I

(Resolucije, priporočila in mnenja)

MNENJA

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV

Mnenje Evropskega nadzornika za varstvo podatkov o Sporočilu Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij – „Celovit pristop k varstvu osebnih podatkov v Evropski uniji“

(2011/C 181/01)

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 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]),

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:

A. **SPLOŠNI DEL**

1. **Uvod**

1.1 *Prva in splošna ocena*

1. Komisija je 4. novembra 2010 sprejela sporočilo z naslovom „Celovit pristop k varstvu osebnih podatkov v Evropski uniji“ (v nadaljnjem besedilu: Sporočilo) ([3]). Sporočilo je poslala Evropskemu nadzorniku za varstvo podatkov (ENVP) v posvetovanje. ENVP pozdravlja dejstvo, da se je Komisija z njim posvetovala v skladu s členom 41 Uredbe (ES) št. 45/2001. ENVP je imel tako še pred sprejetjem Sporočila možnost predložiti neformalne pripombe. Nekatere izmed teh pripomb so bile upoštevane v končni različici dokumenta.

2. Namen Sporočila je predstaviti pristop Komisije k pregledu pravnega sistema EU za varstvo osebnih podatkov na vseh področjih dejavnosti Unije ob upoštevanju zlasti izzivov, ki so posledica globalizacije in novih tehnologij ([4]).

3. ENVP na splošno pozdravlja Sporočilo, saj je prepričan, da je potreben pregled sedanjega pravnega okvira za varstvo podatkov v EU, da se zagotovi učinkovito varstvo v razvijajoči se informacijski družbi. ENVP je že v svojem mnenju z dne 25. julija 2007 o izvajanju Direktive o varstvu podatkov ([5]) sklenil, da se spremembe Direktive 95/46/ES z dolgoročnega vidika zdijo neizogibne.

4. Sporočilo je pomemben korak k taki zakonodajni spremembi, ki bo pomenila najpomembnejši razvoj na področju varstva podatkov v EU od sprejetja Direktive 95/46/ES, ki se na splošno šteje za temeljno izhodišče varstva podatkov v Evropski uniji (in širše v Evropskem gospodarskem prostoru).

5. Sporočilo zagotavlja ustrezen okvir za ciljno usmerjen pregled, tudi zato, ker so v njem – s splošnega vidika – opredeljena glavna vprašanja in izzivi. ENVP se strinja s stališčem Komisije, da bo v prihodnosti še vedno potreben trden sistem varstva podatkov, ki bo temeljil na dejstvu, da v družbi, ki doživlja temeljite spremembe zaradi hitrega tehnološkega razvoja in globalizacije, še vedno veljajo sedanja splošna načela varstva podatkov. V ta namen je treba pregledati veljavne zakonodajne ureditve.

([1]) UL L 281, 23.11.1995, str. 31.
([2]) UL L 8, 12.1.2001, str. 1.
([3]) COM(2010) 609 konč.
([4]) Glej str. 5 Sporočila, prvi odstavek.
([5]) Mnenje ENVP z dne 25. julija 2007 o Sporočilu Komisije Evropskemu parlamentu in Svetu o nadaljevanju delovnega programa za boljše izvajanje Direktive o varstvu podatkov, (UL C 255, 27.10.2007, str. 1).

6. V Sporočilu je pravilno poudarjeno, da so izzivi zelo veliki. ENVP se v celoti strinja s to izjavo in poudarja, da bi morale biti predlagane rešitve ustrezno ambiciozno zastavljene in naj bi okrepile učinkovitost varstva.

1.2 *Namen tega mnenja*

7. V tem mnenju so rešitve, predlagane v Sporočilu, ocenjene na podlagi dveh meril: ambicioznosti in učinkovitosti. Njegovo stališče je na splošno pozitivno. ENVP podpira Sporočilo, hkrati pa je kritičen glede vidikov, skladno s katerimi bi po njegovem mnenju večja ambicioznost vodila v učinkovitejši sistem.

8. ENVP želi s tem mnenjem prispevati k nadaljnjemu razvoju pravnega okvira o varstvu podatkov. Veseli se predloga Komisije, ki naj bi bil sprejet do sredine leta 2011, in upa, da bodo njegovi predlogi upoštevani v besedilu tega predloga. Poleg tega ugotavlja, da se zdi, da Sporočilo iz splošnega akta izključuje nekatera področja, kot je obdelava podatkov v institucijah in organih EU. Če bi se Komisija na obžalovanje ENVP dejansko odločila na tej stopnji izpustiti nekatera področja, jo ENVP poziva, da se zaveže, da bo v kratkem in točno določenem časovnem okviru zagotovila celovito strukturo.

1.3 *Gradniki tega mnenja*

9. To mnenje ni edino. Temelji na prejšnjih stališčih, ki so jih ob različnih priložnostih sprejeli ENVP in evropski organi za varstvo podatkov. Zlasti je treba poudariti, da so bili v že navedenem mnenju ENVP z dne 25. julija 2007 opredeljeni in pripravljeni nekateri najpomembnejši vidiki prihodnjih sprememb ([6]). To mnenje temelji tudi na razpravah z drugimi zainteresiranimi stranmi na področjih zasebnosti in varstva podatkov. Njihovi prispevki so zagotovili zelo koristno podlago za Sporočilo in to mnenje. V zvezi s tem je mogoče skleniti, da velja neka raven usklajenosti o tem, kako izboljšati učinkovitost varstva podatkov.

10. Še en pomemben gradnik tega mnenja je dokument z naslovom „Prihodnost zasebnosti“, ki je skupni prispevek k posvetovanju Evropske komisije iz leta 2009, ki sta ga sprejeli delovna skupina za varstvo podatkov iz člena 29 in delovna skupina za policijo in pravosodje (v nadaljnjem besedilu: „dokument WP o prihodnosti zasebnosti“) ([7]).

11. Pred kratkim je ENVP na tiskovni konferenci 15. novembra 2010 predstavil svoje prve odzive na zadevno sporočilo. V tem mnenju so natančneje razložena splošna stališča, ki so bila predstavljena na tej tiskovni konferenci ([8]).

12. Končno, to mnenje se opira na več prejšnjih mnenj ENVP ter na dokumente delovne skupine za varstvo podatkov iz člena 29. Kadar je to ustrezno, so na različnih mestih v tem mnenju navedena sklicevanja na navedena mnenja in dokumente.

2. **Ozadje**

13. Pregled pravil za varstvo podatkov se dogaja v pomembnem zgodovinskem trenutku. V Sporočilu je ozadje opisano obširno in prepričljivo. Na podlagi tega opisa je ENVP opredelil štiri glavne dejavnike, ki določajo okolje, v katerem se izvaja postopek pregleda.

14. Prvi dejavnik je tehnološki razvoj. Današnja tehnologija se razlikuje od tehnologije v času, ko je bila zasnovana in sprejeta Direktiva 95/46/ES. Tehnološki pojavi, kot so računalništvo v oblaku, vedenjsko oglaševanje, socialna omrežja, elektronsko cestninjenje in elektronske naprave za določanje zemljepisnega položaja, so temeljito spremenili način obdelave podatkov in pomenijo ogromne izzive za varstvo podatkov. Pri pregledu evropskih pravil za varstvo podatkov se bo treba učinkovito spopasti s temi izzivi.

15. Drugi dejavnik je globalizacija. Postopna odprava trgovinskih ovir je podjetjem omogočila vse večjo svetovno razsežnost. Čezmejna obdelava podatkov in mednarodni prenosi podatkov so se v zadnjih letih izredno povečali. Poleg tega je obdelava podatkov zaradi informacijskih in

([6]) Zlasti (glej točko 77 tega mnenja): spremembe sedanjih načel niso potrebne, jasno pa je, da obstaja potreba po drugačnih upravnih ureditvah; širokega področja uporabe zakonodaje o varstvu podatkov, ki velja za vse vrste uporabe osebnih podatkov, ne bi smeli spreminjati; zakonodaja o varstvu podatkov bi morala v konkretnih primerih omogočiti uravnotežen pristop, pa tudi, da organi za varstvo podatkov lahko določijo prednostne naloge; sistem bi moral v celoti veljati za uporabo osebnih podatkov v namene kazenskega pregona, čeprav bodo morda zaradi posebnih težav na tem področju potrebni ustrezni dodatni ukrepi.

([7]) Dokument WP 168 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf). Glavno sporočilo dokumenta je, da je zakonodajna sprememba dobra priložnost za razjasnitev nekaterih ključnih pravil in načel (na primer privolitev, preglednost), uvedbo nekaterih novih načel (na primer vgrajena zasebnost, odgovornost), okrepitev učinkovitosti s posodobitvijo ureditev (na primer z omejevanjem sedanjih zahtev glede priglasitve) in vključitev vseh v en celovit pravni okvir (vključno s policijskim in pravosodnim sodelovanjem).

([8]) Točke govora za tiskovno konferenco so na voljo na spletni strani ENVP: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-11-15_Press_conf_speaking_points_PHBG_EN.pdf

komunikacijskih tehnologij povsod razširjena: svetovni splet in računalništvo v oblaku sta omogočila delokalizirano obdelavo velikih količin podatkov na svetovni ravni. V zadnjem desetletju so se povečale tudi mednarodne policijske in pravosodne dejavnosti v boju proti terorizmu in drugim oblikam mednarodnega organiziranega kriminala, ki so podprte z izmenjavo ogromnih količin informacij za namene kazenskega pregona. Vse to kaže na potrebo po resnem razmisleku o tem, kako učinkovito zagotoviti varstvo osebnih podatkov v globaliziranem svetu, ne da bi pomembneje ovirali mednarodne postopke obdelave.

16. Tretji dejavnik je Lizbonska pogodba. Začetek veljavnosti Lizbonske pogodbe označuje novo dobo varstva podatkov. Člen 16 PDEU ne vsebuje le pravice posameznika, na katerega se podatki nanašajo, temveč zagotavlja tudi neposredno pravno podlago za trdno zakonodajo o varstvu podatkov na ravni EU. Poleg tega sta Evropski parlament in Svet z odpravo stebrne strukture zavezana k zagotovitvi varstva podatkov na vseh področjih zakonodaje EU. Z drugimi besedami, Lizbonska pogodba omogoča celovit pravni okvir za varstvo podatkov, ki se uporablja za zasebni sektor, javni sektor v državah članicah ter institucije in organe EU. Stockholmski program ([9]) v zvezi s tem dosledno navaja, da mora Unija poskrbeti za celovito strategijo na področju varstva podatkov znotraj EU in v odnosih s tretjimi državami.

17. Četrti dejavnik prinašajo vzporedne razvojne spremembe v okviru mednarodnih organizacij. Potekajo različne razprave o posodobitvi sedanjih pravnih aktov za varstvo podatkov. V zvezi s tem je treba omeniti sedanja razmišljanja v zvezi s prihodnjim pregledom Konvencije Sveta Evrope št. 108 ([10]) in Smernic o zasebnosti OECD ([11]). Še en pomemben razvoj zadeva sprejetje mednarodnih standardov o varstvu osebnih podatkov in zasebnosti, ki bi lahko privedli do sprejetja zavezujočega svetovnega dokumenta o varstvu podatkov. Vse te pobude si zaslužijo polno podporo. Njihov skupni cilj bi moral biti zagotavljanje učinkovitega in doslednega varstva v globaliziranem okolju, ki temelji na tehnološkem napredku.

3. **Glavni vidiki**

3.1 *Varstvo podatkov spodbuja zaupanje in mora podpirati druge (javne) interese*

18. Trden okvir za varstvo podatkov je nujna posledica pomembnosti, pripisane varstvu podatkov na podlagi Lizbonske pogodbe, zlasti v členu 8 Listine Evropske unije o temeljnih pravicah in členu 16 PDEU ter v močni povezavi s členom 7 Listine ([12]).

19. Ob tem pa je trden okvir za varstvo podatkov uporaben tudi širšim javnim in zasebnim interesom v informacijski družbi, v kateri je povsod razširjena obdelava podatkov. Varstvo podatkov spodbuja zaupanje, ta pa je ključni element dobrega delovanja naše družbe. Ključno je, da so ureditve na področju varstva podatkov takšne, da kolikor je le mogoče aktivno podpirajo druge zakonite pravice in interese, namesto da jih ovirajo.

20. Pomembni primeri drugih zakonitih interesov so močno evropsko gospodarstvo, varnost posameznikov in odgovornost vlad.

21. Gospodarski razvoj v Evropski uniji poteka vzporedno z uvajanjem in trženjem novih tehnologij in storitev. V informacijski družbi sta pojav in uspešna uvedba informacijskih in komunikacijskih tehnologij in storitev odvisna od zaupanja. Če ljudje IKT ne zaupajo, bodo te tehnologije verjetno neuspešne ([13]). Ljudje pa bodo IKT zaupali le, če so njihovi podatki učinkovito zavarovani. Varstvo podatkov bi zato moralo biti sestavni del tehnologij in storitev. Trden okvir za varstvo podatkov spodbuja evropsko gospodarstvo, vendar mora biti ta okvir ne le trden, temveč tudi ustrezno prilagojen. V tem pogledu sta nujna nadaljnje usklajevanje v EU in zmanjšanje upravnih bremen (glej poglavje 5 tega mnenja).

22. V zadnjih letih je bilo veliko govora o potrebi po uravnoteženosti med zasebnostjo in varnostjo, zlasti v zvezi z instrumenti za obdelavo in izmenjavo podatkov na področju policijskega in pravosodnega sodelovanja ([14]). Varstvo podatkov je bilo pogosto napačno zaznamovano kot ovira za polno zaščito fizične varnosti posameznikov ([15]) ali pa vsaj kot neizogibno stanje, ki ga morajo spoštovati organi kazenskega pregona. Vendar pa to ni celotna zgodba. Trden okvir za varstvo podatkov lahko izboljša in okrepi varnost. Na podlagi načel varstva podatkov – ko se ti ustrezno izvajajo – morajo upravljavci zagotoviti, da so informacije točne in posodobljene ter da so odvečni osebni podatki, ki niso potrebni za namene

([9]) Stockholmski program – odprta in varna Evropa, ki služi državljanom in jih varuje, (UL C 115, 4.5.2010, str. 1), na strani 10.

([10]) Konvencija Sveta Evrope št. 108 o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, ETS št. 108, 28. januarja 1981.

([11]) Smernice OECD o varovanju zasebnosti in čezmejnem prenosu osebnih podatkov, objavljene na http://www.oecd.org

([12]) To pomembnost varstva podatkov in povezavo z zasebnostjo v Listini je poudarilo Sodišče v sodbi z dne 9. novembra 2010, združeni zadevi C-92/09 in C-93/09, *Schecke*, še neobjavljena v ZOdl.

([13]) Glej mnenje ENVP z dne 18. marca 2010 o krepitvi zaupanja v informacijsko družbo s spodbujanjem varstva podatkov in zasebnosti, (UL C 280, 16.10.2010, str. 1), odst. 113.

