I

(Informacije)

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV

Mnenje Evropskega nadzornika za varstvo podatkov o predlogu direktive Evropskega parlamenta in Sveta o hrambi podatkov, obdelanih v povezavi z zagotavljanjem javnih elektronskih komunikacijskih storitev, in spremembi direktive 2002/58/ES (COM(2005) 438 konč.)

(2005/C 298/01)

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV JE –

ob upoštevanju Pogodbe o ustanovitvi Evropske skupnosti in zlasti člena 286 Pogodbe,

ob upoštevanju Listine o temeljnih pravicah Evropske unije in zlasti člena 8 Listine,

ob upoštevanju Direktive 95/46/ES Evropskega parlamenta in Sveta z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ([1]) ter Direktive 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) ([2]),

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 ([3]) ter zlasti člena 41 Uredbe,

ob upoštevanju prošnje za mnenje v skladu s členom 28(2) Uredbe (ES) št. 45/2001, ki jo je 23. septembra 2005 prejel od Komisije –

SPREJEL NASLEDNJE MNENJE:

I. **Uvod**

1. Evropski nadzornik za varstvo podatkov (ENVP) pozdravlja dejstvo, da so ga vprašali za mnenje na podlagi člena 28(2) Uredbe (ES) št. 45/2001. Vendar je treba glede na obvezen značaj člena 28(2) Uredbe (ES) št. 45/2001 to mnenje navesti v preambuli direktive.

2. ENVP priznava pomembnost dejstva, da imajo organi kazenskega pregona držav članic na voljo vse potrebne pravne instrumente, zlasti pri boju proti terorizmu in drugim hujšim

([1]) UL L 281, 23.11.1995, str. 31.

([2]) UL L 201, 31.7.2002, str. 37.

([3]) UL L 8, 12.1.2001, str. 1.

kaznivim dejanjem. Ustrezna razpoložljivost določenih podatkov javnih elektronskih storitev o prometu in lokaciji je lahko ključni instrument za te organe kazenskega pregona ter lahko prispeva k fizični varnosti oseb. Poleg tega je treba omeniti, da to ne pomeni samodejno potrebe po novih instrumentih, kakor je predvideno v navedenem predlogu.

3. Prav tako je očitno, da ima predlog precejšen vpliv na varstvo osebnih podatkov. Če se predlog obravnava zgolj z vidika varstva podatkov, se podatkov o prometu in lokaciji nikakor ne bi smelo hraniti za namene kazenskega pregona. Direktiva 2002/58/ES zato zaradi varstva podatkov vzpostavlja pravno načelo, da je treba podatke o prometu izbrisati takoj, ko shranjevanje ni več potrebno za namene, povezane s samim sporočilom (vključno za namene zaračunavanja). Za izjeme od tega pravnega načela veljajo strogi pogoji.

4. V tem mnenju ENVP izpostavlja vpliv predloga na varstvo osebnih podatkov. ENVP bo poleg tega upošteval, da ne glede na pomen predloga za kazenski pregon morda zaradi tega ljudem ne bo odvzeta temeljna pravica o varstvu njihove zasebnosti.

5. To mnenje ENVP je treba obravnavati v luči teh razmišljanj. ENVP predvideva uravnotežen pristop, v katerem igrata osrednjo vlogo nujnost in sorazmernost posegov v varstvo podatkov.

6. Kar se tiče samega predloga, je treba to obravnavati kot odziv na pobudo Francoske republike, Irske, Kraljevine Švedske in Združenega kraljestva za okvirni sklep o hrambi podatkov, ki se obdelujejo in hranijo v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev, ali podatkov o javnih komunikacijskih omrežjih za namene preprečevanja, preiskovanja, odkrivanja in pregona kriminala ter kaznivih dejanj, vključno s terorizmom („osnutek okvirnega sklepa“), ki ga je Evropski parlament zavrnil (v postopku posvetovanja).

7. O osnutku okvirnega sklepa se z ENVP niso posvetovali, niti ni podal mnenja na lastno pobudo. ENVP še ne namerava podati mnenja o osnutku okvirnega sklepa, vendar pa se bo v tem mnenju skliceval na navedeni osnutek sklepa, kadar se mu bo to zdelo koristno.

II. **Splošne ugotovitve**

Vpliv predloga na varstvo osebnih podatkov

8. Po mnenju ENVP je bistveno, da predlog spoštuje temeljne pravice. Zakonodajni ukrep, ki bi škodil varstvu, zajamčenem z zakonodajo Skupnosti ter še zlasti s sodno prakso Sodišča Evropskih skupnosti in Evropskega sodišča za človekove pravice, je ne samo nesprejemljiv, temveč tudi nezakonit. Okoliščine v družbi so se zaradi terorističnih napadov morda spremenile, vendar posledica tega ne sme biti ogrožanje visokih standardov varstva v pravni državi. Varstvo je zagotovljeno z zakonom ne glede na trenutne potrebe kazenskega pregona. Poleg tega sodna praksa sama po sebi dovoljuje izjeme, če so te v demokratični družbi potrebne.

9. Predlog ima neposreden vpliv na varstvo, podano v členu 8 Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin („ECHR“). V skladu s sodno prakso Evropskega sodišča za človekove pravice:

— je hranjenje informacij o posamezniku poseg v zasebno življenje, četudi ne vsebuje nobenih občutljivih podatkov (Amann ([1])),

— enako velja za prakso „beleženja“ telefonskih klicev („metering“) z uporabo naprave, ki samodejno zapisuje klicane telefonske številke, ter čas in trajanje vsakega klica (Malone ([2])),

— utemeljitve posega morajo odtehtati škodljivi učinek, ki bi ga obstoj zadevnih zakonskih določb lahko imel na subjekte (Dudgeon ([3])).

10. Člen 6(2) Pogodbe EU določa, da Unija spoštuje temeljne pravice, zajamčene z ECHR. V prejšnjem odstavku je bilo prikazano, da na podlagi sodne prakse Evropskega sodišča za človekove pravice obveznost hrambe podatkov spada v področje uporabe člena 8 ECHR, ter da je potrebna tehtna utemeljitev, ki spoštuje merila sodbe Dudgeon. Nujnost in

([1]) Sodba ECHR z dne 16. februarja 2000, Amann, 2000-II, vloga 27798/95.

([2]) Sodba ECHR z dne 2. avgusta 1984, Malone, A82, vloga 8691/79.

