči v carinskih zadevah (CMAA) ([1]). Ta sporazum vzpostavlja Skupni odbor za carinsko sodelovanje (JCCC), ki ga sestavljajo predstavniki carinskih organov EU in ZDA. Medsebojno priznavanje bo vzpostavljeno s sklepom tega odbora. Zato predlog sestavljajo:

— obrazložitveni memorandum,

— predlog sklepa Sveta, v katerem je navedeno, da bo EU v odboru JCCC zavzela stališče iz osnutka sklepa o medsebojnem priznavanju,

— osnutek sklepa odbora JCCC o vzpostavitvi medsebojnega priznavanja programa AEO EU in programa C-TPAT ZDA (v nadaljnjem besedilu: osnutek sklepa) ([2]).

6. Osnutek sklepa bodo izvajali carinski organi, ki so določili postopek skupnih potrditev (postopek vložitve zahtevka za dodelitev članstva subjektom, ocena zahtevkov ter dodelitev članstva in spremljanje statusa člana).

7. Dobro delovanje medsebojnega priznavanja zato temelji na izmenjavi informacij med carinskimi organi EU in ZDA o trgovinskih subjektih, ki so že člani partnerskega programa.

## II. **ANALIZA OSNUTKA SKLEPA**

### II.1 **Obdelava podatkov v zvezi s fizičnimi osebami**

8. Čeprav namen osnutka sklepa ni obdelava osebnih podatkov, se bodo nekatere informacije, ki se bodo izmenjevale, nanašale na fizične osebe, zlasti če je subjekt fizična oseba ([3]), ali če uradni naziv pravne osebe, ki deluje kot subjekt, opredeljuje fizično osebo ([4]).

9. Pomen varstva podatkov v tej zvezi je poudarilo Sodišče Evropske unije v svoji sodbi v zadevi Schecke. V skladu s Sodiščem lahko pravne osebe uveljavljajo zaščito pravic do zasebnosti in varstva podatkov, kot sta priznani v Listini Evropske unije o temeljnih pravicah, če uradni naziv pravne osebe opredeljuje eno ali več fizičnih oseb ([5]). V tem mnenju bo zato analizirano, kako je izmenjava osebnih podatkov o subjektih zakonsko urejena v osnutku sklepa.

---

([1]) Sporazum med Evropsko skupnostjo in Združenimi državami Amerike o carinskem sodelovanju in medsebojni pomoči pri carinskih zadevah (UL L 222, 12.8.1997, str. 17), na voljo na spletni strani: http://ec.europa.eu/world/agreements/prepareCreateTreatiesWorkspace/treatiesGeneralData.do?step=0&redirect=true&treatyId=308 (povzetek in celotno besedilo).

([2]) Predlog sklepa Skupnega odbora za carinsko sodelovanje ZDA-EU o medsebojnem priznavanju programa carinsko-trgovinskega partnerstva v Združenih državah Amerike in programa o pooblaščenih gospodarskih subjektih v Evropski uniji.

([3]) Osebni podatki so v členu 2(a) Direktive 95/46/ES in členu 2(a) Uredbe (ES) št. 45/2001 opredeljeni kot „katera koli informacija, ki se nanaša na določeno ali določljivo fizično osebo“.

([4]) Glej tudi Mnenje Evropskega nadzornika za varstvo podatkov o predlogu sklepa Sveta o stališču Unije v Skupnem odboru za carinsko sodelovanje EU-Japonska glede medsebojnega priznavanja programov o pooblaščenih gospodarskih subjektih v Evropski uniji in na Japonskem, na voljo na spletni strani: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:190:0002:0006:SL:PDF

([5]) Sodba Sodišča Evropske unije z dne 9. novembra 2010 v združenih zadevah Volker und Markus Schecke in Eifert, C-92/09 in C-93/09, točka 53 (na voljo na spletni strani: http://curia.europa.eu/juris/document/document.jsf?docid=79001&doclang=SL&mode=&part=1).

### II.2 **Uporaba okvira varstva podatkov EU**

10. Obdelavo bodo izvajali carinski organi, opredeljeni v členu 1(b) sporazuma CMAA ([1]). V EU se ta opredelitev nanaša na „pristojne službe“ Evropske komisije in carinske organe držav članic EU. V skladu z zakonodajo EU o varstvu podatkov je obdelava, ki jo izvajajo države članice EU, predmet Direktive 95/46/ES (v nadaljnjem besedilu: Direktiva o varstvu podatkov) in nacionalne zakonodaje o varstvu podatkov, ki izvaja Direktivo o varstvu podatkov, medtem ko je obdelava osebnih podatkov v institucijah in organih EU predmet Uredbe (ES) št. 45/2001 (v nadaljnjem besedilu: Uredba). Zato se v tem primeru uporabljata Direktiva o varstvu podatkov in Uredba.