([14]) Glej na primer Mnenje ENVP z dne 10. julija 2009 o sporočilu Komisije Evropskemu parlamentu in Svetu o območju svobode, varnosti in pravice za državljane, (UL C 276, 17.9.2009, str. 8).

([15]) Varnost je širši pojem kot fizična varnost, vendar je za ponazoritev zadevnih argumentov tukaj uporabljena v ožjem smislu.

kazenskega pregona, odstranjeni iz sistemov. Enak pomen je mogoče pripisati obveznostim izvajanja tehnoloških in organizacijskih ukrepov za zagotavljanje varnosti sistemov, na primer varovanje sistemov pred nepooblaščenim razkritjem ali dostopom, kot je razvito na področju varstva podatkov.

23. S spoštovanjem načel varstva podatkov se lahko zagotovi tudi, da organi kazenskega pregona delujejo v skladu z načeli pravne države, kar vzbuja zaupanje v njihovo ravnanje in tako v širšem smislu spodbuja zaupanje v naših družbah. Sodna praksa, ki je bila razvita na podlagi člena 8 Evropske konvencije o človekovih pravicah, zagotavlja, da lahko policijski in pravosodni organi obdelajo vse podatke, pomembne za svoje delo, vendar tega ne morejo izvajati neomejeno. Za varstvo podatkov je potreben sistem preverjanja in ravnovesja (glej poglavje 9 tega mnenja o policiji in pravosodju).

24. V demokratičnih družbah so vlade odgovorne za vse svoje dejavnosti, vključno z uporabo osebnih podatkov za različne javne interese, za katere delujejo. To zajema dejavnosti od objave podatkov na svetovnem spletu zaradi preglednosti do uporabe podatkov kot podpore strategijam na področjih, kot so javno zdravje, prevoz ali obdavčenje oziroma nadzor posameznikov za namene kazenskega pregona. Trden okvir varstva podatkov vladam omogoča spoštovanje svojih odgovornosti in da so odgovorne v smislu dobrega upravljanja.

3.2 *Posledice za pravni okvir varstva podatkov*

3.2.1 Potrebno je nadaljnje usklajevanje

25. V Sporočilu je pravilno ugotovljeno, da je ena od ključnih pomanjkljivosti sedanjega okvira, da državam članicam pušča preveč prosto presojo pri prenašanju evropskih določb v nacionalno zakonodajo. Pomanjkanje usklajevanja ima številne negativne posledice v informacijski družbi, kjer so fizične meje med državami članicami čedalje manj pomembne (glej poglavje 5 tega mnenja).

3.2.2 Še vedno veljajo splošna načela varstva podatkov

26. Prvi in formalnejši razlog, zakaj se splošna načela varstva podatkov ne smejo in ne morejo spreminjati, je pravne narave. Ta načela so opredeljena v Konvenciji Sveta Evrope št. 108, ki zavezuje vse države članice. Ta konvencija je podlaga za varstvo podatkov v EU. Poleg tega je nekaj glavnih načel izrecno navedenih v členu 8 Listine Evropske unije o temeljnih pravicah. Spreminjanje teh načel bi tako zahtevalo spreminjanje pogodb.

27. Vendar pa to ni celotna zgodba. So še tehtni razlogi proti spreminjanju splošnih načel. ENVP trdno verjame, da informacijska družba ne more in ne sme delovati brez ustreznega varstva zasebnosti in osebnih podatkov posameznikov. Kadar se obdeluje več podatkov, je potrebno tudi boljše varstvo. Informacijska družba, v kateri se obdelujejo ogromne količine informacij o vsakomer, mora temeljiti na konceptu nadzora, ki ga izvaja posameznik, da se mu oziroma ji omogoči, da deluje kot posameznik in uresničuje svoje svoboščine v demokratični družbi, kot sta svoboda izražanja in govora.

28. Poleg tega si je težko predstavljati nadzor posameznika brez obveznosti upravljavcev, da omejijo obdelavo v skladu z načeli nujnosti, sorazmernosti in omejitve namena. Enako težko si je predstavljati nadzor, ki ga izvaja posameznik, če niso priznane pravice posameznikov, na katere se nanašajo podatki, kot so pravice do dostopa, popravka, izbrisa ali blokiranja podatkov.

3.2.3 Vidik temeljnih pravic

29. ENVP poudarja, da je varstvo podatkov priznano kot temeljna pravica. To ne pomeni, da mora varstvo podatkov vedno *prevladati* nad drugimi pomembnimi pravicami in interesi v demokratični družbi, ima pa posledice za naravo in področje uporabe varstva, ki mora biti zagotovljeno v skladu s pravnim okvirom EU, da se zagotovi, da se zahteve v zvezi z varstvom podatkov vedno *ustrezno* upoštevajo.

30. Te glavne posledice je mogoče opredeliti, kakor sledi:

— varstvo mora biti učinkovito. Pravni okvir mora zagotoviti instrumente, ki posameznikom omogočajo, da svoje pravice uveljavljajo v praksi,

— okvir mora biti dolgoročno stabilen,

— varstvo mora biti zagotovljeno v vseh okoliščinah in ne sme biti odvisno od političnih preferenc v nekem obdobju,

— omejitve pri uveljavljanju pravic so lahko potrebne, vendar morajo biti izjemne, ustrezno utemeljene in ne smejo nikoli prizadeti ključnih elementov same pravice ([16]).

ENVP priporoča, da Komisija upošteva te posledice pri oblikovanju predlogov za zakonodajne rešitve.

3.2.4 Potrebne so nove zakonodajne ureditve

31. Sporočilo je pravilno osredotočeno na potrebo po okrepitvi zakonodajnih ureditev za varstvo podatkov. V zvezi s tem je smiselno opozoriti, da so organi za varstvo podatkov v dokumentu WP o prihodnosti zasebnosti ([17]) poudarili potrebo po močnejših vlogah različnih

([16]) Glej tudi Mnenje ENVP z dne 25. julija 2007 o Sporočilu Komisije Evropskemu parlamentu in Svetu o nadaljevanju delovnega programa za boljše izvajanje Direktive o varstvu podatkov, odst. 17, ki temelji na sodni praksi Evropskega sodišča za človekove pravice in Sodišča Evropske unije.

([17]) Prim. opombo 7.

udeležencev na področju varstva podatkov, zlasti posameznikov, na katere se nanašajo podatki, upravljavcev podatkov in samih nadzornih organov.

32. Zdi se, da se zainteresirane strani na splošno strinjajo, da so trdnejše zakonodajne ureditve – ob upoštevanju tehnološkega razvoja in globalizacije – ključne za ambiciozno zastavljeno in učinkovito varstvo podatkov tudi v prihodnosti. Kot je že navedeno v točki 7, sta to merili, na podlagi katerih ENVP ocenjuje vse predlagane rešitve.

3.2.5 Celovitost kot temeljni pogoj

33. Kot je poudarjeno v Sporočilu, se Direktiva 95/46/ES uporablja za vse postopke obdelave osebnih podatkov v državah članicah v javnem in zasebnem sektorju, razen dejavnosti, ki ne spadajo na področje uporabe prejšnje zakonodaje Skupnosti ([18]). Medtem ko je bila ta izjema potrebna v okviru prejšnje Pogodbe, po začetku veljavnosti Lizbonske pogodbe ni več tako. Še več, izjema je celo v nasprotju z besedilom in celo duhom člena 16 PDEU.

34. Po mnenju ENVP je treba celovit pravni akt za varstvo podatkov, vključno s policijskim in pravosodnim sodelovanjem v kazenskih zadevah, razumeti kot eno glavnih izboljšav, ki jih lahko prinese novi pravni okvir. To je temeljni pogoj za učinkovito varstvo podatkov v prihodnosti.

35. ENVP v podporo tej trditvi poudarja naslednje argumente:

— razlike med dejavnostmi zasebnega sektorja in sektorja kazenskega pregona so čedalje manj jasne. Subjekti zasebnega sektorja lahko obdelujejo podatke, ki se na koncu uporabljajo za namene kazenskega pregona (primer: podatki iz evidence imen letalskih potnikov – PNR ([19])), v drugih primerih pa se od njih zahteva, da hranijo podatke za namene kazenskega pregona (primer: Direktiva o hrambi podatkov ([20])),

— v skladu z Direktivo 95/46/ES ni pomembne razlike med policijskimi in pravosodnimi organi ter drugimi organi, ki izvajajo kazenski pregon (obdavčenje, carina, boj proti goljufijam, priseljevanje),

— kot je pravilno opisano v Sporočilu, je pravni akt za varstvo podatkov, ki se trenutno uporablja za policijske in pravosodne organe (Okvirni sklep 2008/977/PNZ ([21])), neustrezen.

— večina držav članic je v svojo nacionalno zakonodajo prenesla Direktivo 95/46/ES in Konvencijo št. 108, s čimer so zagotovile, da se ta dva akta uporabljata tudi za njihove policijske in pravosodne organe.

36. Vključitev policije in pravosodja v splošni pravni akt bi zagotovilo več jamstva za državljane in olajšalo delo policijskim organom. Uporaba različnih sklopov pravil je zapletena, po nepotrebnem zahteva veliko časa in ovira mednarodno sodelovanje (glej poglavje 9 tega mnenja). To je tudi argument za vključevanje postopkov obdelave, ki jih izvajajo nacionalne varnostne službe, če je to mogoče v okviru sedanje zakonodaje EU.

3.2.6 Tehnološka nevtralnost

37. Obdobje od sprejetja Direktive 95/46/ES leta 1995 je mogoče opisati kot tehnološko burno obdobje. Nove tehnološke razvojne spremembe in naprave se uvajajo zelo pogosto. To je velikokrat povzročilo pomembne spremembe v načinu obdelave osebnih podatkov posameznikov. Informacijska družba se ne more več šteti za vzporedno okolje, v katerem lahko posamezniki prostovoljno sodelujejo, temveč je postala sestavni del našega vsakdanjega življenja. Tako na primer pojem internet stvari ([22]) povezuje fizične predmete in spletne informacije, ki se na njih nanašajo.

38. Tehnologija se bo še naprej razvijala. To pa ima posledice za nov pravni okvir. Ta mora biti učinkovit dolga leta, hkrati pa ne sme ovirati nadaljnjega tehnološkega razvoja. Zato morajo biti pravne ureditve tehnološko nevtralne. Vendar pa mora okvir zagotoviti tudi več pravne varnosti za podjetja in posameznike. Ti morajo razumeti, kaj se od njih pričakuje, in biti sposobni uveljavljati svoje pravice. Zato morajo biti pravne ureditve natančne.

39. ENVP meni, da mora biti splošni pravni akt za varstvo podatkov oblikovan čim bolj tehnološko nevtralno. To pomeni, da morajo biti pravice in obveznosti različnih udeležencev oblikovane splošno in nevtralno, da lahko načeloma ostanejo veljavne in izvršljive ne glede na izbrano tehnologijo, izbrano za obdelavo osebnih podatkov. Glede na današnji hiter tehnološki napredek ni nobene druge izbire. ENVP poleg veljavnih načel varstva

([18]) To mnenje je osredotočeno predvsem na nekdanji tretji steber EU (policijsko in pravosodno sodelovanje v kazenskih zadevah), ker je nekdanji drugi steber ne le bolj zapleteno področje zakonodaje EU (kot je priznano tudi v členu 16 PDEU in členu 39 EU), temveč tudi manj pomemben za obdelavo podatkov.

([19]) Glej na primer Sporočilo Komisije o globalnem pristopu k prenosu podatkov iz evidence imen letalskih potnikov (PNR) tretjim državam, COM(2010) 492 konč.

([20]) Direktiva 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (UL L 105, 13.4.2006, str. 54).

([21]) Okvirni sklep Sveta 2008/977/PNZ z dne 27. novembra 2008 o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah (UL L 350, 30.12.2008, str. 60)

([22]) Kot je opredeljeno v sporočilu „Internet stvari – akcijski načrt za Evropo“, COM(2009) 278 konč.

podatkov predlaga uvedbo novih „tehnološko nevtralnih“ pravic, ki bi lahko imele poseben pomen v hitro spreminjajočem se elektronskem okolju (glej predvsem poglavji 6 in 7).

3.2.7 Dolgoročni vidik: pravna varnost v daljšem obdobju

40. Direktiva 95/46/ES je že 15 let osrednji dokument na področju varstva podatkov v Evropski uniji. Prenesena je bila v zakonodajo držav članic, uporabljali pa so jo različni udeleženci. Z leti se je njeno izvajanje izboljšalo na podlagi praktičnih izkušenj in dodatnih smernic Komisije, organov za varstvo podatkov (na nacionalni ravni in v okviru delovne skupine iz člena 29) ter nacionalnih in evropskih sodišč.

41. Poudariti je treba, da te razvojne spremembe trajajo dlje časa in da je – zlasti ker gre za splošni okvir, ki omogoča uveljavljanje temeljne pravice – za ustvarjanje pravne varnosti in stabilnosti potreben tak daljši čas. Nov splošni pravni akt mora biti oblikovan s ciljem, da bo lahko ustvaril pravno varnost in stabilnost v daljšem obdobju, ob upoštevanju, da je zelo težko napovedati, kako se bosta v prihodnje razvijali tehnologija in globalizacija. Vsekakor pa ENVP v celoti podpira cilj ustvarjanja pravne varnosti v daljšem obdobju, kar je primerljivo z vidikom Direktive 95/46/ES. Skratka, ob hitrem razvoju tehnologije mora biti zakonodaja stabilna.

3.2.8 Kratkoročni vidik: boljše izkoriščanje sedanjih instrumentov

42. Kratkoročno je ključno zagotoviti učinkovitost veljavnih zakonodajnih ureditev, predvsem z osredotočanjem na izvrševanje na nacionalni ravni in ravni EU (glej poglavje 11 tega mnenja).

B. **ELEMENTI NOVEGA OKVIRA**

4. **Celovit pristop**

43. ENVP v celoti podpira celovit pristop k varstvu podatkov, ki ni le naslov, temveč je tudi izhodiščna točka Sporočila in nujno vključuje razširitev splošnih pravil o varstvu podatkov na policijsko in pravosodno sodelovanje v kazenskih zadevah ([23]).

44. Vendar še ugotavlja, da Komisija ne namerava v ta splošni pravni akt vključiti vseh postopkov obdelave podatkov. Zlasti ne bo vključena obdelava podatkov v institucijah, organih, uradih in agencijah Evropske unije. Komisija navaja le, da bo „ocenila potrebo po prilagoditvi drugih pravnih aktov novemu splošnemu okviru za varstvo podatkov“.

([23]) Glej str. 14 Sporočila in oddelek 3.2.5 tega mnenja.