([3]) Sodba ECHR z dne 22. oktobra 1981, Dudgeon, A45, vloga 7525/76.

sorazmernost obveznosti hrambe podatkov je treba dokazati, in sicer v polni meri.

11. Poleg tega ima predlog velik vpliv na načela o varstvu podatkov, priznana z zakonodajo Skupnosti:

— podatke je treba hraniti veliko daljše obdobje, kot so običajna obdobja hrambe pri ponudnikih javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežjih (obe storitvi sta v nadaljevanju imenovani „ponudniki“),

— na podlagi Direktive 2002/58/ES, še zlasti njenega člena 6, se smejo podatki zbirati in hraniti le iz razlogov, ki so neposredno povezani s samim sporočilom, vključno zaradi zaračunavanja ([1]). Potem je treba podatke izbrisati (ob upoštevanju izjem). Na podlagi tega predloga je hramba za namene izvrševanja kazenskega prava obvezna. Izhodišče je zato nasprotno,

— Direktiva 2002/58/ES zagotavlja varnost in zaupnost. Ta predlog ne sme voditi do vrzeli na tem področju; potrebni so strogi zaščitni ukrepi, treba pa je razjasniti tudi omejitev namena,

— uvedba obveznosti hrambe podatkov, predvidena v predlogu, vodi do obsežnih zbirk podatkov in predstavlja posebna tveganja za osebo, na katero se podatki nanašajo. Podatki se lahko uporabijo v komercialne namene, pa tudi za lovljenje osebnih podatkov („fishing“) in/ali rudarjenje podatkov („data mining“) s strani organov kazenskega pregona ali nacionalnih varnostnih služb.

12. Nenazadnje varstvo zasebnega življenja in varstvo osebnih podatkov priznava tudi Listina o temeljnih pravicah, kot je navedeno v obrazložitvenem memorandumu.

13. Natančno je treba analizirati vpliv predloga na varstvo osebnih podatkov. V tej analizi bo ENVP upošteval prej omenjene elemente in zaključil, da je potrebnih več zaščitnih urkepov. Enostaven sklic na obstoječ pravni okvir o varstvu podatkov (zlasti direktivi 95/46/ES in 2002/58/ES) ni dovolj.

Nujnost hrambe podatkov o prometu in lokaciji

14. ENVP opozarja na sklep Delovne skupine za varstvo podatkov iz člena 29 z dne 9. novembra 2004 o osnutku okvirnega sklepa. Delovna skupina je navedla, da obvezna hramba podatkov o prometu pod pogoji iz osnutka okvirnega sklepa ni sprejemljiva. Ta sklep je med drugim temeljil na nezmožnosti zagotoviti kakršen koli dokaz v zvezi s potrebo po hrambi za namene javnega reda, in sicer na podlagi dejstva, da je analiza pokazala, da znaten del podatkov o prometu, ki so jih zahtevali organi kazenskega pregona, ni bil starejši od šestih mesecev.

15. Po mnenju ENVP bi morala biti razmišljanja Delovne skupine za varstvo podatkov iz člena 29 izhodišče za oceno tega predloga. Vendar pa rezultata teh razmišljanj ni mogoče zgolj prenesti v ta predlog. Pri tem je namreč treba upoštevati, da se okoliščine lahko spremenijo. Po mnenju ENVP bi bili za oceno lahko pomembni naslednji dejavniki.

16. Na prvem mestu so bile pripravljene nekatere številke, ki dokazujejo, da v praksi organi kazenskega pregona zahtevajo podatke, stare do enega leta. Tako Komisija kot predsedstvo Sveta pripisujeta pomen študiji policije Združenega kraljestva ([2]), ki kaže, da so kljub dejstvu, da je bilo 85 % podatkov o prometu, ki jih je zahtevala policija, starih manj kot šest mesecev, v obsežnih preiskavah hujših kaznivih dejanj uporabili podatke, stare od šest mesecev do enega leta. Predstavljenih je bilo tudi nekaj primerov teh zadev. Obdobje hrambe iz predloga – eno leto za telefonske podatke – odraža te prakse organov kazenskega pregona.

17. ENVP ni prepričan, da te številke predstavljajo dokaz o potrebi po hrambi podatkov o prometu za obdobje do enega leta. Dejstvo, da je v nekaterih primerih razpoložljivost podatkov o prometu in/ali lokaciji pomagala rešiti zločin, samodejno ne pomeni, da se ti podatki (na splošno) potrebujejo kot orodje kazenskega pregona. Kljub temu teh številk ni mogoče prezreti. Predstavljajo vsaj resen poizkus dokazati potrebo po hrambi. Poleg tega številke jasno kažejo, da obdobje hrambe, daljše od enega leta, s stališča trenutnih praks kazenskega pregona ni potrebno.

18. Na drugem mestu se obstoječe možnosti ponudnikov za hrambo podatkov za namene zaračunavanja na podlagi Direktive 2002/58/ES ne izkoristijo vedno, ker v vse večjem številu primerov hrambe podatkov za namene zaračunavanja sploh ni (predplačniške kartice mobilnih komunikacij, pav-

([1]) Glej tudi točko 3 tega mnenja.

([2]) Svoboda in varnost, iskanje pravega ravnotežja. Dokument predsedstva UK Evropske unije z dne 7. septembra 2005.

šalne naročnine itd). V teh primerih – ki v praksi postajajo vse pogostejši – se podatkov o prometu in lokaciji sploh ne bo hranilo, temveč bodo izbrisani takoj po koncu komunikacije. Enako velja za neuspele klice. To lahko vpliva na učinkovitost kazenskega pregona.

19. Poleg tega ta razvoj telekomunikacijskih storitev lahko vodi do motenj v delovanju notranjega trga, med drugim zaradi (bližnjega) sprejetja zakonodajnih ukrepov v državah članicah na podlagi člena 15 Direktive 2002/58/ES. Italijanska vlada je na primer nedavno objavila odlok, ki ponudnike obvezuje k štiriletnemu hranjenju telefonskih podatkov. Ta obveznost bo vodila do precejšnjih stroškov v določenih državah članicah, kot je Italija.