### II.3 **Raven varstva**

11. Informacije se izmenjujejo v elektronski obliki in v skladu s sporazumom CMAA. V členu 17(2) sporazuma CMAA je navedeno, da se lahko osebni podatki med pogodbenicama sporazuma prenašajo le, če pogodbenica, ki bo podatke prejela, zagotavlja raven varstva, ki je vsaj enakovredna tisti, ki jo v takem primeru uporablja država, ki podatke predloži.

12. ENVP pozdravlja to določbo, v zvezi s katero je treba razumeti, da je njen cilj vzpostavitev skladnosti z zakonodajo EU o varstvu podatkov. V skladu s členom 25 Direktive o varstvu podatkov in členom 9 Uredbe je podatke iz EU v tretje države praviloma mogoče prenašati le, če država prejemnica zagotavlja „ustrezno“ raven varstva ([2]). Člen 17(2) sporazuma CMAA se zato zdi strožji od zahtev iz Direktive o varstvu podatkov.

13. Zato je treba na podlagi vseh ustreznih okoliščin preučiti, ali organi prejemniki v Združenih državah Amerike zares zagotavljajo enakovredno raven varstva (ali vsaj „ustrezno“ raven). Analizo ustreznosti je treba opraviti ob upoštevanju vseh okoliščin prenosa ali niza prenosov ([3]).

14. Evropska komisija ni ugotovila, da ZDA kot celota zagotavljajo ustrezno raven varstva. Ker ni bila sprejeta odločitev o splošni ustreznosti, se lahko nadzorniki ([4]) pod nadzorom organov za varstvo podatkov ([5]) odločijo, da je varstvo, zagotovljeno v tem posebnem primeru, ustrezno. Države članice EU (ali ENVP, če prenose opravljajo institucije ali organi EU) lahko dovolijo tudi poseben prenos ali niz prenosov osebnih podatkov tretji državi, če nadzornik navede ustrezne zaščitne ukrepe ([6]).

15. Te priložnostne odločitve o ustreznosti je mogoče uporabiti v tem primeru, če nacionalni carinski organi in službe Evropske komisije, pristojne za carinske zadeve, predložijo zadostne dokaze, ki podpirajo navedbe, da so carinski organi ZDA sprejeli ustrezne zaščitne ukrepe v zvezi s prenosi, predvidenimi v osnutku sklepa ([7]).

16. Vendar ENVP nima zadostnih dokazov, da carinski organi ZDA zagotavljajo raven varstva podatkov, ki je „ustrezna“ ali „vsaj enaka tisti, ki jo v takem primeru uporablja država, ki podatke predloži“, kot je določeno v členu 17(2) sporazuma CMAA.

---

([1]) Glej oddelek I(2) osnutka sklepa.
([2]) Uredba dodaja, da ti prenosi lahko potekajo le, če se podatki prenašajo „samo zato, da se omogoči izvedba nalog, za katere je pristojen upravljavec“.
([3]) Glej člen 9(1) in 9(2) Uredbe, člen 25(1) in 25(2) Direktive o varstvu podatkov in nacionalno zakonodajo EU o varstvu podatkov, ki te člene izvajajo. Glej tudi zgoraj navedeno mnenje ENVP o Skupnem odboru za carinsko sodelovanje EU-Japonska.
([4]) V teh primerih carinski organi EU in njenih držav članic.
([5]) V nekaterih državah članicah lahko prenos dovolijo le organi za varstvo podatkov.
([6]) Člen 26(2) Direktive o varstvu podatkov in člen 9(7) Uredbe.
([7]) Glej tudi dopis ENVP glede „Prenosov osebnih podatkov tretjim državam: ‚ustreznost‘ držav podpisnic Konvencije št. 108 Sveta Evrope (primer 2009-0333)“, na voljo na spletni strani: http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Adminmeasures/2009/09-07-02_OLAF_transfer_third_countries_EN.pdf

17. ENVP zato poziva k zagotovitvi, da bodo dokazi, da carinski organi ZDA zagotavljajo raven varstva podatkov, ki je „ustrezna“ ali „vsaj enaka tisti, ki jo v takem primeru uporablja država, ki podatke predloži“, kot je določeno v členu 17(2) sporazuma CMAA, na voljo ENVP in nacionalnim organom za varstvo podatkov. To je treba zahtevati v določbi v osnutku sklepa.