45. ENVP daje jasno prednost vključitvi obdelave podatkov na ravni EU v splošni pravni okvir. Opozarja, da je bil to prvotni namen prejšnjega člena 286 PES, v katerem je bilo varstvo podatkov prvič omenjeno na ravni Pogodbe. V členu 286 PES je navedeno le, da se pravni akti o obdelavi osebnih podatkov uporabljajo tudi za institucije. Kar je še pomembnejše, z enim pravnim besedilom bi se izognili tveganju neskladnosti med določbami in bi zagotovili najprimernejši način izmenjave podatkov med ravnjo EU ter javnimi in zasebnimi subjekti v državah članicah. Izognili bi se tudi tveganju, da po spremembi Direktive 95/46/ES ne bi bilo več političnega interesa za spremembo Uredbe (ES) št. 45/2001 ali da ne bi dali tej spremembi zadostne prednosti v izogib neskladnosti v datumih začetka veljavnosti.

46. ENVP poziva Komisijo, da se ta – če bi sklenila, da vključitev obdelave podatkov na ravni EU v splošni pravni akt ne bi bila izvedljiva – zaveže, da bo predlagala prilagoditev Uredbe (ES) št. 45/2001 (ne pa „ocenila potrebo“) v najkrajšem možnem času, po možnosti do konca leta 2011.

47. Enako pomembno je, da Komisija zagotovi, da se ne izključijo niti druga področja, zlasti:

— varstvo podatkov pri izvajanju skupne zunanje in varnostne politike na podlagi člena 39 PEU ([24]),

— ureditve na področju varstva podatkov v posameznih sektorjih za organe EU, kot sta Europol in Eurojust, ter za velike informacijske sisteme, če jih je treba prilagoditi novemu pravnemu aktu,

— Direktiva 2002/58 o e-zasebnosti, če jo je treba prilagoditi novemu pravnemu aktu.

48. Končno, splošni pravni akt za varstvo podatkov se lahko in ga je verjetno tudi treba dopolniti z dodatnimi sektorskimi in posebnimi predpisi, na primer na področju policijskega in pravosodnega sodelovanja ter tudi na drugih področjih ([25]). Kjer je to potrebno in skladno z načelom subsidiarnosti, je treba navedene dodatne predpise sprejeti na ravni EU. Države članice lahko na posebnih področjih, kjer je to utemeljeno, pripravijo dodatna pravila (glej 5.2).

([24]) Glej tudi Mnenje ENVP z dne 24. novembra 2010 o Sporočilu Komisije Evropskemu parlamentu in Svetu – „Politika EU za boj proti terorizmu: glavni dosežki in izzivi za prihodnost“, točka 31.

([25]) Glej tudi dokument WP o prihodnosti zasebnosti (opomba 7), točke 18–21.

5. **Nadaljnje usklajevanje in poenostavitev**

5.1 *Potreba po usklajevanju*

49. Usklajevanje je izredno pomembno za zakonodajo EU na področju varstva podatkov. V Sporočilu je pravilno poudarjeno, da ima varstvo podatkov močno razsežnost notranjega trga, saj mora zagotoviti prost pretok osebnih podatkov med državami članicami na notranjem trgu. Vendar pa je usklajevanje v okviru sedanje Direktive ocenjeno pod zadovoljivo ravnjo. V Sporočilu je ugotovljeno, da je to eden od glavnih pomislekov zainteresiranih strani. Zainteresirane strani so zlasti poudarile potrebo po večji pravni varnosti, zmanjšanju upravnih bremen ter zagotovitvi enakih pogojev za gospodarske subjekte. Kot je Komisija pravilno ugotovila, to še posebej zadeva upravljavce podatkov, ki imajo sedež v več državah članicah in morajo upoštevati (po možnosti različne) zahteve nacionalnih zakonov na področju varstva podatkov ([26]).

50. Usklajevanje ni pomembno le za notranji trg, temveč tudi z vidika zagotavljanja ustreznega varstva podatkov. V členu 16 PDEU je določeno, da ima „vsakdo“ pravico do varstva osebnih podatkov, ki se nanašajo nanj. Da bi se ta pravica dejansko spoštovala, mora biti po vsej Evropski uniji zagotovljena enakovredna raven varstva. V dokumentu WP o prihodnosti zasebnosti je poudarjeno, da se več določb v zvezi s stališči posameznikov, na katere se podatki nanašajo, ne izvaja ali razlaga enotno v vseh državah članicah ([27]). V globaliziranem in povezanem svetu bi lahko te razlike ogrozile ali omejile varstvo posameznikov.

51. ENVP meni, da je nadaljnje in izboljšano usklajevanje eden od glavnih ciljev postopka pregleda. ENVP pozdravlja zavezo Komisije, da bo proučila sredstva za nadaljnje usklajevanje predpisov o varstvu podatkov na ravni EU. Vendar pa nekoliko presenečeno ugotavlja, da v Sporočilu na tej stopnji niso predstavljene nobene konkretne možnosti Zato sam navaja nekaj področij, na katerih je večja uskladitev najbolj potrebna (glej 5.3). Nadaljnje usklajevanje na teh področjih bi bilo treba doseči ne le z zmanjšanjem manevrskega prostora v nacionalni zakonodaji, temveč tudi s preprečevanjem nepravilnega izvajanja v državah članicah (glej tudi poglavje 11) in z zagotavljanjem bolj doslednega in usklajenega izvrševanja (glej tudi poglavje 10).

5.2 *Zmanjšanje manevrskega prostora pri izvajanju Direktive*

52. Direktiva vsebuje veliko določb, ki so oblikovane splošno in zato dopuščajo precej manevrskega prostora za različno izvajanje. V uvodni izjavi 9 Direktive je izrecno potrjeno, da je državam članicam puščen manevrski prostor in da bi se lahko v mejah tega manevrskega prostora pojavila neskladja pri izvajanju Direktive. Več določb se različno izvaja v državah članicah, vključno z nekaterimi ključnimi določbami ([28]). Razmere niso zadovoljive in doseči je treba večjo uskladitev.

53. To ne pomeni, da je treba razlike popolnoma odpraviti. Na nekaterih področjih je morda potrebna prilagodljivost, da se ohranijo upravičene posebnosti, pomembni javni interesi ali institucionalna samostojnost držav članic. Po mnenju ENVP mora biti manevrski prostor za razlike med državami članicami omejen zlasti na naslednje posebne okoliščine:

— svoboda izražanja: v skladu s sedanjim okvirom (člen 9) lahko države članice določijo izjeme ali odstopanja za obdelavo podatkov, ki se izvaja v novinarske namene ali zaradi umetniškega ali literarnega izražanja. Glede na različne tradicije in kulturne razlike, ki lahko veljajo v državah članicah na tem področju, se zdi ta prilagodljivost dobro zasnovana, seveda v skladu z omejitvami iz Listine in Evropske konvencije o človekovih pravicah. Vendar pa to ne bo oviralo morebitne posodobitve sedanjega člena 9 glede na razvoj svetovnega spleta,

— posebni javni interesi: v skladu s sedanjim okvirom (člen 13) lahko države članice sprejmejo predpise za omejitev obsega obveznosti in pravic, kadar taka omejitev predstavlja potrebni ukrep za zaščito pomembnega javnega interesa, kot so državna varnost, obramba, javna varnost itd. Ta pristojnost držav članic je še naprej upravičena. Vendar pa je treba, kadar je to mogoče, razlago izjem dodatno uskladiti (glej oddelek 9.1). Poleg tega se zdi, da je sedanji obseg izjem od člena 6(1) neupravičeno velik,

— pravna sredstva, sankcije in upravni postopki: evropski okvir bi moral določiti glavne pogoje, vendar je treba v skladu s sedanjo zakonodajo EU opredelitev sankcij, pravnih sredstev, postopkovnih pravil in možnosti za pregledovanje, kot se uporabljajo na nacionalni ravni, prepustiti državam članicam.

([26]) Sporočilo, str. 10.

([27]) Glej dokument WP o prihodnosti zasebnosti (opomba 7), točka 70. Dokument se zlasti sklicuje na določbe o odgovornosti in možnosti odškodninskih zahtevkov za nematerialno škodo.

([28]) Nekaj različnih pristopov je vezanih tudi na ročno vnesene podatke.

5.3 *Področja za nadaljnje usklajevanje*

54. *Opredelitev pojmov* (člen 2 Direktive 95/46/ES). Opredelitve pojmov so temeljno izhodišče pravnega sistema in jih je treba razlagati enotno v vseh državah članicah, in to brez manevrskega prostora pri izvajanju. Na podlagi sedanjega okvira so nastale razlike, kot na primer glede pojma upravljavec ([29]). ENVP predlaga, da se za zagotovitev večje pravne varnosti na sedanji seznam v členu 2 dodajo še drugi pojmi, kot so anonimni podatki, psevdonimni podatki, pravosodni podatki, prenos podatkov in pooblaščenec za varstvo podatkov.

55. *Zakonitost obdelave (člen 5).* Nov pravni akt mora biti čim bolj natančen, kar zadeva osnovne elemente za opredelitev zakonitosti obdelave podatkov. Člen 5 (in uvodna izjava 9) Direktive, ki določa, da morajo države članice natančneje določiti pogoje, po katerih je obdelava zakonita, tako v prihodnjem okviru morda ne bo več potreben.

56. *Razlogi za obdelavo podatkov* (člena 7 in 8). Opredelitev pogojev za obdelavo podatkov je ključni element vsake zakonodaje o varstvu podatkov. Državam članicam se ne bi smelo dovoliti, da uvedejo dodatne ali spremenjene razloge za obdelavo ali da izključijo kateri koli razlog. Možnost odstopanja je treba izključiti ali omejiti (zlasti v zvezi z občutljivimi podatki ([30])). V novem pravnem aktu je treba jasno oblikovati razloge za obdelavo podatkov in s tem zmanjšati možnosti prostega preudarka pri izvajanju ali izvrševanju. Zlasti je morda treba dodatno opredeliti pojem privolitve (glej oddelek 6.5). Poleg tega razlog, ki temelji na zakonitih interesih upravljavca podatkov (člen 7(f)), zaradi svoje prilagodljive narave dopušča zelo različne razlage. Potrebna je dodatna opredelitev. Določba, ki jo je tudi verjetno treba dodatno opredeliti, je člen 8(2)(b), ki dopušča obdelavo občutljivih podatkov, potrebno zaradi izpolnjevanja obveznosti in posebnih pravic upravljavca na področju prava zaposlovanja ([31]).

57. *Pravice posameznikov, na katere se nanašajo podatki* (členi 10–15). To je eno od področij, na katerih države članice niso dosledno izvajale in razlagale vseh elementov Direktive. Pravice posameznikov, na katere se nanašajo podatki, so osrednji element učinkovitega varstva podatkov. Zato je treba znatno zmanjšati manevrski prostor. ENVP priporoča, da so informacije, ki jih upravljavec posreduje posameznikom, na katere se nanašajo podatki, enotne po vsej EU.

58. *Mednarodni prenosi* (členi 25–26). To področje je zaradi pomanjkanja enotne prakse po vsej EU spodbudilo veliko kritike. Zainteresirane strani so imele pomisleke, da države članice zelo različno razlagajo in izvajajo odločitve Komisije o ustreznosti. ENVP predlaga nadaljnje usklajevanje tudi na področju zavezujočih poslovnih pravil (Binding Corporate Rules, BCR) (glej poglavje 9).

59. *Nacionalni organi za varstvo podatkov* (člen 28). Za nacionalne organe za varstvo podatkov veljajo zelo različna pravila v 27 državah članicah, zlasti kar zadeva njihov status, sredstva in pooblastila. K tem razlikam je delno prispeval člen 28 zaradi nezadostne natančnosti ([32]), zato ga je treba dodatno opredeliti v skladu s sodbo Sodišča v zadevi C-518/07 ([33]) (glej tudi poglavje 10).

5.4 *Poenostavitev sistema obveščanja*

60. Tudi na področju zahtev glede obveščanja (členi 18–21 Direktive 95/46/ES) je bila do zdaj državam članicam prepuščena precejšnja svoboda. V Sporočilu je pravilno priznano, da bi usklajen sistem zmanjšal stroške in upravna bremena za upravljavce podatkov ([34]).

61. Na tem področju bi moral biti glavni cilj poenostavitev. Pregled okvira za varstvo podatkov je edinstvena priložnost za nadaljnjo poenostavitev in/ali zmanjšanje področja uporabe sedanjih zahtev glede obveščanja. Sporočilo priznava, da se zainteresirane strani na splošno strinjajo, da je sedanji sistem obveščanja precej neroden in kot tak brez prave dodane vrednosti za varstvo osebnih podatkov posameznikov ([35]). ENVP zato pozdravlja zavezo Komisije, da bo proučila različne možnosti za poenostavitev sedanjega sistema obveščanja.

62. Po mnenju ENVP bi bila izhodiščna točka za tako poenostavitev prehod s sistema, v katerem je obveščanje pravilo, razen kadar je določeno drugače (tj. „sistem oprostitev"), na bolj ciljno usmerjen sistem. Sistem oprostitev se je izkazal za neučinkovitega, saj se ni dosledno izvajal v vseh državah članicah ([36]). ENVP predlaga, da se proučijo naslednje možnosti:

([29]) Glej Mnenje delovne skupine iz člena 29 1/2010 o pojmih „upravljavec" in „obdelovalec" (WP 169).

([30]) Člen 8(4) in (5) zdaj pod določenimi pogoji dovoljuje državam članicam, da določijo dodatna odstopanja v zvezi z občutljivimi podatki.

([31]) V zvezi s tem glej zgoraj navedeno prvo poročilo Komisije o izvajanju direktive o varstvu podatkov, str. 14.

([32]) Dokument WP o prihodnosti zasebnosti, odst. 87.

([33]) Zadeva C-518/07, *Komisija proti Nemčiji*, še neobjavljena v ZOdl.

([34]) Prim. opombo 26.

([35]) Prim. opombo 26.

([36]) Poročilo delovne skupine iz člena 29 o obveznosti obveščanja nacionalnih nadzornih organov, čim boljšem izkoriščanju izjem in poenostavitev ter vlogi pooblaščencev za varstvo podatkov v Evropski uniji, WP 106, 2005, str. 7.

— omejitev obveznosti obveščanja na posebne vrste postopkov obdelave, ki pomenijo posebne nevarnosti (ta obveščanja lahko povzročijo nadaljnje korake, kot je predhodno preverjanje obdelave),

— obveznost preproste prijave, v skladu s katero se morajo upravljavci prijaviti (v nasprotju z obsežno prijavo vseh postopkov obdelave podatkov).

Poleg tega bi se lahko uvedel enotni vseevropski obrazec za obveščanje, ki bi zagotovil usklajene pristope glede zahtevanih informacij.