20. Na tretjem mestu so se razvile tudi delovne metode organov kazenskega pregona: pomembnejše so postale proaktivne preiskave in uporaba tehnične podpore. Ta razvoj zahteva, da imajo organi na voljo primerna in natančno izoblikovana orodja, ki jim omogočajo opravljati delo s primernim spoštovanjem načel o varstvu podatkov. Eno od orodij, s katerim organi držav članic ponavadi razpolagajo, je ohranitev podatkov ali zamrznitev podatkov o komunikacijah na zahtevo v konkretni preiskavi. Ugotovljeno je bilo, da to orodje, ki ima samo po sebi manj vpliva na ta načela kot sedaj predlagano orodje (hramba podatkov), morda ne zadošča vedno, zlasti pri iskanju oseb, vpletenih v terorizem ali druga hujša kazniva dejanja, ki pred tem niso bile osumljene nobene kriminalne dejavnosti. Vendar je za potrditev tega treba zbrati več dokazov.

21. Na četrtem mestu so se skrbi v zvezi s terorističnimi napadi povečale. ENVP se strinja s stališčem, izraženim v okviru predlogov o hrambi podatkov, da je fizično varstvo samo po sebi bistvenega pomena. Družbo je treba zaščititi. Zaradi tega so vlade v primeru napadov na družbo obvezane pokazati, da resno upoštevajo potrebo po varstvu, ter raziskati, če se morajo odzvati z uvedbo novih zakonodajnih ukrepov. Samoumevno je, da ENVP polno podpira nalogo vlad – tako na nacionalni kot na evropski ravni – zaščititi družbo in prikazati, da delajo vse, kar je potrebno za zagotavljanje zaščite, vključno s sprejetjem novih, legitimnih in učinkovitih ukrepov, ki so rezultat njihovih preiskav.

22. ENVP upošteva spremembe okoliščin, a še ni prepričan o potrebi po hrambi podatkov o prometu in lokaciji za namene kazenskega pregona, kakor je opredeljeno v predlogu. Poudarja pomen pravnega načela, določenega z Direktivo 2002/58/ES, da je treba podatke o prometu izbrisati takoj, ko shranjevanje ni več potrebno za namene, ki niso povezani s samim sporočilom. Poleg tega predložene številke ne dokazujejo, da obstoječi pravni okvir ne ponuja instrumentov, ki so potrebni za zaščito fizične varnosti, niti da države članice polno uporabljajo svoje pristojnosti iz evropskega prava o sodelovanju, kakor so jim bile podeljene v skladu z obstoječim pravnim okvirom (toda brez potrebnih rezultatov).

23. Če pa bosta Evropski parlament in Svet po previdnem uravnoteženju obravnavanih interesov vendarle prišla do zaključka, da je potreba po hrambi podatkov o prometu in lokaciji zadovoljivo dokazana, bo ENVP zavzel stališče, da je hramba lahko upravičena le na podlagi prava Skupnosti, v kolikor se spoštuje načelo sorazmernosti in so zagotovljeni ustrezni zaščitni ukrepi v skladu s tem mnenjem.

Sorazmernost

24. Sorazmernost samega predlaganega novega zakonodajnega ukrepa je odvisna od vsebine njegovih določb: ali vsebuje ustrezen in sorazmeren odziv na potrebe družbe?

25. Prvi razmislek se dotika ustreznosti predloga: ali se lahko pričakuje, da bo predlog povečal fizično varnost prebivalcev Evropske unije? Prvi razlog za dvom o ustreznosti, pogosto omenjen v javnih razpravah, je, da podatki o prometu in lokaciji niso vedno povezani z določenim posameznikom, zato informacije o telefonski številki (ali številki IP) ne razkrijejo nujno identitete posameznika. Drugi, še pomembnejši razlog za dvom je, ali obstoj velikanskih zbirk podatkov organom kazenskega pregona omogoča z lahkoto najti, kar v določenem primeru potrebujejo.

26. ENVP je mnenja, da zgolj hramba podatkov o prometu in lokaciji ni ustrezen ali učinkovit odziv. Potrebni so dodatni ukrepi za zagotovitev, da imajo organi na voljo natančen in hiter dostop do podatkov, ki jih v določenem primeru potrebujejo. Hramba podatkov je ustrezna in učinkovita le v primeru obstoja učinkovitih iskalnikov.

27. Drugi razmislek se dotika sorazmerne narave odziva. Če želi biti sorazmeren, bi moral predlog:

— omejiti obdobja hrambe. Obdobja morajo odražati dokazane potrebe organov kazenskega pregona,

— omejiti število podatkov, ki naj se hranijo. Ta številka mora odražati dokazane potrebe organov kazenskega pregona, treba pa je zagotoviti, da dostop do podatkov o vsebini ni mogoč,

— vsebovati ustrezne varnostne ukrepe, tako da se omejita dostop in nadaljnja uporaba, zajamči zaščita podatkov in zagotovi, da osebe, na katere se podatki nanašajo, lahko uveljavljajo svoje pravice.

28. ENVP poudarja pomen teh strogih omejitev z ustreznimi varovali, katerih namen je omejeni dostop. Njegovo stališče je, da države članice na podlagi pomembnosti treh elementov, omenjenih v zgornji točki, v zvezi z njimi ne smejo sprejeti dodatnih nacionalnih ukrepov, ki posegajo v sorazmernost. Potreba po uskladitvi bo obravnavana v oddelku IV.

Ustrezni varnostni ukrepi

29. Posledica predloga bo, da bodo imeli ponudniki na voljo zbirke podatkov, v katerih bo shranjena znatna količina podatkov o prometu in lokaciji.

30. Na prvem mestu bo predlog moral zagotoviti, da bosta dostop do teh podatkov in njihova nadaljnja uporaba omejena in mogoča le v določenih okoliščinah in za omejeno število določenih namenov.

31. Na drugem mestu bodo morale biti zbirke podatkov ustrezno zaščitene (zaščita podatkov). V ta namen je treba zagotoviti, da so po poteku obdobja hrambe podatki uspešno izbrisani. Ne sme priti do odlaganja podatkov ali izkoriščanja podatkov. Na kratko to torej zahteva visoko zaščito podatkov in ustrezne tehnične in organizacijske varnostne ukrepe.

32. Visoka zaščita podatkov je še bolj pomembna, ker bi že sam obstoj podatkov lahko vodil do zahtev vsaj treh interesnih skupin za dostop in uporabo:

— samih ponudnikov: morda bodo skušali podatke uporabiti za svoje lastne komercialne namene. Potrebna so jamstva za preprečevanje kopiranja teh datotek,

— organov, pristojnih za kazenski pregon: predlog jim nudi pravico dostopa, a le v posebnih primerih in v skladu z nacionalno zakonodajo (člen 3(2) predloga). Dostop ne bi smel biti dovoljen za namene rudarjenja podatkov ali lovljenja osebnih podatkov (fishing). Izmenjavo podatkov z organi drugih držav članic je treba jasno urediti s predpisi,

— obveščevalnih služb (ki so pristojne za nacionalno varnost).