18. Nazadnje, prenose osebnih podatkov iz EU v države, ki ne zagotavljajo „ustrezne“ ravni varstva, je mogoče dovoliti tudi v primeru katere koli izjeme iz člena 26(1) Direktive o varstvu podatkov ali člena 9(6) Uredbe. V tem posebnem primeru bi bilo mogoče trditi, da je prenos „potreben oziroma ga zahteva zakon na temelju pomembnega javnega interesa“ ([1]). Vendar te izjeme, ki jih je treba razumeti omejevalno, ne morejo biti podlaga za obsežne ali sistematične prenose osebnih podatkov ([2]). ENVP meni, da v tem primeru te izjeme ne bi bile koristne.

### II.4 **Omejitev namena**

19. V oddelku V(1) osnutka sklepa je navedeno, da se izmenjani podatki, ki jih pridobi carinski organ, lahko obdelujejo le za namene izvajanja osnutka sklepa v skladu s členom 17 sporazuma CMAA.

20. Vendar obdelavo za druge namene dovoljujeta tudi četrta alinea oddelka V(3) in člen 17(3) sporazuma CMAA. Ker nameni osnutka sklepa presegajo carinsko sodelovanje in vključujejo boj proti terorizmu, ENVP svetuje, naj se v besedilu sklepa podrobno navedejo vsi mogoči nameni prenosov osebnih podatkov. Poleg tega morajo biti vsi preneseni podatki nujni in sorazmerni za izpolnjevanje teh namenov. Opredeliti je treba tudi, da je treba posameznike, na katere se nanašajo osebni podatki, celovito obveščati o vseh namenih in pogojih obdelave njihovih osebnih podatkov.

### II.5 **Kategorije podatkov za izmenjavo**

21. Podatki o članih programov trgovinskega partnerstva, ki se lahko izmenjujejo med carinskimi organi, so: ime, naslov, status članstva, datum potrditve ali pooblastitve, začasne prekinitve in preklici, enotna številka pooblastila ali enotna identifikacijska številka in „podrobnosti, ki jih skupaj določijo carinski organi in katerih izmenjava je, kadar je to ustrezno, odvisna od vseh potrebnih zaščitnih ukrepov“ ([3]). Ker je ta zadnja postavka preširoka, ENVP priporoča opredelitev kategorij podatkov, ki jih lahko vključuje.

22. ENVP poleg tega ugotavlja, da lahko izmenjani podatki vključujejo podatke o kršitvah ali domnevnih kršitvah, na primer podatke o preklicu in začasni prekinitvi članstva. ENVP poudarja, da zakonodaja EU o varstvu podatkov omejuje obdelavo osebnih podatkov o kršitvah, kazenskih obsodbah ali varnostnih ukrepih ([4]). Obdelava teh kategorij podatkov je lahko predmet predhodnega preverjanja, ki ga opravijo ENVP in nacionalni organi EU za varstvo podatkov ([5]).

### II.6 **Nadaljnji prenosi**

23. Tretja alinea oddelka V(3) dovoljuje prenos podatkov tretjim državam ali mednarodnim organom, če je organ, ki je informacije zagotovil, dal predhodno soglasje in če je prenos v skladu s pogoji, ki jih določi ta organ. Nadaljnjih prenosov se ne sme dovoliti, če ni bila predložena utemeljitev.

---

([1]) Glej člen 9(6)(d) Uredbe ali člen 26(1)(d) Direktive o varstvu podatkov, ki v skladu z uvodno izjavo 58 Direktive o varstvu podatkov vključuje prenose med davčnimi ali carinskimi organi.

([2]) Glej tudi delovni dokument delovne skupine iz člena 29 z dne 25. novembra 2005 o skupni razlagi člena 26(1) Direktive 95/46/ES z dne 24. oktobra 1995 (WP 114), strani 7–9, na voljo na spletni strani: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_en.pdf

([3]) Glej oddelek IV(3) od (a) do (g) osnutka sklepa.