63. Pregled sedanjega sistema obveščanja ne bi smel posegati v izboljšanje obveznosti predhodnega preverjanja za nekatere obveznosti obdelave, ki lahko pomenijo posebne nevarnosti (kot so veliki informacijski sistemi). ENVP podpira vključitev neizčrpnega seznama primerov, ko je potrebno tako predhodno preverjanje, v nov pravni akt. V ta namen je Uredba (ES) št. 45/2001 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih EU koristen model ([37]).

5.5 *Uredba, ne direktiva*

64. Končno, ENVP meni, da je postopek pregleda tudi priložnost za ponovno proučitev vrste pravnega akta za varstvo podatkov. Uredba je kot enotni akt, ki se neposredno uporablja v državah članicah, najučinkovitejši način zaščite temeljne pravice do varstva podatkov in oblikovanja resničnega notranjega trga, na katerem je mogoč prost pretok osebnih podatkov in kjer je raven varstva enaka neodvisno od države ali sektorja, kjer se podatki obdelujejo.

65. Uredba bi zmanjšala manevrski prostor za nasprotujoče si razlage in neutemeljene razlike pri izvajanju in uporabi zakonodaje. Zmanjšala bi tudi pomen določanja prava, ki se uporablja za postopke obdelave v EU, ki je eden najbolj spornih vidikov sedanjega sistema (glej poglavje 9).

66. Na področju varstva podatkov je uredba veliko bolj utemeljena, ker

— je v členu 16 PDEU pravica do varstva osebnih podatkov dvignjena na raven Pogodbe in je predvidena – oziroma celo določena – enotna raven varstva posameznikov po vsej EU,

— se obdelava podatkov izvaja v elektronskem okolju, kjer so notranje meje med državami članicami postale manj pomembne.

67. Izbira uredbe kot splošnega akta po potrebi omogoča, da so določbe naslovljene neposredno na države članice, kadar je potrebna prilagodljivost. Poleg tega ne vpliva na pristojnost držav članic, da po potrebi sprejmejo dodatna pravila za varstvo podatkov v skladu z zakonodajo EU.

6. **Krepitev pravic posameznikov**

6.1 *Potreba po krepitvi pravic*

68. ENVP v celoti podpira predlog Komisije glede krepitve pravic posameznikov, saj sedanji pravni akti ne zagotavljajo povsem učinkovitega varstva, potrebnega v čedalje bolj zapletenem digitaliziranem svetu.

69. Po eni strani razvoj digitaliziranega sveta prinaša s seboj močno povečanje izredno zapletenega in nepreglednega zbiranja, uporabe in nadaljnjega prenosa osebnih podatkov. Posamezniki se pogosto ne zavedajo ali ne razumejo, kako se to zgodi, kdo zbira njihove podatke ali kako izvajati nadzor. Primer takega pojava je spremljanje dejavnosti spletnega brskanja posameznikov, ki ga izvajajo ponudniki oglaševalskih omrežij z uporabo piškotkov ali podobnih naprav za namene ciljnega oglaševanja. Ko uporabniki obiščejo spletne strani, ne pričakujejo, da nevidna tretja stran zapisuje take obiske in ustvarja evidence o uporabnikih na podlagi informacij, ki razkrivajo njihov življenjski slog oziroma kaj imajo radi in česa ne marajo.

70. Po drugi strani pa razvoj spodbuja posameznike, da si proaktivno izmenjujejo svoje osebne informacije, na primer v okviru socialnih omrežij. Čedalje več mladih ljudi se vključuje v socialna omrežja in tako komunicira z vrstniki. Malo verjetnosti je, da se (mladi) ljudje zavedajo razsežnosti svojega razkritja podatkov in dolgoročnih učinkov svojih dejanj.

6.2 *Povečanje preglednosti*

71. Preglednost je izredno pomembna v vsakem sistemu varstva podatkov, ne le zaradi svoje nedvomne vrednosti, temveč tudi zato, ker omogoča izvajanje drugih načel varstva podatkov. Posamezniki lahko uveljavljajo svoje pravice le, če vedo za obdelavo podatkov.

72. V Direktivi 95/46/ES več določb obravnava preglednost. Člena 10 in 11 vsebujeta obveznost zagotavljanja informacij posameznikom o zbiranju njihovih osebnih podatkov. Poleg tega je v členu 12 priznana pravica do prejema kopije posameznikovih osebnih podatkov v razumljivi obliki (pravica do dostopa). V členu 15 je priznana pravica do dostopa do logike, na podlagi katere so sprejete avtomatizirane odločitve, ki imajo pravne učinke. Ne nazadnje je zahteva glede preglednosti vključena tudi v člen 6.1(a), ki določa pošteno obdelavo podatkov. Osebnih podatkov ni mogoče obdelovati na podlagi prikritih ali tajnih razlogov.

([37]) Glej člen 27 Uredbe, (UL L 8, 12.1.2001, str. 1).

73. V Sporočilu se predlaga uvedba splošnega načela preglednosti. ENVP v zvezi s tem predlogom poudarja, da je pojem preglednosti že sestavni del sedanjega pravnega okvira za varstvo podatkov, čeprav implicitno. To je mogoče sklepati iz različnih določb, ki obravnavajo preglednost, kot je navedeno v prejšnjem odstavku. Po mnenju ENVP bi lahko dodano vrednost prinesla vključitev *izrecnega* načela preglednosti, ki je lahko povezano s sedanjo določbo o pošteni obdelavi ali ne. S tem bi se povečala pravna varnost in poudarila obveznost upravljavca, da mora osebne podatke obdelovati pregledno v vseh okoliščinah, ne le na zahtevo ali kadar tako določajo posebni predpisi.

74. Vendar je morda še pomembnejše okrepiti sedanje določbe, ki obravnavajo preglednost, kot sta sedanja člena 10 in 11 Direktive 95/46/ES. V navedenih določbah so opredeljene informacije, ki se morajo zagotoviti, niso pa natančno opredeljeni načini. ENVP konkretneje predlaga, da se sedanje določbe okrepijo z:

— zahtevo, da mora upravljavec zagotavljati informacije o obdelavi podatkov na način, ki je lahko dostopen in razumljiv ter v jasnem in preprostem jeziku ([38]). Informacije morajo biti jasne, opazne in dobro vidne. Določba lahko vključuje tudi obveznost zagotovitve preprostega razumevanja informacij. Na podlagi te obveznosti bi se politike zasebnosti, ki so nejasne ali težko razumljive, štele za nezakonite,

— zahtevo, da je treba informacije zagotavljati na preprost način in neposredno posameznikom, na katere se nanašajo podatki. Informacije morajo biti tudi stalno dostopne, ne pa po zelo kratkem času izginiti iz elektronskega medija. To bi uporabnikom pomagalo, da informacije shranijo in jih v prihodnosti kopirajo, kar omogoča nadaljnji dostop.

6.3 *Podpora obveznosti obveščanja o kršitvah varstva podatkov*

75. ENVP podpira uvedbo določbe o obveščanju o kršitvah varstva osebnih podatkov v splošni akt, ki razširja obveznost, ki je v spremenjeni direktivi o e-zasebnosti veljala le za nekatere ponudnike, na vse upravljavce podatkov, kot je predlagano v Sporočilu. V skladu s spremenjeno direktivo o e-zasebnosti obveznost velja le za ponudnike elektronskih komunikacijskih storitev (ponudniki storitev telefonije (vključno z govorom po omrežju IP) in spletnega dostopa). Drugi upravljavci podatkov niso vključeni v obveznost. Razlogi, ki upravičujejo obveznost, pa se v celoti nanašajo na upravljavce podatkov, ki niso ponudniki elektronskih komunikacijskih storitev.

76. Obveščanje o kršitvah varstva podatkov ima različne namene in cilje. Najočitnejši namen, poudarjen v Sporočilu, je njegova uporaba kot orodje za ozaveščanje posameznikov o nevarnostih, ki so jim izpostavljeni, ko so ogroženi njihovi osebni podatki. To jim lahko pomaga, da sprejmejo potrebne ukrepe za zmanjšanje takih nevarnosti. Posamezniki bodo na primer lahko, ko bodo opozorjeni o kršitvah, ki zadevajo njihove finančne informacije, med drugim spremenili geslo ali zaprli svoj račun. Poleg tega obveščanje o kršitvah varstva podatkov prispeva k učinkovitemu izvajanju drugih načel in obveznosti iz Direktive. Na primer, zahteve glede obveščanja o kršitvah varstva podatkov spodbujajo upravljavce podatkov, da izvajajo strožje varnostne ukrepe za preprečevanje kršitev. Obveščanje o kršitvah varstva podatkov je tudi orodje za krepitev odgovornosti upravljavcev podatkov in zlasti za povečanje odgovornosti (glej poglavje 7). Končno, kot orodje za izvrševanje ga uporabljajo tudi organi za varstvo podatkov. Obveščanje organov za varstvo podatkov o kršitvah lahko vodi v preiskavo vseh postopkov upravljavca podatkov.

77. Med parlamentarno obravnavo zakonodajnega okvira, ki je potekala pred sprejetjem direktive o e-zasebnosti, je potekala obširna razprava o posebnih pravilih v zvezi s kršitvami varstva podatkov v spremenjeni direktivi o e-zasebnosti. Med to razpravo so bila upoštevana mnenja delovne skupine iz člena 29 in ENVP, skupaj s stališči drugih zainteresiranih strani. Pravila vsebujejo stališča različnih zainteresiranih strani. Pri tem gre za ravnovesje interesov – merila za določanje obveznosti obveščanja so načeloma ustrezna za zaščito posameznikov, vendar pri tem ne nalagajo čezmerno obremenjujočih in nekoristnih zahtev.

6.4 *Okrepitev privolitve*

78. V členu 7 direktive o varstvu podatkov je naštetih šest pravnih podlag za obdelavo osebnih podatkov. Ena od njih je privolitev posameznika. Upravljavec podatkov lahko obdeluje osebne podatke v takem obsegu, za kakršnega so posamezniki dali prostovoljno privolitev, da se njihovi podatki zbirajo in nadalje obdelujejo.

79. V praksi imajo uporabniki pogosto omejen nadzor glede svojih podatkov, zlasti v tehnoloških okoljih. Ena od metod, ki se včasih uporablja, je domnevna privolitev, to je kadar se sklepa, da gre za privolitev. To se lahko sklepa iz dejanja posameznika (na primer dejanje, ki vključuje uporabo spletne strani, se šteje kot privolitev,

([38]) Glej Sporočilo, str. 6.

da se uporabnikovi podatki zapišejo za namene trženja). Privolitev se lahko sklepa tudi iz molka ali neukrepanja (če uporabnik ne odznači kljukice v okencu, se šteje, da je dal privolitev).

80. V skladu z Direktivo je privolitev veljavna, če je informirana, prostovoljna in posebna. Privolitev mora biti informirana izjava volje, s katero posameznik izrazi soglasje, da se osebni podatki o njem obdelujejo. Privolitev mora biti dana nedvoumno.

81. Privolitev, ki se sklepa iz dejanja in zlasti iz molka ali neukrepanja, pogosto ni nedvoumna privolitev. Vendar pa ni vedno jasno, kaj pomeni resnična, nedvoumna privolitev. Nekateri upravljavci podatkov izkoriščajo to negotovost tako, da se opirajo na metode, ki niso ustrezne za zagotovitev resnične, nedvoumne privolitve.

82. Glede na zgoraj navedeno ENVP podpira stališče Komisije, da je treba pojasniti omejitve glede privolitve in zagotoviti, da se za privolitev šteje le tista, ki je jasno razumljena kot taka. V zvezi s tem ENVP predlaga naslednje ([39]):

— morda bi bilo treba razmisliti o razširitvi situacij, v katerih je potrebna izrecna privolitev in ki so trenutno omejene na občutljive podatke,

— sprejetje dodatnih pravil za privolitev v spletnem okolju,

— sprejetje dodatnih pravil za privolitev glede obdelave podatkov za sekundarne namene (tj. obdelava, ki se izvaja poleg glavne obdelave ali ni očitna),

— v dodatnem zakonodajnem aktu, ne glede na to, ali ga sprejme Komisija v skladu s členom 290 PDEU ali ne, opredeliti vrsto potrebne privolitve, na primer za določitev ravni privolitve za obdelavo podatkov iz oznak RFID na potrošniških izdelkih ali za druge posebne tehnike.

6.5 *Prenosljivost podatkov in pravica biti pozabljen*

83. Prenosljivost podatkov in pravica biti pozabljen sta povezana pojma, predstavljena v Sporočilu za okrepitev pravic posameznikov, na katere se nanašajo podatki. Dopolnjujeta načela, ki so že navedena v Direktivi, tako da določata pravico posameznika, na katerega se nanašajo podatki, da nasprotuje nadaljnji obdelavi svojih osebnih podatkov, in obveznost upravljavca podatkov, da izbriše podatke takoj, ko niso več potrebni za namene obdelave.

84. Ta dva nova pojma imata po navadi dodano vrednost v okolju informacijske družbe, v kateri se čedalje več podatkov avtomatično shranjuje in hrani neomejen čas. Praksa kaže, da imajo celo posamezniki, ki so sami naložili podatke, dejansko zelo omejen nadzor nad svojimi osebnimi podatki. To je toliko bolj očitno glede na velikanski spomin, ki ga ima danes svetovni splet. Poleg tega je z ekonomskega vidika za upravljavca podatkov dražje brisati kot pa hraniti podatke. Uresničevanje pravic posameznikov je zato v nasprotju z naravnim gospodarskim gibanjem.

85. Prenosljivost podatkov in pravica biti pozabljen bi lahko prispevali k spremembi ravnovesja v prid posameznika, na katerega se nanašajo podatki. Cilj prenosljivosti podatkov bi bil posamezniku zagotoviti več nadzora nad svojimi informacijami, pravica biti pozabljen pa bi zagotovila, da informacije po določenem času avtomatično izginejo, tudi če posameznik, na katerega se nanašajo podatki, ne ukrepa ali se niti ne zaveda, da so bili podatki shranjeni.

86. Natančneje, prenosljivost podatkov se razume kot sposobnost uporabnikov, da spremenijo stališče glede obdelave svojih podatkov, zlasti v povezavi s storitvami nove tehnologije. To se čedalje bolj nanaša na storitve, ki vključujejo shranjevanje informacij, vključno z osebnimi podatki, kot je mobilna telefonija, in storitve, ki vključujejo shranjevanje slik, elektronske pošte in drugih informacij, včasih z uporabo storitev računalništva v oblaku.

87. Posamezniki morajo imeti možnost, da preprosto in svobodno zamenjajo ponudnika in prenesejo svoje osebne podatke drugemu ponudniku storitev. ENVP meni, da bi se lahko veljavne pravice iz Direktive 95/46/ES okrepile z vključitvijo pravice do prenosljivosti podatkov, zlasti v zvezi s storitvami informacijske družbe, da bi se posameznikom pomagalo zagotoviti, da jim ponudniki in drugi zadevni upravljavci omogočijo dostop do osebnih informacij ter da prejšnji ponudniki ali drugi upravljavci izbrišejo take informacije, tudi če bi jih želeli ohraniti zaradi svojih zakonitih namenov.