33. Kar se tiče dostopa obveščevalnih služb ENVP opaža, da na podlagi člena 33 Pogodbe EU in člena 64 Pogodbe ES intervencije v okviru tretjega in prvega stebra ne vplivajo na izpolnjevanje obveznosti držav članic glede vzdrževanja javnega reda in miru ter varovanja notranje varnosti. Po mnenju ENVP je posledica teh določb dejstvo, da Evropska unija nima dovolj pristojnosti za nadzor dostopa varnostnih ali obveščevalnih služb do podatkov, ki jih hranijo ponudniki. Drugače povedano, zakonodaja Evropske unije ne vpliva niti na dostop teh služb do podatkov ponudnikov o prometu in lokaciji niti na nadaljnjo uporabo informacij, ki so jih zbrale te službe. To je element, ki ga je treba upoštevati pri oceni predloga. Države članice so tiste, ki morajo sprejeti potrebne ukrepe za ureditev dostopa obveščevalnih služb.

34. Na tretjem mestu imajo vplivi, opisani v prejšnjih odstavkih, možne posledice za osebo, na katero se podatki nanašajo. Potrebna so dodatna varovala za zagotovitev, da lahko ta oseba, na katero se podatki nanašajo, hitro in učinkovito uveljavlja svoje pravice. ENVP izpostavlja potrebo po učinkovitem nadzoru dostopa in nadaljnje uporabe, po možnosti s strani pravosodnih organov držav članic. Varovala je treba uporabljati tudi v primeru dostopa do podatkov o prometu in njihovi nadaljnji uporabi s strani organov iz drugih držav članic.

35. V tej zvezi se ENVP sklicuje na pobude za nov pravni okvir o varstvu podatkov, namenjen kazenskemu pregonu (v tretjem stebru PEU). Po njegovem mnenju takšen pravni okvir zahteva dodatna varovala in se ne sme omejiti zgolj na ponovno potrditev splošnih načel o varstvu podatkov iz prvega stebra ([1]).

36. Na četrtem mestu obstaja neposredna povezava med ustreznostjo varnostnih ukrepov in stroški teh ukrepov. Ustrezen zakon o hrambi podatkov mora zato vsebovati vzpodbude za ponudnike, da vlagajo v tehnično infrastrukturo. Takšna vzpodbuda bi lahko bila, da se ponudnikom povrne dodatne stroške, ki so jih imeli zaradi uvedbe ustreznih varnostnih ukrepov.

37. Če povzamemo, bi morali ustrezni varnostni ukrepi:

— omejiti dostop do podatkov in njihovo nadaljnjo uporabo,

— zagotoviti ustrezne tehnične in organizacijske varnostne ukrepe za zaščito zbirk podatkov. To vključuje ustrezen izbris podatkov po poteku obdobja hrambe in upošteva

([1]) V tej zvezi glej tudi Pogajalsko izhodišče za kazenski pregon in izmenjavo informacij v EU, sprejeto na spomladanski konferenci evropskih organov za varstvo podatkov v Krakovu, 25. in 26. aprila 2005.

zahteve za dostop in uporabo s strani različnih interesnih skupin,

— zagotoviti uveljavljanje pravic oseb, na katere se podatki nanašajo, in sicer ne zgolj s ponovno potrditvijo splošnih načel o varstvu podatkov,

— vsebovati vzpodbude za ponudnike za vlaganje v tehnično infrastrukturo.

III. Pravna podlaga in osnutek okvirnega sklepa

38. Predlog temelji na Pogodbi ES, zlasti na členu 95 Pogodbe, v skladu z njegovim členom 1 pa je njegov namen uskladitev obveznosti ponudnikov v zvezi z obdelavo in hrambo podatkov o prometu in lokaciji. Navaja, da se podatke pristojnim organom priskrbi le v posameznih primerih, povezanih s kaznivimi dejanji, vendar pa natančnejšo opredelitev namena oziroma dostopa do podatkov in njihove nadaljnje uporabe prepušča državam članicam, ob upoštevanju varoval obstoječega okvira Skupnosti o varstvu podatkov.

39. V tej zvezi ima predlog bolj omejeno področje uporabe kot osnutek okvirnega sklepa, ki temelji na členu 31(1)(c) Pogodbe EU in ki vsebuje dodatne določbe o dostopu do hranjenih podatkov oziroma o zahtevah drugih držav članic po dostopu. Obrazložitveni memorandum utemeljuje to omejitev področja uporabe predloga. Navaja, da sta dostop in izmenjava informacij med zadevnimi organi kazenskega pregona zadeva, ki ne spada v področje uporabe Pogodbe ES.

40. ENVP ta izjava iz obrazložitvenega memoranduma ne prepriča. Glavni cilj intervencije Skupnosti na podlagi člena 95 Pogodbe ES (notranji trg) mora biti odstranitev ovir za trgovanje. V skladu s sodno prakso Sodišča mora biti takšna intervencija dejansko primerna za to, da prispeva k odstranitvi takšne ovire. Kljub temu mora zakonodajalec Skupnosti v svoji intervenciji zagotoviti spoštovanje temeljnih pravic (člen 6(2) Pogodbe EU; glej oddelek II tega mnenja). Zaradi vsega tega lahko oblikovanje pravil na ravni Skupnosti o hrambi podatkov v korist notranjega trga zahteva, da se na ravni Evropske skupnosti obravnava tudi spoštovanje temeljnih pravic. Če zakonodajalec Skupnosti ne more oblikovati pravil za dostop do podatkov in njihovo uporabo, ne more izpolniti svoje obveznosti iz člena 6 Pogodbe EU, saj so ta pravila nujno potrebna za zagotovitev, da se podatki hranijo z ustreznim spoštovanjem temeljnih pravic. Povedano z drugimi besedami so po mnenju ENVP pravila za dostop, uporabo in izmenjavo podatkov neločljivo povezana s samo obveznostjo hrambe podatkov.

41. Kar se tiče vzpostavitve pristojnih organov ENVP priznava, da je to pristojnost držav članic. Enako velja za organizacijo kazenskega pregona in sodnega varstva. Kljub temu Skupnost lahko državam članicam naloži pogoje glede imenovanja pristojnih organov, sodnega nadzora ali dostopa državljanov do pravnega varstva. Te določbe zagotavljajo, da na nacionalni ravni obstajajo primerni mehanizmi za zagotovitev polne učinkovitosti akta, vključno s polnim upoštevanjem zakonodaje o varstvu podatkov.