([4]) Glej člen 8(5) Direktive 95/46/ES in člen 10(5) Uredbe (ES) št. 45/2001.

([5]) Glej člen 27(a) Uredbe (ES) št. 45/2001 in nacionalno zakonodajo EU o varstvu podatkov, ki izvaja člen 20 Direktive 95/46/ES.

24. Zato se zdi, da bi moral oddelek V(3) vključevati podobno določbo, kot je določba iz člena 17(2) sporazuma CMAA, ki določa, da je osebne podatke mogoče prenesti tretji državi le, če država prejemnica podatkov zagotavlja raven varstva, ki je vsaj enakovredna ravni iz osnutka sklepa. Varstvo osebnih podatkov, zagotovljeno na podlagi tega osnutka sklepa, bi se sicer lahko zaobšlo z nadaljnjimi prenosi.

25. Ta določba bi morala vsekakor opredeliti namene takih prenosov in posebne primere, v katerih so ti dovoljeni. Prav tako bi morala izrecno opredeliti, da bosta nujnost in sorazmernost mednarodnih nadaljnjih prenosov ocenjena za vsak primer posebej in da obsežni ali sistematični prenosi niso dovoljeni. V besedilo je treba vključiti tudi obveznost obveščanja posameznikov, na katere se nanašajo osebni podatki, o možnosti mednarodnih nadaljnjih prenosov.

### II.7 **Hramba podatkov**

26. ENVP pozdravlja oddelek V(2), ki prepoveduje obdelavo ali hrambo informacij dlje, kot je potrebno za namen, zaradi katerega so prenesene. Vendar je treba opredeliti tudi najdaljše obdobje hrambe.

### II.8 **Varnost in odgovornost**

27. V oddelku IV je navedeno, da se informacije izmenjujejo v elektronski obliki. ENVP meni, da je treba v tem oddelku zagotoviti več podrobnih informacij o sistemu izmenjave informacij, ki bo vzpostavljen. Izbrani sistem mora vsekakor vključevati zasebnost in varstvo podatkov od faze zasnove (vgrajena zasebnost).

28. ENVP v zvezi s tem pozdravlja varnostne zaščitne ukrepe, predvidene v prvi in drugi alinei oddelka V(3), ki vključujejo nadzor dostopa, „zaščito pred nepooblaščenim dostopom, razširjanjem, spremembo, izbrisom ali uničenjem“ in nadzor, da se podatki uporabljajo le za namene iz osnutka sklepa. Pozdravlja tudi dnevnike o dostopih, predvidene v peti alinei oddelka V(3).

29. ENVP še priporoča, naj se v te določbe vključi tudi obveznost izvedbe ocene učinka na varstvo podatkov (vključno z oceno tveganja) pred začetkom izmenjav podatkov. Ocena mora vključevati oceno tveganja in ukrepe, predvidene za obravnavo tveganj ([1]). V besedilu je treba tudi opredeliti, da je treba redno preverjati skladnost s temi ukrepi in njihovo izvajanje ter o njih poročati. To je še toliko bolj pomembno, če se upošteva možnost, da se bodo obdelovali občutljivi podatki.

### II.9 **Kakovost podatkov in pravice posameznikov, na katere se nanašajo osebni podatki**

30. ENVP pozdravlja obveznost carinskih organov, da zagotavljajo, da so izmenjane informacije natančne in da se redno posodabljajo (glej oddelek V(2) in V(5)). Pozdravlja tudi oddelek V(4), ki subjektom, ki so člani partnerskih programov, zagotavlja pravico do dostopa in popravljanja njihovih osebnih podatkov.

31. Vendar ENVP ugotavlja, da je uresničevanje teh pravic predmet domače zakonodaje carinskega organa. V zvezi s podatki, ki jih predložijo carinski organi EU, in za zagotavljanje „ustrezne“ ravni varstva (glej oddelek II.3 tega mnenja) je treba te pravice omejiti le, če je taka omejitev nujna za zaščito pomembnega gospodarskega ali finančnega interesa.

32. ENVP pozdravlja tudi dejstvo, da morajo carinski organi izbrisati podatke, ki so jih prejeli, če je njihovo zbiranje ali nadaljnja obdelava v nasprotju z osnutkom sklepa ali sporazumom CMAA ([2]). ENVP želi opozoriti, da bi se v skladu s členom 17(2) sporazuma CMAA ta določba uporabljala za vse obdelave, ki so v nasprotju z zakonodajo EU o varstvu podatkov.