88. Na novo uzakonjena „pravica biti pozabljen“ bi zagotovila izbris osebnih podatkov ali prepoved njihove nadaljnje uporabe, ne da bi moral posameznik, na katerega se podatki nanašajo, ukrepati, vendar pod pogojem, da so

([39]) Delovna skupina iz člena 29 trenutno pripravlja mnenje o „privolitvi“. Na podlagi tega mnenja bodo morda oblikovani dodatni predlogi.

bili ti podatki določen čas že shranjeni. Z drugimi besedami, podatkom bi se določil neke vrste rok uporabe. To načelo so že potrdila nacionalna sodišča v svojih zadevah ali pa je bilo uporabljeno v posebnih sektorjih, na primer za policijske, kazenske ali disciplinske evidence. Tako se v skladu z nekaterimi nacionalnimi zakonodajami informacije o posameznikih avtomatično izbrišejo ali se ne smejo nadalje uporabljati ali razširjati, zlasti po določenem časovnem obdobju, brez potrebe po predhodni analizi za vsak primer posebej.

89. V tem smislu bi morala biti nova „pravica biti pozabljen“ povezana s prenosljivostjo podatkov. Njena dodana vrednost bi bila, da si posamezniku, na katerega se nanašajo podatki, ne bi bilo treba prizadevati ali zahtevati, da se njegovi podatki izbrišejo, saj bi se to izvajalo objektivno in avtomatično. Le v zelo posebnih okoliščinah, v katerih bi se lahko ugotovila posebna potreba po daljšem hranjenju podatkov, bi lahko imel upravljavec podatkov pravico hraniti podatke. Navedena „pravica biti pozabljen“ bi tako dokazno breme prenesla s posameznika na upravljavca podatkov in bi vključevala nastavitev „vgrajene zasebnosti“ za obdelavo osebnih podatkov.

90. ENVP meni, da bi bila lahko pravica biti pozabljen zlasti koristna v zvezi s storitvami informacijske družbe. Obveznost, da je treba informacije izbrisati ali da se jih ne sme nadalje razširjati po določenem časovnem obdobju, je smiselna zlasti za sredstva javnega obveščanja ali svetovni splet in socialna omrežja. Koristna bi bila tudi v zvezi s terminalsko opremo: podatki, shranjeni na prenosnih napravah ali računalnikih, bi se avtomatično izbrisali ali blokirali po določenem časovnem obdobju, ko posameznik ne razpolaga več z njimi. V tem smislu bi se lahko pravica biti pozabljen prenesla v obveznost „vgrajene zasebnosti“.

91. Skratka, ENVP meni, da sta prenosljivost podatkov in pravica biti pozabljen koristni. Morda bi ju bilo koristno vključiti v pravni akt, verjetno pa bi ju omejili na elektronsko okolje.

6.6 *Obdelava osebnih podatkov, povezanih z otroki*

92. Direktiva 95/46/ES ne določa posebnih pravil glede obdelave osebnih podatkov o otrocih. Zato se ne priznava potreba po posebni zaščiti otrok v posebnih okoliščinah zaradi njihove ranljivosti in ker to povzroča pravno negotovost, zlasti na naslednjih področjih:

— zbiranje podatkov o otrocih in način obveščanja otrok o zbiranju,

— način pridobivanja privolitve otrok. Ker ni posebnih pravil o načinu pridobivanja privolitve otrok in o starosti, do katere se oseba šteje za otroka, se to področje ureja z nacionalno zakonodajo, ki se razlikuje med državami članicami ([40]),

— način in pogoji, v skladu s katerimi lahko otroci in njihovi zakoniti zastopniki uveljavljajo svoje pravice na podlagi Direktive.

93. ENVP meni, da bi bili posebni interesi otrok bolje zaščiteni, če bi novi pravni akt vseboval dodatne določbe, ki bi posebej obravnavale zbiranje in nadaljnjo obdelavo podatkov o otrocih. Take posebne določbe bi zagotovile tudi pravno varnost na tem posebnem področju in prinesle koristi upravljavcem podatkov, ki morajo trenutno izpolnjevati različne zakonske zahteve.

94. ENVP predlaga, da se v pravni akt vključijo naslednje določbe:

— zahteva, da morajo biti informacije prilagojene otrokom, če bi to otrokom omogočilo lažje razumevanje pomena zbiranja podatkov o njih,

— otrokom je treba prilagoditi druge zahteve po informacijah glede načina zagotavljanja informacij in po možnosti tudi glede njihove vsebine,

— posebna določba o zaščiti otrok pred vedenjskim oglaševanjem,

— načelo omejitve namena bi bilo treba okrepiti v zvezi s podatki o otrocih,

— nekatere kategorije podatkov se ne bi nikoli smele zbirati od otrok,

— starostna meja, pod katero bi se lahko informacije na splošno zbirale od otrok le z izrecno in preverljivo privolitvijo staršev,

— če je potrebna privolitev staršev, bi bilo treba določiti pravila o dokazovanju starosti otroka ali z drugimi

([40]) Privolitev je običajno povezana s starostjo, pri kateri lahko otroci sklenejo pogodbene obveznosti. To je starost, ko naj bi otroci dosegli določeno raven zrelosti. Na primer španska zakonodaja zahteva privolitev staršev za zbiranje podatkov o otrocih, mlajših od 14 let. Nad to starostjo se šteje, da lahko otroci sami dajo privolitev. V Združenem kraljestvu se Zakon o varstvu podatkov ne sklicuje na določeno starost ali starostno mejo. Vendar pa lahko po razlagi organa za varstvo podatkov v Združenem kraljestvu privolitev dajo otroci, starejši od 12 let. Otroci, mlajši od 12 let, tako ne morejo sami dati privolitve, zato je za pridobivanje njihovih osebnih podatkov najprej treba pridobiti dovoljenje staršev ali skrbnikov.

besedami, kako vedeti, da je otrok mladoleten, in kako preveriti privolitev staršev. Na tem področju se lahko EU zgleduje po drugih državah, kot so Združene države Amerike ([41]).

6.7 *Mehanizmi skupinskih tožb*

95. Krepitev vsebine pravic posameznikov je nesmiselna, če ni učinkovitih postopkovnih mehanizmov za izvrševanje takih pravic. V zvezi s tem ENVP priporoča, da se v zakonodajo EU uvedejo mehanizmi skupinskih tožb za kršenje pravil o varstvu podatkov. Mehanizmi skupinskih tožb, ki skupinam državljanov omogočajo, da združijo svoje zahtevke v skupno tožbo, so lahko zelo močno orodje za lažje izvrševanje pravil o varstvu podatkov ([42]). To novost podpirajo tudi organi za varstvo podatkov v dokumentu WP o prihodnosti zasebnosti.

96. V zadevah z manjšim učinkom je malo verjetnosti, da bi žrtve kršitve pravil o varstvu podatkov vložile posamezne tožbe zoper upravljavce glede na stroške, zamude, negotovosti, tveganja in obremenitve, ki bi jim bile izpostavljene. Te težave bi bilo mogoče premostiti ali znatno zmanjšati, če bi se vzpostavil sistem skupinskih tožb, s katerimi bi bilo žrtvam kršitev omogočeno, da svoje posamezne zahtevke združijo v skupno tožbo. ENVP bi podprl tudi pooblastitev pooblaščenih subjektov, kot so združenja potrošnikov ali javni organi, za vlaganje odškodninskih tožb v imenu žrtev kršitev varstva podatkov. Te tožbe pa ne bi smele posegati v pravico posameznikov, na katere se nanašajo podatki, da vložijo posamezne tožbe.

97. Skupinske tožbe so pomembne ne le za zagotavljanje polne odškodnine ali drugih popravnih ukrepov, temveč posredno zagotavljajo tudi večji odvračalni učinek. Tveganje dragih kolektivnih odškodnin zaradi takih tožb bi upravljavce bolj spodbudilo k učinkovitemu zagotavljanju skladnosti. V zvezi s tem bi okrepljeno zasebno izvrševanje z mehanizmi skupinskih tožb dopolnjevalo javno izvrševanje.

98. V Sporočilu ni opredeljeno stališče glede tega vprašanja. ENVP se zaveda, da na evropski ravni poteka razprava o uvedbi kolektivnih odškodnin za potrošnike. Prav tako se zaveda nevarnosti pretiranih odškodnin, ki jih lahko spodbudijo ti mehanizmi na podlagi izkušenj v drugih pravnih sistemih. Vendar pa po njegovem mnenju ti dejavniki ne pomenijo zadostnih argumentov za zavrnitev ali odložitev uvedbe teh mehanizmov v zakonodajo o varstvu podatkov glede na koristi, ki bi jih prinesli ([43]).

7. **Okrepitev vloge organizacij/upravljavcev**

7.1 *Splošno*

99. ENVP meni, da mora sodoben pravni akt za varstvo podatkov poleg okrepitve pravic posameznikov vsebovati potrebna orodja, ki povečujejo odgovornost upravljavcev podatkov. Natančneje, akt mora zlasti vsebovati spodbude za upravljavce podatkov v zasebnem ali javnem sektorju, da bi ti v svoje poslovne postopke proaktivno uvajali ukrepe za varstvo podatkov. Prvič, ta orodja bi bila koristna, ker je, kot je že omenjeno, tehnološki razvoj povzročil močno povečanje zbiranja, uporabe in nadaljnjega prenosa osebnih podatkov, kar še dodatno ogroža zasebnost in varstvo osebnih podatkov posameznikov, zato se je treba tega učinkovito lotiti. Drugič, sedanji akt – razen nekaj podrobno opredeljenih določb (glej spodaj) – ne vsebuje takih orodij, zato lahko upravljavci podatkov zavzamejo *reaktivni* pristop k varstvu podatkov in zasebnosti ter ukrepajo šele, ko se pojavi težava. Tak pristop je razviden iz statističnih podatkov, ki kažejo na ponavljajoče se težave zaradi nezadostne skladnosti s predpisi in izgube podatkov.

100. Po mnenju ENVP sedanji akt ne zadostuje za učinkovito varstvo osebnih podatkov v sedanjih razmerah in v prihodnosti. Večja kot so tveganja, večja je potreba po izvajanju konkretnih ukrepov, ki varujejo podatke na praktični ravni in zagotavljajo učinkovito zaščito. Če se ti proaktivni ukrepi ne bodo *dejansko* izvedli, se bodo še naprej dogajale napake, nesreče in malomarnosti, ki bodo ogrožale zasebnost posameznikov v čedalje bolj digitalizirani družbi. Za dosego tega ENVP predlaga naslednje ukrepe.

7.2 *Okrepitev odgovornosti upravljavcev podatkov*

101. ENVP priporoča, da se v pravni akt vstavi nova določba, s katero se od upravljavcev podatkov zahteva, da sprejmejo ustrezne in učinkovite ukrepe za izvajanje načel in obveznosti pravnega akta in to na zahtevo dokažejo.

([41]) V ZDA je v zakonu COPPA določeno, da morajo operaterji komercialnih spletnih strani ali spletnih storitev, namenjenih otrokom, mlajšim od 13 let, pridobiti privolitev staršev pred zbiranjem osebnih podatkov, in da se morajo operaterji komercialnih strani za splošno občinstvo dejansko zavedati, da so otroci posebni obiskovalci.

([42]) Glej tudi Mnenje ENVP z dne 25. julija 2007 o Sporočilu Komisije Evropskemu parlamentu in Svetu o nadaljevanju delovnega programa za boljše izvajanje Direktive o varstvu podatkov, (UL C 255, 27.10.2007, str. 10).

([43]) V nekaterih nacionalnih zakonodajah so že določen podobni mehanizmi.

102. Take vrste določba ni popolnoma nova. Člen 6(2) Direktive 95/46/ES se sklicuje na načela v zvezi s kakovostjo podatkov in določa, da mora „upravljavec zagotoviti, da se ravna v skladu z odstavkom 1“. Poleg tega člen 17(1) določa, da morajo upravljavci podatkov izvajati ustrezne tehnične in organizacijske ukrepe. Vendar pa imajo te določbe omejeno področje uporabe. Vključitev splošne določbe o odgovornosti bi spodbudila upravljavce, da uvedejo proaktivne ukrepe, ki bi jim omogočili uskladitev z vsemi elementi zakonodaje o varstvu podatkov.

103. Posledica določbe o odgovornosti bi bila, da bi se od upravljavcev podatkov zahtevalo, da uvedejo notranje mehanizme in sisteme nadzora za zagotovitev skladnosti z načeli in obveznostmi iz akta. To bi na primer pomenilo vključevanje najvišjega vodstva v politike varstva podatkov, postopke opredelitve za zagotovitev ustrezne identifikacije vseh postopkov obdelave informacij, uvedbo zavezujočih politik varstva podatkov, ki jih je treba stalno pregledovati in posodabljati za vključitev novih postopkov obdelave informacij, skladnost z načeli kakovosti podatkov, obveščanja, varnosti, dostopa itd. Pomenilo bi tudi, da morajo upravljavci hraniti evidenco, da lahko organom na zahtevo dokažejo skladnost. V nekaterih primerih bi moralo biti obvezno tudi dokazovanje skladnosti širši javnosti. To se lahko doseže na primer tako, da se od upravljavcev zahteva, da vključijo varstvo podatkov v javna (letna) poročila, kadar so taka poročila obvezna na podlagi drugih razlogov.

104. Seveda morajo biti vrste notranjih in zunanjih ukrepov, ki naj bi se izvedli, ustrezne in odvisne od dejstev in okoliščin posameznega primera. Razlika je, če upravljavec obdeluje nekaj sto evidenc o strankah, ki vsebujejo le imena in naslove, ali pa evidence o milijonih bolnikov, vključno z njihovo zdravstveno anamnezo. Enako velja za posebne načine ocenjevanja učinkovitosti ukrepov. Obstaja potreba po nadgradljivosti sistema.

105. Splošni celoviti pravni akt za varstvo podatkov naj ne bi določil posebnih zahtev glede odgovornosti, temveč le njene ključne elemente. V Sporočilu so predvideni nekateri elementi za okrepitev odgovornosti upravljavcev podatkov, ki so zelo dobrodošli. Natančneje, ENVP še posebej podpira obvezno imenovanje pooblaščencev za varstvo podatkov in oceno učinka na zasebnost, ob upoštevanju nekaterih pragov.

106. Poleg tega ENVP priporoča, da se v skladu s členom 290 PDEU na Komisijo prenese pooblastila za dopolnjevanje osnovnih zahtev, potrebnih za izpolnitev standarda odgovornosti. Z uporabo teh pooblastil bi se povečala pravna varnost upravljavcev podatkov in dosegla usklajenost po vsej EU. Pri pripravi takih posebnih aktov se je treba posvetovati z delovno skupino iz člena 29.