42. ENVP odpira še eno točko, povezano s pravno podlago. Naloga zakonodaje Skupnosti je, da izbere ustrezno pravno podlago in skladno s tem ustrezen zakonodajni postopek. Ta izbira presega nalogo ENVP. Vendar se ENVP zaradi pomembnih temeljnih vprašanj, ki se tu obravnavajo, močno zavzema za postopek soodločanja. Ta postopek edini predstavlja pregleden postopek odločanja, v katerem polno sodelujejo tri vključene institucije, ter primerno spoštuje načela, na katerih temelji Unija.

IV. Potreba po uskladitvi

43. Predlog direktive usklajuje vrste podatkov, ki naj se hranijo, obdobja hrambe podatkov, pa tudi namene, za katere se podatki smejo predložiti pristojnim organom. Predlog predvideva popolno uskladitev teh elementov. V tej zvezi je povsem drugačne narave kot osnutek okvirnega sklepa, ki določa minimalna pravila.

44. ENVP poudarja potrebo po polni uskladitvi teh elementov zaradi delovanja notranjega trga, potreb kazenskega pregona in nenazadnje zaradi ECHR in načel o varstvu podatkov.

45. Kar se tiče delovanja notranjega trga, uskladitev obveznosti za hrambo podatkov upravičuje izbiro pravne podlage predloga (člen 95 Pogodbe ES). Dopuščanje osnovnih razlik med zakonodajo držav članic ne bo odpravilo obstoječih motenj na notranjem trgu elektronskih komunikacij, med drugim zaradi (bližnjega) sprejetja zakonodajnih ukrepov v državah članicah na podlagi člena 15 Direktive 2002/58/ES (glej točko 19 tega mnenja).

46. To je še bolj pomembno, ker za znaten del elektronskih komunikacij velja pristojnost več kot ene države članice. Na primer: čezmejni telefonski klici, gostovanje („roaming“), prečkanje meje *med* mobilnim komuniciranjem ter uporaba ponudnika v državi članici, ki ni država prebivališča posameznika.

47. Poleg tega bi v tej zvezi pomanjkljiva uskladitev škodila potrebam kazenskega pregona, če morajo pristojni organi upoštevati drugačne pravne zahteve. To bi lahko oviralo izmenjavo informacij med organi držav članic.

48. Na koncu ENVP poudarja – na podlagi svoje odgovornosti iz člena 41 Uredbe (ES) št. 45/2001 – da je popolna uskladitev glavnih elementov iz predloga nujno potrebna za skladnost z ECHR in načeli o varstvu podatkov. Vsak zakonodajni ukrep, ki obvezuje k hrambi podatkov o prometu in lokaciji, mora jasno omejiti število podatkov, ki naj se hranijo, obdobje hrambe ter (namen) dostopa do podatkov in njihove nadaljnje uporabe, da bo na ta način sprejemljiv s stališča varstva podatkov oziroma usklajen z zahtevami glede nujnosti in sorazmernosti.

V. **Pripombe v zvezi s členi predloga**

Člen 3: Obveznost hrambe podatkov

49. Člen 3 je glavna določba predloga. Člen 3(1) uvaja obveznost hrambe podatkov o prometu in lokaciji, člen 3(2) pa uveljavlja načelo omejitve namena. Člen 3(2) določa tri pomembne omejitve. Hranjeni podatki se lahko posredujejo le:

— pristojnim nacionalnim organom,

— v določenih primerih,

— za namene preprečevanja, preiskovanja, odkrivanja in pregona hujših kaznivih dejanj, kot sta terorizem in organizirani kriminal.

Člen 3(2) prepušča natančno opredelitev nadaljnjih omejitev nacionalni zakonodaji držav članic.

50. ENVP priznava člen 3(2) za pomembno določbo, vendar pa meni, da omejitve niso dovolj natančne, da je treba dostop in nadaljnjo uporabo izrecno urediti s predpisi v okviru direktive ter da so potrebna dodatna varovala. Kot je zapisano v oddelku III tega mnenja, ENVP ni prepričan, da je nevključitev (natančnih) določb o dostopu do podatkov in njihovi nadaljnji uporabi o prometu in lokaciji neizogibna posledica pravne podlage predloga (člen 95 Pogodbe ES). To pelje do naslednjih pripomb.

51. Na prvem mestu: ni natančno opredeljeno, da druge interesne skupine, tako kot sam ponudnik, nimajo dostopa do podatkov. Na podlagi člena 6 Direktive 2002/58/ES lahko ponudniki podatke o prometu obdelujejo le do poteka obdobja hrambe podatkov za namene zaračunavanja. Po mnenju ENVP dostop ponudnikov ali drugih interesnih skupin ni upravičen na drug način kot dostop, predviden v Direktivi 2002/58/ES in ob upoštevanju pogojev te direktive.

52. ENVP priporoča, da se v besedilu doda določba za zagotovitev, da posamezniki, razen pristojnih organov, nimajo dostopa do podatkov. Besedilo te določbe bi lahko bilo: „dostop do podatkov in/ali njihova obdelava sta mogoča le za namen iz člena 3(2)“ ali „ponudniki morajo učinkovito zagotoviti, da je dostop do podatkov dovoljen le pristojnim organom“.

53. Na drugem mestu: zdi se, da omejitev na določene primere prepoveduje rutinski dostop za lovljenje osebnih podatkov („fishing“) ali rudarjenje podatkov. Vendar je treba v besedilu predloga natančno opredeliti, da se podatki lahko posredujejo le, če so potrebni v zvezi z določenim kaznivim dejanjem.

54. Na tretjem mestu: ENVP pozdravlja dejstvo, da je namen dostopa omejen na hujša kazniva dejanja, kot sta terorizem in organizirani kriminal. V drugih, lažjih primerih, dostop do podatkov o prometu in lokaciji ne bo z lahkoto sorazmeren. Kljub temu ENVP izraža dvome, ali je ta omejitev dovolj natančna, zlasti takrat, ko bo prošnja za dostop povezana s hujšim kaznivim dejanjem, ki ni teroristično dejanje ali organizirani kriminal. Ta praksa se bo v državah članicah razlikovala. ENVP je v oddelku IV tega mnenja izpostavil potrebo po popolni uskladitvi glavnih elementov iz predloga. ENVP zato priporoča omejitev določbe na *določena* hujša kazniva dejanja.