---

([1]) Kot je že predvideno v členu 33 novega predloga uredbe o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (Splošna uredba o varstvu podatkov) (COM(2012) 11/4 osnutek).

([2]) Glej oddelek V(5) osnutka sklepa.

33. ENVP pozdravlja obveznost carinskih organov, da članom programov zagotavljajo informacije o možnostih uveljavljanja pravnega sredstva [1]. Vendar je treba pojasniti, katere so možnosti za uveljavljanje pravnega sredstva v primeru kršitve zaščitnih ukrepov o varstvu podatkov, ki so določeni v osnutku sklepa. V tej določbi je treba tudi opredeliti, da je treba tudi druge posameznike, na katere se nanašajo osebni podatki (in sicer subjekte, ki so vložili zahtevek za članstvo), obvestiti o možnostih za uveljavljanje pravnega sredstva.

### II.10 **Nadzor**

34. ENVP pozdravlja oddelek V(6), ki določa, da je ves oddelek V predmet „neodvisnega nadzora ali pregleda“, ki ga izvajajo vodja službe za varstvo zasebnosti na ministrstvu za domovinsko varnost v ZDA, Evropski nadzornik za varstvo podatkov in nacionalni organi za varstvo podatkov.

35. Poleg tega je treba opredeliti, da morajo ENVP in nacionalni organi za varstvo podatkov nadzirati „ustreznost“ ravni varstva, ki jo v zvezi z osebnimi podatki zagotavlja carinski organ, ki te podatke prejme (glej oddelek III.1). Tudi oddelek IV mora biti predmet nadzora in pregleda.

## III. **SKLEPNA UGOTOVITEV**

36. ENVP pozdravlja zaščitne ukrepe, predvidene v osnutku sklepa, zlasti v zvezi z varnostjo podatkov. Vendar je treba ENVP in nacionalnim organom za varstvo podatkov zagotoviti dokaze, da carinski organi ZDA zagotavljajo raven varstva podatkov, ki je „ustrezna“ ali „vsaj enaka tisti, ki jo v takem primeru uporablja država, ki podatke predloži“, kot je določeno v členu 17(2) sporazuma CMAA. To je treba določiti z določbo v osnutku sklepa.

37. ENVP poleg tega priporoča še:

— opredelitev namena(-ov) izmenjav podatkov, predvidenih v osnutku sklepa, ki morajo biti nujne in sorazmerne,

— opredelitev kategorij podatkov, vključenih na podlagi oddelka IV(3)(g),

— opredelitev, da je treba v primeru utemeljene potrebe po nadaljnjih mednarodnih prenosih te prenose dovoliti le za vsak primer posebej, za skladne namene in če država, ki podatke prejme, zagotavlja raven zaščite, ki je vsaj enakovredna tisti iz osnutka sklepa,

— vključitev obveznosti obveščanja vseh posameznikov, na katere se nanašajo osebni podatki, o zgoraj navedenem,

— dopolnitev določb o varnosti,

— opredelitev najdaljših obdobij hrambe podatkov,

— neomejitev pravic posameznikov iz EU, na katere se nanašajo osebni podatki, razen če je taka omejitev nujna za zaščito pomembnega gospodarskega ali finančnega interesa,

— zagotavljanje pravice do uveljavljanja pravnega sredstva,

— določitev, da je oddelek IV predmet nadzora in pregleda,

— opredelitev, da morajo ENVP, nacionalni organi EU za varstvo podatkov in vodja službe za varstvo zasebnosti na ministrstvu za domovinsko varnost v ZDA nadzirati, da so zaščitni ukrepi, ki jih izvaja carinski organ, ki prejme podatke, za zagotavljanje ustrezne ravni varstva osebnih podatkov učinkoviti in v skladu z zahtevami EU.

[1] Glej zadnji stavek oddelka V(4).

38. ENVP poleg tega ugotavlja, da lahko predlog vključuje obdelavo osebnih podatkov o kršitvah ali domnevnih kršitvah. Za te podatke se na podlagi zakonodaje EU uporabljajo strožji zaščitni ukrepi in v zvezi z njimi se lahko uporablja obveznost predhodnega preverjanja, ki ga izvajajo ENVP in nacionalni organi EU za varstvo podatkov.

V Bruslju, 9. februarja 2012

Giovanni BUTTARELLI

*Pomočnik Evropskega nadzornika za varstvo podatkov*