107. Končno, konkretne ukrepe v zvezi z odgovornostjo, ki jih morajo uvesti upravljavci podatkov, lahko naložijo tudi organi za varstvo podatkov v okviru svojih izvršilnih pooblastil. V ta namen je treba organom za varstvo podatkov podeliti nova pooblastila, ki jim omogočajo nalaganje popravnih ukrepov ali sankcij. Primeri bi morali vključevati vzpostavitev programov notranje skladnosti, izvajanje vgrajene zasebnosti v zvezi z nekaterimi proizvodi in storitvami itd. Pravna sredstva se lahko uvedejo le, če so ustrezna, sorazmerna in učinkovita za zagotovitev skladnosti z veljavnimi in izvršljivimi pravnimi standardi.

7.3 Vgrajena zasebnost

108. Vgrajena zasebnost pomeni vključevanje varstva podatkov in zasebnosti od same zasnove novih proizvodov, storitev in postopkov, ki vključujejo obdelavo osebnih podatkov. ENVP meni, da je vgrajena zasebnost element odgovornosti. V skladu s tem bi se od upravljavcev podatkov zahtevalo tudi, da po potrebi dokažejo, da so uvedli vgrajeno zasebnost. Nedavno je bila na 32. mednarodni konferenci pooblaščencev za varstvo osebnih podatkov in zasebnost objavljena resolucija, ki je priznala, da je vgrajena zasebnost ključni element temeljnega varstva zasebnosti ([44]).

109. Direktiva 95/46/ES vsebuje nekatere določbe, ki spodbujajo vgrajeno zasebnost ([45]), vendar ne priznava izrecno take obveznosti. ENVP je zadovoljen, da je v Sporočilu potrjen pomen vgrajene zasebnosti kot orodja za zagotavljanje skladnosti s pravili o varstvu podatkov. Predlaga, da se vključi zavezujoča določba, ki določa obveznost „vgrajene zasebnosti“, ki bi lahko temeljila na besedilu uvodne izjave 46 Direktive 95/46/ES. Natančneje, določba

([44]) Resolucija o vgrajeni zasebnosti (Resolution on Privacy by Design), sprejeta na 32. mednarodni konferenci pooblaščencev za varstvo osebnih podatkov in zasebnost, Jeruzalem, 27.–29. oktober 2010.

([45]) Direktiva vsebuje določbe, ki v različnih razmerah posredno zahtevajo izvajanje vgrajene zasebnosti. Zlasti člen 17 določa, da morajo upravljavci podatkov izvajati ustrezne tehnične in organizacijske ukrepe za preprečitev nezakonite obdelave podatkov. Direktiva o e-zasebnosti je jasnejša. Člen 14.3 določa, da „kadar je potrebno, se lahko sprejmejo ukrepi, ki zagotovijo, da je terminalska oprema zgrajena na način, ki je združljiv s pravico uporabnikov do varstva in nadzora uporabe njihovih osebnih podatkov, v skladu z Direktivo 1999/5/ES in Sklepom Sveta 87/95/EGS z dne 22. decembra 1986 o standardizaciji na področju informacijske tehnike/tehnologije in komunikacij“.

bi vsebovala izrecno zahtevo, da morajo upravljavci podatkov izvesti tehnične in organizacijske ukrepe, in sicer med načrtovanjem sistema obdelave in med samo obdelave, zlasti da se zagotovi varstvo osebnih podatkov in prepreči nedovoljena obdelava ([46]).

110. Na podlagi take določbe bi morali upravljavci podatkov – med drugim – zagotoviti, da so sistemi obdelave podatkov načrtovani tako, da se obdeluje čim manj osebnih podatkov, da se na primer v socialnih omrežjih uvedejo nastavitve vgrajene zasebnosti, da je varovanje zasebnosti profilov posameznikov privzeto in da se uvedejo orodja, ki uporabnikom omogočajo boljše varovanje svojih osebnih podatkov (na primer nadzor dostopa, šifriranje).

111. Prednosti bolj izrecne navedbe vgrajene zasebnosti lahko povzamemo, kakor sledi:

— poudarjen bi bil pomen samega načela kot orodja za zagotavljanje, da se postopki, proizvodi in storitve od samega začetka načrtujejo ob upoštevanju zasebnosti,

— zmanjšala bi se zloraba zasebnosti in kar najbolj bi se zmanjšalo nepotrebno zbiranje podatkov, posameznikom pa bi omogočili, da se resnično sami odločajo glede svojih osebnih podatkov,

— izognili bi se poznejši uporabi „obližev“ za reševanje težav, ki jih je težko ali celo nemogoče popraviti,

— organom za varstvo podatkov bi se omogočila učinkovita uporaba in izvrševanje tega načela.

112. Posledica združenega učinka te obveznosti bi bilo večje povpraševanje po proizvodih in storitvah z vgrajeno zasebnostjo, kar bi bolj spodbudilo industrijo, da se prilagodi takemu povpraševanju. Poleg tega bi bilo treba razmisliti o oblikovanju posebne obveznosti za oblikovalce in proizvajalce novih proizvodov in storitev, ki bi lahko vplivali na varstvo podatkov in zasebnost. ENVP predlaga vključitev take posebne obveznosti, ki bi lahko upravljavcem podatkov dodatno olajšala uskladitev s svojimi obveznostmi.

113. Uzakonitev vgrajene zasebnosti bi lahko dopolnili z določbo, ki določa splošne zahteve vgrajene zasebnosti, ki veljajo za vse sektorje, proizvode in storitve, kot na primer zagotavljanje ukrepov opolnomočenja uporabnikov, ki bi se sprejeli v skladu z načelom.

114. Poleg tega ENVP priporoča, da se v skladu s členom 290 PDEU na Komisijo po potrebi prenese pooblastila za dopolnjevanje osnovnih zahtev vgrajene zasebnosti za izbrane proizvode in storitve. Z uporabo teh pooblastil bi se povečala pravna varnost upravljavcev podatkov in dosegla usklajenost po vsej EU. Pri pripravi takih posebnih aktov se je treba posvetovati z delovno skupino iz člena 29 in ENVP (glej tudi točko 106 o odgovornosti).

115. Končno, organom za varstvo podatkov je treba podeliti pooblastilo, ki jim omogoča nalaganje popravnih ukrepov ali sankcij pod podobnimi omejevalnimi pogoji, kot se navedeni v točki 107, kadar nadzorniki očitno niso sprejeli konkretnih ukrepov v primerih, ko bi to bilo potrebno.

7.4 *Storitve potrjevanja*

116. V Sporočilu je priznana potreba po proučitvi možnosti oblikovanja shem potrjevanja EU za proizvode in storitve, ki so v skladu s predpisi o spoštovanju zasebnosti. ENVP v celoti podpira ta cilj in predlaga vključitev določbe, ki določa njihovo oblikovanje in morebitne učinke po vsej EU in ki se lahko pozneje še razvija v dodatni zakonodaji. Ta določba bi morala dopolnjevati določbe o odgovornosti in vgrajeni zasebnosti.

117. Prostovoljne sheme potrjevanja bi omogočile preverjanje, ali je upravljavec podatkov uvedel ukrepe za uskladitev s pravnim aktom. Poleg tega je velika verjetnost, da bodo imeli upravljavci podatkov – ali celo proizvodi ali storitve –, ki jim bo dodeljena certifikacijska oznaka, konkurenčno prednost pred drugimi. Take sheme bi organom za varstvo podatkov tudi omogočile lažje izvajanje nadzora in izvrševanja.

8. **Globalizacija in pravo, ki se uporablja**

8.1 *Jasna potreba po doslednejšem varstvu*

118. Kot je že navedeno v poglavju 2, se je prenos osebnih podatkov čez meje EU eksponentno povečal kot posledica razvoja novih tehnologij, vloge multinacionalnih družb in povečanega vpliva vlad na obdelavo in izmenjavo osebnih podatkov na mednarodni ravni. To je eden glavnih razlogov, ki utemeljuje pregled sedanjega pravnega okvira. Zato je to eno od področij, na katerem ENVP poziva k ambicioznosti in učinkovitosti, saj je jasna potreba po doslednejšem varstvu, kadar se podatki obdelujejo zunaj EU.

([46]) V sedanjem okviru uvodna izjava 46 spodbuja upravljavce, da izvajajo take ukrepe, seveda pa nima zavezujočega učinka.

8.2 *Vlaganje v mednarodna pravila*

119. ENVP meni, da je treba več vlagati v razvoj mednarodnih pravil. Večja usklajenost glede ravni varstva osebnih podatkov po vsem svetu bi znatno prispevala k razjasnitvi vsebine načel, ki jih je treba upoštevati, in pogojev za prenos podatkov. S temi pravili na svetovni ravni bi se moralo doseči ravnovesje med potrebo po visokem standardu varstva podatkov, vključno z osnovnimi elementi varstva podatkov v EU, in regionalnimi posebnostmi.

120. ENVP podpira dosedanje ambiciozno delo v okviru mednarodne konference pooblaščencev za varstvo osebnih podatkov, usmerjeno v razvoj in širjenje tako imenovanih „madridskih standardov" z namenom njihovega vključevanja v zavezujoč akt in po možnosti uvedbe medvladne konference ([47]). Komisijo poziva, da sprejme potrebne pobude, da bi se omogočila uresničitev tega cilja.

121. Po mnenju ENVP je pomembno tudi zagotoviti usklajenost med to pobudo glede mednarodnih standardov, sedanjim pregledom okvira EU za varstvo podatkov in drugimi razvojnimi ukrepi, kot je trenutni pregled Smernic OECD o zasebnosti in Konvencije Sveta Evrope št. 108, ki je na voljo za podpis tretjim državam (glej tudi točko 17). ENVP meni, da mora Komisija pri tem igrati posebno vlogo ter opredeliti, kako bo spodbujala tako doslednost v pogajanjih v OECD in Svetu Evrope.

8.3 *Razjasnitev meril za pravo, ki se uporablja*

122. Ker ni lahko doseči popolne doslednosti, bodo – vsaj v bližnji prihodnosti – še vedno veljale nekatere razlike med zakonodajami v EU in še zlasti zunaj meja EU. ENVP meni, da bo treba v novem pravnem aktu razjasniti merila za določanje prava, ki se uporablja, in zagotoviti posodobljene mehanizme za tokove podatkov ter odgovornost udeležencev, vključenih v tokove podatkov.

123. Prvič, v pravnem aktu je treba zagotoviti, da se pravo EU uporablja, kadar se osebni podatki obdelujejo zunaj meja EU, vendar obstaja utemeljeni zahtevek za uporabo prava EU. Potreba po tem je na primer razvidna iz primera neevropskih storitev računalništva v oblaku, usmerjenih v prebivalce EU. V okolju, kjer se podatki fizično ne shranjujejo in obdelujejo na fiksni lokaciji, ponudniki storitev in uporabniki, ki so v različnih državah, pa vplivajo na podatke, je zelo težko ugotoviti, kdo je odgovoren za uskladitev in s katerimi načeli varstva podatkov se mora uskladiti. Zlasti organi za varstvo podatkov so zagotovili smernice za razlago in uporabo Direktive 95/46/ES v takih primerih, vendar te same po sebi ne zadostujejo za zagotovitev pravne varnosti v tem novem okolju.

124. Na ozemlju EU je delovna skupina iz člena 29 v svojem nedavnem mnenju poudarila potrebo po večji natančnosti v pravnem okviru in poenostavljenem merilu za določanje prava, ki se uporablja ([48]).

125. Po mnenju ENVP bi bila uredba najprimernejša možnost za oblikovanje pravnega akta, saj bi tako zagotovili uporabo enakih pravil v vseh državah članicah. Uredba bi zmanjšala pomen potrebe po določitvi prava, ki se uporablja. To je eden izmed razlogov, zakaj ENVP močno podpira sprejetje uredbe. Vendar pa bi lahko tudi uredba državam članicam dovolila nekaj manevrskega prostora. Če se v novem aktu ohrani precejšni manevrski prostor, bi ENVP podprl predlog delovne skupine glede prehoda iz porazdeljene uporabe različnih nacionalnih zakonodaj na centralizirano uporabo enotne zakonodaje v vseh državah članicah, kjer ima upravljavec podjetja. Poleg tega poziva k okrepljenemu sodelovanju in usklajevanju med organi za varstvo podatkov v mednarodnih zadevah in pritožbah (glej poglavje 10).

8.4 *Posodobitev mehanizmov za tokove podatkov*

126. Potrebo po doslednosti in visoko zastavljenem merilu je treba upoštevati ne le v povezavi z globalnimi načeli varstva podatkov, temveč tudi na področju mednarodnih prenosov podatkov. ENVP v celoti podpira cilj Komisije glede posodobitve veljavnih postopkov mednarodnih prenosov podatkov ter zagotovitve enotnejšega in skladnejšega pristopa v razmerju do tretjih držav in mednarodnih organizacij.

127. Mehanizem za tokove podatkov vključuje prenose v zasebnem sektorju, zlasti na podlagi pogodbenih klavzul ali zavezujočih poslovnih pravil, in prenose med javnimi organi. Zavezujoča poslovna pravila so eden od elementov, v zvezi s katerimi bi bil zaželen skladnejši in bolj posodobljen pristop. ENVP priporoča, da se v novem pravnem aktu izrecno obravnavajo pogoji za zavezujoča poslovna pravila ([49]), tako da se:

— zavezujoča poslovna pravila priznajo kot orodje, ki zagotavlja ustrezne zaščitne ukrepe,

— določijo glavni elementi/pogoji za sprejetje zavezujočih poslovnih pravil,

([47]) Kot se predlaga v Resoluciji o mednarodnih standardih (Resolution on International Standards), sprejeti na 32. mednarodni konferenci pooblaščencev za varstvo osebnih podatkov in zasebnost, Jeruzalem, 27.–29. oktober 2010.

([48]) Mnenje 8/2010 delovne skupine iz člena 29 o pravu, ki se uporablja, WP 179.

([49]) O mednarodnih prenosih glej tudi poglavje 8 tega mnenja.

— določijo postopki sodelovanja za sprejetje zavezujočih poslovnih pravil, vključno z merili za izbiro vodilnega nadzornega organa (vse na enem mestu).

9. **Policijsko in pravosodno področje**

9.1 *Splošni okvir*

128. Komisija je večkrat poudarila pomen krepitve varstva podatkov na področju kazenskega pregona in preprečevanja kaznivih dejanj, na katerem sta se znatno povečali izmenjava in uporaba osebnih informacij. Tudi stockholmski program, ki ga je odobril Evropski svet, se sklicuje na trden sistem za varstvo podatkov kot glavni pogoj za strategijo EU za upravljanje informacij na tem področju ([50]).

129. Pregled splošnega okvira za varstvo podatkov je odlična priložnost za doseganje napredka na tem področju, zlasti ker je v Sporočilu Okvirni sklep 2008/977 pravilno opisan kot neustrezen ([51]).