55. Na četrtem mestu: v nasprotju z osnutkom okvirnega sklepa predlog ne vsebuje določbe o dostopu. Po mnenju ENVP se dostop in nadaljnja uporaba podatkov v direktivi ne smeta prezreti. Predstavljata neločljiv del zadeve (glej oddelek III tega mnenja).

56. ENVP priporoča, da se predlogu doda enega ali več členov o dostopu pristojnih organov do podatkov o prometu in lokaciji ter o nadaljnji uporabi podatkov. Cilj teh členov bi morala biti zagotovitev, da se podatki uporabljajo le za namene iz člena 3(2), da organi poskrbijo za kakovost, zaupnost in zaščito pridobljenih podatkov ter da bodo podatki potem, ko ne bodo več potrebni za preprečevanje, preisko-

vanje, odkrivanje in pregon določenih kaznivih dejanj, izbrisani. Poleg tega je treba določiti, da dostop v določenih primerih ne bo pod sodnim nadzorom držav članic.

57. Na petem mestu: predlog ne vsebuje dodatnih varoval za varstvo podatkov. V uvodnih izjavah je naveden enostaven sklic na varovala v obstoječi zakonodaji, zlasti na Direktivo 95/46/ES in Direktivo 2002/58/ES. ENVP se ne strinja s tem omejenim pristopom do varstva podatkov, kljub posebnemu pomenu (dodatnih) varoval (glej oddelek II tega mnenja).

58. Zato ENVP priporoča vključitev odstavka o varstvu podatkov. V ta odstavek bi se lahko vstavila prejšnja priporočila glede člena 3(2), pa tudi druge določbe o varstvu podatkov, na primer določbe o uveljavljanju pravic osebe, na katero se podatki nanašajo (glej oddelek II tega mnenja), kakovosti podatkov in zaščiti podatkov ter o podatkih o prometu in lokaciji oseb, ki niso osumljene kaznivih dejanj.

Člen 4: Kategorije podatkov, ki naj se hranijo

59. ENVP na splošno pozdravlja člen in prilogo, in sicer zaradi:

— izbrane zakonodajne tehnike s funkcionalnimi opisi v normativnem delu direktive ter tehničnimi podrobnostmi v prilogi. Dovolj je prilagodljiva, da se ustrezno odzove na tehnološki razvoj, državljanom pa zagotavlja pravno varnost,

— razlikovanja med podatki o telekomunikacijah in internetnimi podatki, kljub dejstvu, da razlikovanje s tehnološkega stališča postaja manj pomembno. S stališča varstva podatkov pa razlikovanje je pomembno, saj na internetu meja med podatki o vsebini in podatki o prometu ni jasna (glej npr. trditev iz člena 1(2) direktive, da so informacije, ki se jih pregleduje na internetu, podatki o vsebini),

— ravni uskladitve: predlog predvideva visoko raven uskladitve z obsežnim seznamom kategorij podatkov, ki naj se hranijo (v nasprotju z osnutkom okvirnega sklepa, ki vsebuje minimalni seznam in državam članicam pušča veliko manevrskega prostora za dodajanje novih podatkov). S stališča varstva podatkov je popolna uskladitev bistvenega pomena (glej oddelek IV).

60. ENVP priporoča naslednje spremembe:

— drugi odstavek člena 4 bi moral vsebovati več stvarnih meril za zagotovitev, da podatki o vsebini niso vključeni. Dodati bi bilo treba naslednji stavek: „Priloga ne sme vključevati podatkov, ki razkrivajo vsebino komunikacije“,

— člen 5 odpira možnost za revizijo priloge z direktivo Komisije („postopek v odboru“). ENVP svetuje, da bi morale biti revizije priloge s precejšnjim vplivom na varstvo podatkov po možnosti sprejete z direktivo, v skladu s postopkom soodločanja [1].

Člen 7: Obdobja hrambe

61. ENVP pozdravlja dejstvo, da so obdobja hrambe iz predloga precej krajša kot obdobja, predvidena v osnutku okvirnega sklepa:

— ob sklicevanju na dvome, ki so bili v tem mnenju izraženi glede dokazov o potrebi po hrambi podatkov o prometu do enega leta, enoletno obdobje odraža prakse kazenskega pregona, *kot so bile prikazane s številkami*, ki sta jih predložila Komisija in predsedstvo Sveta,

— te številke kažejo tudi, da hramba podatkov za daljša obdobja, razen v izjemnih primerih, ne odraža praks kazenskega pregona,

— obdobje, krajše od šestih mesecev, za podatke o elektronskih komunikacijah, ki se vršijo zgolj ali večinoma z uporabo internetnega protokola, je pomembno s stališča varstva podatkov, saj so posledica hrambe internetnih komunikacij obsežne zbirke podatkov (ti podatki se ponavadi ne hranijo za namene zaračunavanja), ločnica s podatki o vsebini je nejasna, hramba za dalj kot šest mesecev pa ne odraža praks kazenskega pregona.

62. V besedilu bi bilo treba pojasniti:

— da so šestmesečna oziroma enoletna obdobja hrambe najdaljša obdobja hrambe,

[1] V tej zvezi glej tudi mnenje ENVP z dne 23. marca 2005 o predlogu uredbe Evropskega parlamenta in Sveta o Vizumskem informacijskem sistemu (VIS) in izmenjavi podatkov o vizumih za kratkoročno bivanje med državami članicami (odst. 3.12).

— da so podatki po poteku obdobja hrambe izbrisani. Besedilo bi moralo tudi pojasniti, na kakšen način naj bodo podatki izbrisani. Po mnenju ENVP mora ponudnik z avtomatskimi sredstvi najmanj vsakodnevno brisati podatke.

Člen 8: Zahteve glede skladiščenja hranjenih podatkov

63. Ta člen je tesno povezan s členom 3(2) in vsebuje pomembno določbo, ki lahko zagotovi, da je dostop v določenih primerih lahko omejen zgolj na podatke, izrecno potrebne za ta primer. Člen 8 in člen 3(2) predpostavljata, da zahtevane podatke organom posredujejo ponudniki ter da organi nimajo neposrednega dostopa do zbirk podatkov. ENVP priporoča, da se ta predpostavka izrecno navede v besedilu.

64. Določbo bi bilo treba natančno opredeliti z navedbo:

— da podatke organom posredujejo ponudniki (glej točko 63),

— da morajo ponudniki namestiti potrebno tehnično infrastrukturo, vključno z iskalniki, za lažji natančen dostop do točno določenih podatkov,

— da bi morali ponudniki zagotoviti, da imajo dostop do zbirk podatkov iz tehničnih razlogov le člani njihovega osebja s posebnimi tehničnimi odgovornostmi, ter da se to osebje zaveda občutljivega značaja podatkov ter ravna v skladu s strogimi notranjimi predpisi o zaupnosti,

— da bi se moral prenos podatkov vršiti brez nepotrebnih zamud, pa tudi brez razkrivanja drugih podatkov o prometu in lokaciji, razen podatkov, ki so potrebni za namene prošnje.

Člen 9: Statistika

65. Obveznost ponudnikov, da letno pripravljajo statistične podatke, institucijam Skupnosti pomaga spremljati učinkovitost izvajanja in uporabo tega predloga. Potrebne so ustrezne informacije.

66. Po mnenju ENVP ta obveznost uveljavlja načelo preglednosti. Evropski državljan ima pravico vedeti, kako učinkovita je hramba podatkov. Iz tega razloga bi moral biti ponudnik še dodatno obvezan voditi sezname prijav in opravljati sistematične (samo-) revizije, s čimer bi nacionalnim organom za varstvo podatkov omogočil nadzor uporabe pravil o varstvu podatkov v praksi ([1]). Predlog bi bilo v tem smislu treba spremeniti.

Člen 10: Stroški

67. Kot je bilo zapisano v oddelku II, je med ustreznostjo varnostnih ukrepov in stroški teh ukrepov neposredna povezava, oziroma z drugimi besedami, med varnostjo in stroški. Po mnenju ENVP je zato člen 10 – ki določa povračilo dokazanih dodatnih stroškov – pomembna določba, ki bi lahko služila kot vzpodbuda za ponudnike, da vlagajo v tehnično infrastrukturo.

68. V skladu z ocenami presoje vpliva, ki jo je ENVP predložila Komisija, so stroški hrambe precejšnji. Za velikega ponudnika omrežja in storitev bi stroški za 12-mesečno obdobje hrambe presegli 150 milijonov EUR, z letnimi operativnimi stroški okoli 50 milijonov EUR ([2]). Ni pa številk o stroških dodatnih varnostnih ukrepov, kot so na primer iskalniki (glej pripombo glede člena 6), niti o (ocenjenih) finančnih posledicah celotnega povračila dodatnih stroškov ponudnikom.

69. Po mnenju ENVP so za celovito presojo predloga potrebne natančnejše številke. Predlaga pojasnitev finančnih posledic predloga v obrazložitvenem memorandumu.

70. Kar se tiče same določbe člena 10, bi moralo biti razmerje med ustreznostjo varnostnih ukrepov in stroški pojasnjeno v besedilu določbe. Poleg tega bi moral predlog predvideti minimalne standarde za varnostne ukrepe, ki naj jih sprejmejo ponudniki, da bi bili tako upravičeni do povračila stroškov s strani države članice. Po mnenju ENVP določitve

([1]) V tej zvezi glej tudi mnenje ENVP z dne 23. marca 2005 o predlogu uredbe Evropskega parlamenta in Sveta o Vizumskem informacijskem sistemu (VIS) in izmenjavi podatkov o vizumih za kratkoročno bivanje med državami članicami (odst. 3.9).

([2]) Komisija se sklicuje na številke ETNO (zveza telekomunikacijskih operaterjev EU) ter na poročilo poslanca Evropskega parlamenta Alvara o osnutku okvirnega sklepa.

teh standardov ne bi smeli v celoti prepustiti državam članicam. To bi lahko poseglo v raven uskladitve, predvidene z direktivo. Poleg tega je treba upoštevati, da finančne posledice povračila stroškov nosijo države članice.

Člen 11: Sprememba Direktive 2002/58/ES

71. Treba je pojasniti razmerje s členom 15(1) Direktive 2002/58/ES, saj ta predlog to določbo prikrajša za precej njene vsebine. Sklica v členu 15(1) Direktive 2002/58/ES na člen 6 in člen 9 (iste direktive) bi bilo treba črtati oziroma vsaj preoblikovati zaradi pojasnitve, da države članice niso več pristojne za sprejemanje zakonov v zvezi s kaznivimi dejanji, kar bi predstavljalo dopolnilo temu predlogu. Treba se je izogniti kakršni koli dvoumnosti glede preostalih pristojnosti – na primer v zvezi s hrambo podatkov za namen „lažjih“ kaznivih dejanj.

Člen 12: Ocenjevanje

72. ENVP pozdravlja dejstvo, da predlog vsebuje člen o ocenjevanju direktive v treh letih po začetku njene veljavnosti. Ocenjevanje je še posebej pomembno s stališča dvomov o nujnosti in sorazmernosti predloga.

73. S tega stališča ENVP svetuje določitev še strožje obveznosti, ki vsebuje naslednje elemente:

— ocenjevanje bi moralo zajeti presojo učinkovitosti izvajanja direktive s stališča kazenskega pregona, pa tudi presojo vpliva na temeljne pravice osebe, na katero se podatki nanašajo. Komisija bi morala vključiti vsak dokaz, ki bi lahko vplival na ocenjevanje,

— ocenjevanje bi bilo treba opravljati redno (vsaj na vsaki dve leti),

— Komisija bi morala biti obvezana po potrebi predložiti spremembe k predlogu (tako kot v členu 18 Direktive 2002/58/ES).

VI. **Sklepi**

Predpogoji

74. Po mnenju ENVP je bistveno, da predlog spoštuje temeljne pravice. Zakonodajni ukrep, ki bi škodil varstvu, zajamčenem z zakonodajo Skupnosti, ter še zlasti s sodno prakso Sodišča Evropskih skupnosti in Evropskega sodišča za človekove pravice, je ne samo nesprejemljiv, temveč tudi nezakonit.

75. Potrebo in sorazmernost obveznosti hrambe podatkov je treba dokazati, in sicer v polni meri.

76. Kar se tiče nujnosti: ENVP priznava spremembe okoliščin, a še ni prepričan o potrebi po hrambi podatkov o prometu in lokaciji za namene kazenskega pregona, kakor je opredeljeno v predlogu.