130. ENVP je v oddelku 3.2.5 tega mnenja pojasnil, zakaj je treba v splošni akt vključiti policijsko in pravosodno sodelovanje. Vključitev policije in pravosodja ima številne dodatne prednosti. Pomenila bo, da se pravila ne bodo več uporabljala le za čezmejno izmenjavo podatkov ([52]), temveč tudi za domače postopke obdelave. Bolje bo zagotovljeno ustrezno varstvo pri izmenjavi osebnih podatkov s tretjimi državami, tudi kar zadeva mednarodne sporazume. Poleg tega bodo imeli organi za varstvo podatkov enaka obširna in usklajena pooblastila v razmerju do policijskih in pravosodnih organov, kot jih imajo v razmerju do drugih upravljavcev podatkov. Končno, sedanji člen 13, ki določa pristojnost držav članic za sprejemanje posebnih predpisov za omejitev obsega obveznosti in pravic iz splošnega akta na podlagi posebnih javnih interesov, bo treba uporabljati enako omejevalno, kot se uporablja na drugih področjih. Zlasti bo treba posebne zaščitne ukrepe, ki so za to področje določeni v splošnem aktu, upoštevati tudi v nacionalni zakonodaji, sprejeti na področju policijskega in pravosodnega sodelovanja.

9.2 *Dodatna posebna pravila za policijo in pravosodje*

131. Vendar pa iz take vključitve niso izključena posebna pravila in odstopanja, v katerih se ustrezno upoštevajo posebnosti tega sektorja, v skladu z izjavo št. 21, priloženo k Lizbonski pogodbi. Lahko se predvidijo omejitve pravic posameznikov, na katere se nanašajo podatki, vendar morajo biti te nujne in sorazmerne ter ne smejo spreminjati ključnih elementov same pravice. V zvezi s tem je treba poudariti, da se Direktiva 95/46/ES, vključno s členom 13, trenutno uporablja na različnih področjih kazenskega pregona (na primer obdavčenje, carina, boj proti goljufijam), ki se ne razlikujejo pomembno od številnih dejavnosti na policijskem in pravosodnem področju.

132. Poleg tega je treba uvesti še posebne zaščitne ukrepe, da se posamezniku, na katerega se nanašajo podatki, zagotovi dodatno varstvo na področju, na katerem je lahko obdelava osebnih podatkov bolj moteča.

133. Glede na zgoraj navedeno ENVP meni, da mora novi okvir v skladu s Konvencijo št. 108 in Priporočilom št. R (87) 15 zajemati vsaj naslednje elemente:

— razlikovanje med različnimi kategorijami podatkov in dokumentov glede na njihovo točnost in zanesljivost, ob upoštevanju načela, da je treba podatke, ki temeljijo na dejstvih, ločiti od podatkov, ki temeljijo na mnenjih ali osebni presoji,

— razlikovanje med različnimi kategorijami posameznikov, na katere se nanašajo podatki (osumljenci kaznivih dejanj, žrtve, priče itd.), in dokumenti (začasni, stalni in obveščevalni dokumenti). Predvideti je treba posebne pogoje in zaščitne ukrepe za obdelavo podatkov oseb, ki niso osumljene,

— mehanizme za zagotavljanje rednega preverjanja in popravkov, da se zavaruje kakovost podatkov, ki se obdelujejo,

— posebne določbe in/ali zaščitni ukrepi, ki se lahko oblikujejo v zvezi z (čedalje bolj pomembno) obdelavo biometričnih in genetskih podatkov na področju kazenskega pregona. Njihova uporaba mora biti omejena samo na primere, ko niso na voljo manj moteča sredstva, ki lahko zagotovijo enak učinek ([53]),

— pogoje za prenos osebnih podatkov nepristojnim organom in fizičnim osebam ter za dostop in nadaljnjo uporabo osebnih podatkov, ki jih zberejo fizične osebe, s strani organov kazenskega pregona.

([50]) V zvezi s tem glej Mnenje ENVP z dne 30. septembra 2010 o sporočilu Komisije Evropskemu parlamentu in Svetu z naslovom „Pregled upravljanja informacij na območju svobode, varnosti in pravice“, odst. 9–19.

([51]) Glej oddelek 3.2.5 zgoraj.

([52]) To je trenutno omejeno področje uporabe Okvirnega sklepa 2008/977.

([53]) V zvezi s tem glej dokument WP o prihodnosti zasebnosti, točka 112.

9.3 *Ureditve na področju varstva podatkov za posamezne sektorje*

134. V Sporočilu je navedeno, da „Okvirni sklep ne nadomešča različnih zakonodajnih aktov za posamezne sektorje na področju policijskega in pravosodnega sodelovanja v kazenskih zadevah, ki so bili sprejeti na ravni EU, zlasti tistih, ki urejajo delovanje Europola, Eurojusta, schengenskega informacijskega sistema (SIS) in carinskega informacijskega sistema (CIS), in vsebujejo posebne ureditve varstva podatkov in/ali se po navadi sklicujejo na akte Sveta Evrope o varstvu podatkov".

135. S tega vidika bi moral biti novi pravni okvir po mnenju ENVP čim bolj jasen, preprost in dosleden. Kadar veljajo različne ureditve, ki se uporabljajo na primer za Europol, Eurojust, SIS in Prümsko pogodbo, skladnost s pravili ostaja ali postane celo še bolj zapletena. To je eden od razlogov, zakaj ENVP podpira celovit pravni akt za vse sektorje.

136. Vendar pa ENVP razume, da bo usklajevanje pravil iz različnih sistemov zahtevalo veliko dela, ki ga bo treba natančno opraviti. ENVP meni, da je postopen pristop, kot je naveden v Sporočilu, smiseln, če je še vedno jasna in vidna zavezanost k zagotavljanju visoke ravni doslednega in učinkovitega varstva podatkov. Konkretneje:

— na prvi stopnji je treba zagotoviti, da se splošni pravni akt za varstvo podatkov uporablja za vso obdelavo podatkov na področju policijskega in pravosodnega sodelovanja, vključno s prilagoditvami za policijo in pravosodje (kot je navedeno v 9.2),

— na drugi stopnji je treba ureditve na področju varstva podatkov za posamezne sektorje uskladiti s tem splošnim aktom. Komisija se mora zavezati, da bo v kratkem in točno določenem časovnem okviru sprejela predloge za to drugo stopnjo.

10. **Organi za varstvo podatkov in sodelovanje med njimi**

10.1 *Okrepitev vloge organov za varstvo podatkov*

137. ENVP v celoti podpira cilj Komisije glede proučitve vprašanja statusa organov za varstvo podatkov ter zlasti glede okrepitve njihove neodvisnosti, sredstev in izvršilnih pooblastil.

138. ENVP vztraja tudi, da je treba v novem pravnem aktu pojasniti temeljni pojem neodvisnosti organov za varstvo podatkov. Sodišče Evropske unije je nedavno sprejelo odločitev o tem vprašanju v zadevi C-518/07 ([54]), v kateri je poudarilo, da neodvisnost pomeni, da ne sme biti nikakršnega zunanjega vpliva. Organ za varstvo podatkov ne sme pri nikomer iskati in od nikogar prevzemati navodil. ENVP predlaga, da se ti elementi neodvisnosti izrecno uzakonijo.

139. Da bi lahko organi za varstvo podatkov opravljali svoje naloge, jim je treba zagotoviti zadostne človeške vire in finančna sredstva. ENVP predlaga, da se ta zahteva vključi v zakonodajo ([55]). Poudarja še potrebo po zagotovitvi, da so pooblastila organov v celoti usklajena glede preiskav in nalaganja ustreznih odvračalnih in popravnih ukrepov ter sankcij. To bi povečalo pravno varnost za posameznike, na katere se nanašajo podatki, in za upravljavce podatkov.

140. Okrepitev neodvisnosti, sredstev in pooblastil organov za varstvo podatkov bi morala potekati skupaj z okrepljenim sodelovanjem na večstranski ravni, zlasti glede na čedalje več vprašanj v zvezi z varstvom podatkov na evropski ravni. Seveda pa je glavna infrastruktura, ki se mora uporabiti za to sodelovanje, delovna skupina iz člena 29.

10.2 *Okrepitev vloge delovne skupine*

141. Zgodovina kaže, da se je delovanje skupine od njenega začetka leta 1997 do danes razvijalo. Postala je bolj neodvisna, tako da je v praksi ni več mogoče opredeliti le kot preprosto svetovalno delovno skupino Komisije. ENVP predlaga nadaljnje izboljšave v delovanju delovne skupine, vključno z njeno infrastrukturo in neodvisnostjo.

142. ENVP meni, da je moč skupine neločljivo povezana z neodvisnostjo in pooblastili njenih članov. Samostojnost delovne skupine je treba zagotoviti v novem pravnem okviru v skladu z merili, ki jih je Sodišče oblikovalo v zadevi C-518/07 v zvezi s popolno neodvisnostjo organov za varstvo podatkov. ENVP meni, da mora imeti delovna skupina na voljo tudi zadostna sredstva in proračun ter okrepljen sekretariat, ki podpira njene prispevke.

143. Kar zadeva sekretariat delovne skupine, ENVP pozdravlja dejstvo, da je ta vključen v oddelek za varstvo podatkov GD za pravosodje, saj je prednost v tem, da ima lahko delovna skupina koristi od učinkovitih in prilagodljivih stikov ter najnovejših informacij o razvoju na področju varstva podatkov. Po drugi strani pa se mu zdi vprašljivo, da ima Komisija (in natančneje oddelek) hkrati vlogo člana, sekretariata in naslovnika mnenj delovne skupine. To upravičuje večjo neodvisnost sekretariata. ENVP poziva Komisijo, da v tesnem posvetovanju z zainteresiranimi stranmi oceni, kako bi se lahko najbolje zagotovila taka neodvisnost.

([54]) Zadeva C-518/07, *Komisija proti Nemčiji*, še neobjavljena v ZOdl.

([55]) Glej na primer člen 43(2) Uredbe (ES) št. 45/2001, ki vsebuje tako zahtevo za ENVP.

144. Končno, za okrepitev pooblastil organov za varstvo podatkov so potrebna tudi večja pooblastila delovne skupine, pri čemer mora struktura vključevati boljša pravila in zaščitne ukrepe ter večjo preglednost. Ta bodo oblikovana za svetovalno vlogo in za izvršilno vlogo delovne skupine.

10.3 *Svetovalna vloga delovne skupine*

145. Stališča delovne skupine je treba učinkovito izvajati z vidika njene svetovalne vloge Komisiji, zlasti kar zadeva razlago in uporabo načel Direktive in drugih aktov o varstvu podatkov, ali z drugimi besedami, zagotoviti je treba avtoritativnost stališč delovne skupine. Potrebna je nadaljnja razprava med organi za varstvo podatkov, da se opredeli, kako to vključiti v pravni akt.

146. ENVP priporoča rešitve, ki bi zagotovile večjo avtoritativnost mnenj delovne skupine, ne da bi se znatno spremenil način njenega delovanja. Predlaga vključitev obveznosti, ki od organov za varstvo podatkov in Komisije zahteva, da dosledno upoštevajo mnenja in skupna stališča, ki jih sprejme delovna skupina, v skladu z modelom, sprejetim za stališča Organa evropskih regulatorjev za elektronske komunikacije (BEREC) ([56]). Poleg tega bi lahko v novem pravnem aktu za delovno skupino določili izrecno nalogo sprejemanja „pojasnjevalnih priporočil". Te alternativne rešitve bi zagotovile močnejšo vlogo stališč delovne skupine, tudi pred sodišči.

10.4 *Usklajeno izvrševanje, ki ga izvaja delovna skupina*

147. V skladu s sedanjim okvirom je izvrševanje zakonodaje o varstvu podatkov v državah članicah prepuščeno 27 organom za varstvo podatkov, pri čemer je zelo malo usklajevanja glede obravnave posebnih primerov. V primerih, ki vključujejo več kot eno državo članico ali imajo jasno svetovno razsežnost, to pomeni večje stroške za podjetja, ki se morajo za isto dejavnost ukvarjati z različnimi javnimi organi, kar povečuje tveganje za nedosledno uporabo: v izjemnih primerih lahko namreč en organ za varstvo podatkov iste postopke obdelave šteje za zakonite, drugi organ za varstvo podatkov pa za prepovedane.

148. V nekaterih primerih gre za strateško razsežnost, ki jo je treba obravnavati centralizirano. Delovna skupina iz člena 29 podpira ukrepe usklajevanja in izvrševanja med organi za varstvo podatkov ([57]) v zvezi s pomembnimi vprašanji varstva podatkov s takimi mednarodnimi posledicami. Tak primer so bila socialna omrežja in spletni iskalniki ([58]) ter usklajeni pregledi, ki se izvajajo v različnih državah članicah na področju telekomunikacij in zdravstvenega zavarovanja.

149. Vendar pa so izvršilni ukrepi, ki jih delovna skupina lahko izvaja v skladu s sedanjim okvirom, omejeni. Delovna skupina lahko sprejme skupna stališča, ni pa instrumenta, ki bi zagotovil, da se ta stališča v praksi učinkovito izvedejo.

150. ENVP predlaga, da se v pravni akt vključijo dodatne določbe, ki bi podprle usklajeno izvrševanje, in zlasti

— obveznost, ki od organov za varstvo podatkov in Komisije zahteva, da *dosledno upoštevajo mnenja in skupna stališča*, ki jih sprejme delovna skupina iz člena 29 ([59]),

— obveznost, ki od organov za varstvo podatkov zahteva, da tesno sodelujejo med seboj ter s Komisijo in delovno skupino iz člena 29 ([60]). Praktičen primer tesnega sodelovanja bi lahko bila vzpostavitev postopka, po katerem bi organi za varstvo podatkov obveščali Komisijo ali delovno skupino v primeru nacionalnih izvršilnih ukrepov s čezmejno razsežnostjo, analogno s postopkom, ki se uporablja v skladu s sedanjim okvirom v zvezi z nacionalnimi odločitvami o ustreznosti,

— določitev pravil glasovanja, da bi se povečala zavezanost organov za varstvo podatkov k izvajanju odločitev delovne skupine. Lahko bi določili, da je za delovno skupino predvideno soglasno odločanje, če pa ne more doseči soglasja, odloča le s kvalificirano

([56]) Uredba (ES) št. 1211/2009 Evropskega parlamenta in Sveta z dne 25. novembra 2009 o ustanovitvi Organa evropskih regulatorjev za elektronske komunikacije (BEREC) in Urada, (UL L 337, 18.12.2009, str. 1).