77. Kljub temu ENVP v tem mnenju podaja svoje stališče o sorazmernosti predloga. To na prvem mestu pomeni, da zgolj hramba podatkov o prometu in lokaciji ni ustrezen ali učinkovit odziv. Potrebni so dodatni ukrepi za zagotovitev, da imajo organi na voljo natančen in hiter dostop do podatkov, ki jih v določenem primeru potrebujejo. Na drugem mestu bi moral predlog:

— omejiti obdobja hrambe. Obdobja morajo odražati potrebe organov kazenskega pregona,

— omejiti število podatkov, ki naj se hranijo. To število mora odražati potrebe kazenskega pregona in zagotoviti, da dostop do podatkov o vsebini ni mogoč,

— vsebovati ustrezne varnostne ukrepe.

Splošna ocena

78. ENVP poudarja pomen dejstva, da to besedilo predloga predvideva popolno uskladitev glavnih elementov predloga, zlasti vrst podatkov, ki naj se hranijo, obdobja hrambe podatkov, pa tudi (namene) dostopa in nadaljnje uporabe podatkov.

79. V nekaterih točkah so potrebna dodatna pojasnila, da se na primer zagotovi, da so podatki po poteku obdobja hrambe ustrezno izbrisani ter da se različnim interesnim skupinam učinkovito preprečita dostop in uporaba.

80. Po mnenju ENVP so naslednje točke bistvenega pomena, da bi bil predlog sprejemljiv s stališča varstva podatkov:

— predlog bi bilo treba dopolniti s posebnimi določbami o dostopu do podatkov o prometu in lokaciji s strani pristojnih organov ter o nadaljnji uporabi podatkov, in sicer kot bistven in neločljiv del vsebine,

— predlog bi bilo treba dopolniti z nadaljnjimi dodatnimi varovali za varstvo podatkov (v nasprotju z enostavnim sklicevanjem na varovala v obstoječi zakonodaji, zlasti na Direktivo 95/46/ES in Direktivo 2002/58/ES), da se med drugim zagotovi uveljavljanje pravic oseb, na katere so podatki nanašajo,

— predlog bi bilo treba dopolniti z nadaljnjimi, tudi finančnimi vzpodbudami za ponudnike, da bi vlagali v ustrezno tehnično infrastrukturo. Ta infrastruktura je lahko ustrezna le, če obstajajo učinkoviti iskalniki.

Priporočila za preoblikovanje predloga

81. Kar se tiče člena 3(2):

— dodatek določbe za zagotovitev, da posamezniki, razen pristojnih organov, nimajo dostopa do podatkov. Besedilo te določbe bi lahko bilo: „dostop do podatkov in/ali njihova obdelava sta mogoča le za namen iz člena 3 (2)“ ali „ponudniki morajo učinkovito zagotoviti, da je dostop do podatkov dovoljen le pristojnim organom“,

— natančna opredelitev, da se podatki lahko posredujejo le v zvezi z določenim kaznivim dejanjem,

— omejitev določbe na *določena* hujša kazniva dejanja,

— dodatek enega ali več členov o dostopu pristojnih organov do podatkov o prometu in lokaciji ter o nadaljnji uporabi podatkov, pa tudi določbe, da mora biti dostop v določenih primerih pod sodnim nadzorom držav članic,

— vključitev odstavka o varstvu podatkov.

82. Kar se tiče členov 4 in 5:

— v drugem odstavku člena 4 dodatek naslednjega stavka: „Priloga ne sme vključevati podatkov, ki razkrivajo vsebino komunikacije.“,

— natančna opredelitev, da bi morale biti revizije priloge s precejšnjimi vplivi na varstvo podatkov po možnosti sprejete z direktivo, v skladu s postopkom soodločanja.

83. Kar se tiče člena 7, bi bilo treba v besedilu natančno opredeliti:

— da so šestmesečna oziroma enoletna obdobja hrambe najdaljša obdobja hrambe,

— da so podatki po poteku obdobja hrambe izbrisani. Besedilo bi moralo pojasniti tudi, na kakšen način naj bodo podatki izbrisani, in sicer ali to stori ponudnik z avtomatskimi sredstvi najmanj vsakodnevno.

84. Kar se tiče člena 8, bi bilo treba v besedilu natančno opredeliti:

— da zahtevane podatke organom posredujejo ponudniki,

— da bi morali ponudniki namestiti potrebno tehnično infrastrukturo, vključno z iskalniki, za lažji natančen dostop do točno določenih podatkov,

— da bi morali ponudniki zagotoviti, da imajo dostop do zbirk podatkov iz tehničnih razlogov le člani njihovega osebja s posebnimi tehničnimi odgovornostmi, ter da se to osebje zaveda občutljivega značaja podatkov ter ravna v skladu s strogimi notranjimi predpisi o zaupnosti,

— da bi se moral prenos podatkov vršiti brez nepotrebnih zamud, pa tudi brez razkrivanja drugih podatkov o prometu in lokaciji, razen podatkov, ki so potrebni za namene prošnje.

85. Kar se tiče člena 9:

— dodatek določbe, ki ponudnika obvezuje voditi sezname prijav in opravljati sistematične (samo-) revizije, s čimer bi nacionalnim organom za varstvo podatkov omogočil nadzor uporabe pravil o varstvu podatkov v praksi.

86. Kar se tiče člena 10:

— pojasnitev razmerja med ustreznostjo varnostnih ukrepov in stroški bi bilo treba pojasniti v besedilu določbe,

— dodatek minimalnih standardov za varnostne ukrepe, ki naj jih sprejmejo ponudniki, da bi bili tako upravičeni do povračila stroškov s strani države članice,

— pojasnitev finančnih posledic predloga v obrazložitvenem memorandumu.

87. Kar se tiče člena 11:

— sprememba člena 15(1) Direktive 2002/58/ES zaradi črtanja sklicev na člen 6 in člen 9 (iste direktive) oziroma vsaj preoblikovanja, da bi se pojasnilo, da države članice niso več pristojne za sprejemanje zakonov v zvezi s kaznivimi dejanji, kar bi predstavljalo dopolnilo temu predlogu.

88. Kar se tiče člena 12, sprememba določbe o ocenjevanju:

— zajemati bi morala presojo učinkovitosti izvajanja direktive,

— opravljati bi ga bilo treba redno (vsaj na vsaki dve leti),

— Komisija bi morala biti obvezana po potrebi predložiti spremembe k predlogu (tako kot v členu 18 Direktive 2002/58/ES).

V Bruslju, 26. septembra 2005.

Peter HUSTINX

Evropski nadzornik za varstvo podatkov