([57]) Evropska konferenca pooblaščencev za varstvo osebnih podatkov je poleg delovne skupine iz člena 29 pred približno desetimi leti ustanovila stalno delavnico, katere namen je usklajeno obravnavati čezmejne pritožbe. Čeprav ta delavnica nesporno prinaša dodano vrednost v smislu izmenjave med osebjem organov za varstvo podatkov in zagotavlja zanesljivo mrežo kontaktnih točk, se ne more šteti za mehanizem usklajevanja pri odločanju.

([58]) Glej dopisa delovne skupine iz člena 29 z dne 12. maja 2010 in 26. maja 2010, objavljena na spletni strani delovne skupine iz člena 29 (http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010-others_en.htm).

([59]) Kot je navedeno zgoraj, je podobna obveznost določena v Uredbi (ES) št. 1211/2009, ki določa vlogo Organa evropskih regulatorjev za elektronske komunikacije (BEREC).

([60]) V zvezi s tem glej člen 3 zgoraj navedene Uredbe (ES) št. 1211/2009.

večino. Poleg tega bi lahko v uvodni izjavi predvideli, da za organe za varstvo podatkov, ki glasujejo za neki dokument, velja obveznost ali zaveza politike, da ga izvedejo na nacionalni ravni.

151. ENVP opozarja na nevarnosti uvedbe strožjih ukrepov, kot je zavezujoč učinek stališč delovne skupine iz člena 29. To bi ogrozilo neodvisen status posameznih organov za varstvo podatkov, ki ga morajo države članice zagotoviti v skladu z nacionalno zakonodajo. Če bodo imele odločitve delovne skupine neposreden učinek na tretje strani, kot so upravljavci podatkov, je treba predvideti nove postopke, vključno z zaščitnimi ukrepi, kot sta preglednost in pravno varstvo z možnostjo pritožbe pred Sodiščem Evropske unije.

10.5 *Sodelovanje med ENVP in delovno skupino*

152. Natančno bi lahko določili tudi način sodelovanja med ENVP in delovno skupino. ENVP je član delovne skupine in v njenem okviru prispeva k stališčem o glavnih strateških razvojih dogodkov v EU, pri tem pa zagotavlja skladnost s svojimi stališči. ENVP ugotavlja, da se povečuje število vprašanj v zvezi z zasebnostjo, in sicer v zasebnem in javnem sektorju, kar ima v številnih državah članicah posledice na nacionalni ravni, pri tem pa ima posebno vlogo delovna skupina.

153. Dopolnilna naloga ENVP je svetovanje o razvoju dogodkov v EU in to nalogo je treba ohraniti. ENVP kot evropski organ izvaja to svetovalno nalogo institucijam EU enako, kot organi za varstvo podatkov svetujejo svojim vladam.

154. ENVP in delovna skupina delujeta z različnih vidikov, vendar se pri tem dopolnjujeta. Zaradi teh razlogov obstaja potreba po ohranitvi in morda celo izboljšanju usklajevanja med delovno skupino in ENVP, da bi zagotovili, da skupaj delujeta na področju glavnih vprašanj varstva podatkov, na primer z rednim usklajevanjem obravnavanih tem ([61]) in zagotavljanjem preglednosti v zvezi z vprašanji, ki imajo bolj nacionalno ali posebno EU-razsežnost.

155. Usklajevanje v veljavni Direktivi ni omenjeno iz preprostega razloga, ker ENVP v času sprejetja Direktive ni obstajal, vendar so po šestih letih obstoja vidni dopolnjujoči se elementi med ENVP in delovno skupino, ki bi jih lahko formalno priznali. ENVP poudarja, da je v skladu z Uredbo (ES) št. 45/2001 njegova dolžnost sodelovati z nacionalnimi organi za varstvo podatkov in se vključiti v dejavnosti delovne skupine. ENVP priporoča, da se sodelovanje izrecno navede v novem pravnem aktu in da se ga po potrebi strukturira, na primer z določitvijo postopka za sodelovanje.

10.6 *Sodelovanje med ENVP in organi za varstvo podatkov pri nadzoru sistemov EU*

156. Ti vidiki veljajo tudi za področja, na katerih mora biti nadzor usklajen med evropsko in nacionalno ravnjo. To velja za organe EU, ki obdelujejo znatne količine podatkov, ki jih zagotavljajo nacionalni organi, ali za velike informacijske sisteme z evropsko in nacionalno razsežnostjo.

157. Sedanji sistem nekaterih organov EU in velikih informacijskih sistemov – na primer Europol, Eurojust in schengenski informacijski sistem prve generacije (SIS) imajo skupne nadzorne organe, v katerih so predstavniki nacionalnih organov za varstvo podatkov – je ostanek medvladnega sodelovanja v času pred sprejetjem Lizbonske pogodbe in ni skladen z institucionalno strukturo EU, katere sestavni del sta zdaj Europol in Eurojust in v katero je zdaj vključen tudi „schengenski pravni red“ ([62]).

158. V Sporočilu je navedeno, da bo Komisija leta 2011 začela posvetovanje z zainteresiranimi stranmi o spremembi veljavnih nadzornih sistemov. ENVP poziva Komisijo, da čim prej (v kratkem in točno določenem časovnem okviru, glej zgoraj) sprejme stališče glede razprave, ki poteka o nadzoru. V tej razpravi bo ENVP sprejel naslednje stališče.

159. Kot izhodiščno točko je treba zagotoviti, da vsi nadzorni organi izpolnjujejo nujna merila glede neodvisnosti, sredstev in izvršilnih pooblastil. Nato je treba zagotoviti, da se upoštevajo vidiki ter strokovno znanje in izkušnje na ravni EU. To pomeni, da mora potekati sodelovanje ne le med nacionalnimi organi, temveč tudi z evropskim organom za varstvo podatkov (trenutno je to ENVP). ENVP meni, da je treba uporabiti model, ki izpolnjuje te zahteve ([63]).

160. V zadnjih letih se je razvil model „usklajenega nadzora“. Ta model nadzora, ki zdaj deluje v sistemu Eurodac in delih Carinskega informacijskega sistema, bo kmalu razširjen na Vizumski informacijski sistem (VIS) in schengenski informacijski sistem druge generacije (SIS II). Ta model ima tri plasti: (1) nadzor na nacionalni ravni zagotavljajo organi za varstvo podatkov; (2) nadzor na ravni EU zagotavlja ENVP; (3) usklajevanje se zagotavlja z

([61]) Na primer na podlagi letno objavljenega seznama zakonodajnih dejavnosti, ki se redno posodablja in je na voljo na spletni strani ENVP.

([62]) V skladu z Uredbo (ES) št. 45/2001 je dolžnost ENVP, da sodeluje s temi organi.

([63]) V modelu za Eurojust je treba upoštevati še, da se pri nadzoru varstva podatkov upošteva neodvisnost sodstva, kadar Eurojust obdeluje podatke v kazenskih postopkih.

rednimi sestanki, ki jih skliče ENVP, ki ima v tem mehanizmu usklajevanja vlogo sekretariata. Ta model se je izkazal za uspešnega in učinkovitega in ga je treba v prihodnosti predvideti za druge informacijske sisteme.

C. KAKO IZBOLJŠATI UPORABO SEDANJEGA OKVIRA?

11. Kratkoročni vidik

161. Medtem ko poteka postopek pregleda, je treba prizadevanja usmeriti v zagotavljanje polnega in učinkovitega izvajanja veljavnih pravil. Ta pravila se bodo uporabljala do sprejetja prihodnjega okvira in njegovega prenosa v nacionalne zakonodaje držav članic. V zvezi s tem se lahko opredeli več vrst ukrepov.

162. Prvič, Komisija mora še naprej spremljati skladnost držav članic z Direktivo 95/46 in, kjer je to potrebno, uporabiti svoja pooblastila iz člena 258 PDEU. Pred kratkim so bili uvedeni postopki za ugotavljanje kršitev zaradi pomanjkljivega izvajanja člena 28 Direktive v zvezi s pogojem neodvisnosti organov za varstvo podatkov ([64]). Tudi na drugih področjih je treba spremljati in izvrševati popolno skladnost ([65]). ENVP zato pozdravlja in v celoti podpira zavezo Komisije v Sporočilu, da bo izvajala dejavno politiko glede kršitev. Poleg tega bi morala Komisija nadaljevati strukturiran dialog z državami članicami v zvezi z izvajanjem ([66]).

163. Drugič, spodbujati je treba izvrševanje na nacionalni ravni, da se zagotovi praktična uporaba pravil o varstvu podatkov, tudi v zvezi z novimi tehnološkimi pojavi in svetovnimi udeleženci. Organi za varstvo podatkov bi morali v celoti izkoristiti svoja pooblastila v zvezi s preiskovanjem in sankcioniranjem. Pomembno je tudi, da se veljavne pravice posameznikov, na katere se nanašajo podatki, zlasti pravice do dostopa, v praksi v celoti izvajajo.

164. Tretjič, zdi se, da je s kratkoročnega vidika potrebno bolj usklajeno izvrševanje. Vloga delovne skupine iz člena 29 in njenih razlagalnih dokumentov v zvezi s tem je ključna, vendar si morajo tudi organi za varstvo podatkov po najboljših močeh prizadevati, da jih uresničijo v praksi. Izogibati se je treba različnim izidom v zadevah, ki se obravnavajo na ravni EU ali svetovni ravni, ob tem pa se lahko sprejmejo in tudi morajo sprejeti skupni pristopi v okviru delovne skupine. Tudi usklajene preiskave na ravni EU, ki se izvajajo pod okriljem delovne skupine, lahko zagotovijo pomembno dodano vrednost.

165. Četrtič, načela varstva podatkov morajo biti proaktivno „vgrajena“ v nove predpise, ki lahko vplivajo, neposredno ali posredno, na varstvo podatkov. ENVP si na ravni EU zelo prizadeva, da bi prispeval k boljši evropski zakonodaji, in taka prizadevanja so potrebna tudi na nacionalni ravni. Organi za varstvo podatkov morajo zato v celoti izkoristiti svoja svetovalna pooblastila, da bi zagotovili tak proaktivni pristop. Poleg ENVP imajo lahko tudi organi za varstvo podatkov proaktivno vlogo pri spremljanju tehnološkega razvoja. Spremljanje je pomembno z vidika zgodnjega ugotavljanja pojavljajočih se trendov, poudarjanja možnih posledic za varstvo podatkov, podpiranja prijaznih rešitev za varstvo podatkov in ozaveščanja zainteresiranih strani.

166. Končno, dejavno si je treba prizadevati za nadaljnje sodelovanje med različnimi udeleženci na mednarodni ravni. Zato je pomembno okrepiti mednarodne instrumente sodelovanja. Podpreti je treba pobude, kot so madridski standardi in prizadevanja, ki potekajo v okviru Sveta Evrope in OECD. V zvezi s tem je zelo spodbudno, da se je tudi ameriška zvezna komisija za trgovino pridružila skupini pooblaščencev za varstvo osebnih podatkov in zasebnost v okviru njihove mednarodne konference.

D. SKLEPNE UGOTOVITVE

SPLOŠNE UGOTOVITVE

167. ENVP na splošno pozdravlja Sporočilo Komisije, saj je prepričan, da je potreben pregled sedanjega pravnega okvira za varstvo podatkov, da se zagotovi učinkovito varstvo v čedalje bolj razvijajoči se in globalizirani informacijski družbi.

168. V Sporočilu so opredeljena glavna vprašanja in izzivi. ENVP se strinja s stališčem Komisije, da bo v prihodnosti še vedno potreben trden sistem varstva podatkov, ki bo temeljil na dejstvu, da v družbi, ki doživlja temeljite spremembe, še vedno veljajo sedanja splošna načela varstva podatkov. ENVP se strinja z izjavo v Sporočilu, da so izzivi ogromni, in poudarja, da bi morale biti predlagane rešitve ustrezno ambiciozno zastavljene in okrepiti učinkovitost varstva. Zato poziva k bolj ambiciozno zastavljenemu pristopu v zvezi s številnimi vprašanji.

169. ENVP v celoti podpira celovit pristop k varstvu podatkov. Zato obžaluje, da je Sporočilo iz splošnega pravnega akta izključilo nekatera področja, kot je obdelava podatkov

([64]) Glej zgoraj navedeno zadevo C-518/07 in sporočilo za javnost Komisije z dne 28. oktobra 2010 (IP/10/1430).

([65]) Komisija je začela postopek za ugotavljanje kršitev proti Združenemu kraljestvu v zvezi z domnevno kršitvijo različnih določb o varstvu podatkov, vključno z zahtevo po zaupnosti elektronskih komunikacij v zvezi z vedenjskim oglaševanjem. Glej sporočilo za javnost Komisije z dne 9. aprila 2009 (IP/09/570).

([66]) Glej zgoraj navedeno prvo poročilo Komisije o izvajanju direktive o varstvu podatkov, str. 22 in naslednje.

v institucijah in organih EU. Če bi se Komisija odločila izključiti ta področja, jo ENVP poziva, da v najkrajšem možnem času, po možnosti pa do konca leta 2011 sprejme predlog za raven EU.

GLAVNI VIDIKI

170. Izhodiščne točke postopka pregleda ENVP so naslednje:

— ureditve v zvezi z varstvom podatkov morajo čim bolj dejavno podpirati druge zakonite interese (kot so evropsko gospodarstvo, varnost posameznikov in odgovornost vlad), namesto da jih ovirajo,

— splošna načela varstva podatkov se ne smejo in ne morejo spremeniti,

— eden glavnih ciljev pregleda mora biti nadaljnje usklajevanje,

— vidik temeljnih pravic mora biti v središču pozornosti postopka pregleda. Cilj temeljne pravice je zaščititi državljane v vseh okoliščinah,

— novi pravni akt mora vključevati policijski in pravosodni sektor,

— novi pravni akt mora biti oblikovan čim bolj tehnološko nevtralno, njegov cilj pa mora biti zagotoviti dolgoročno pravno varnost.

ELEMENTI NOVEGA OKVIRA

Uskladitev in poenostavitev

171. ENVP pozdravlja zavezo Komisije, da bo proučila sredstva za nadaljnje usklajevanje predpisov o varstvu podatkov na ravni EU. ENVP opredeljuje področja, na katerih je potrebna nadaljnja in boljša uskladitev: opredelitve pojmov, razlogi za obdelavo podatkov, pravice posameznikov, na katere se nanašajo podatki, mednarodni prenosi in organi za varstvo podatkov.

172. ENVP predlaga, da se proučijo naslednje možnosti za poenostavitev in/ali zmanjšanje področja uporabe zahtev glede obveščanja:

— omejitev obveznosti obveščanja na posebne vrste postopkov obdelave, ki pomenijo posebne nevarnosti,

— obveznost preproste prijave, v skladu s katero se morajo upravljavci prijaviti (v nasprotju z obsežno prijavo vseh postopkov obdelave podatkov),

— uvedba enotnega vseevropskega obrazca za obveščanje.

173. Po mnenju ENVP je uredba kot enotni akt, ki se neposredno uporablja v državah članicah, najučinkovitejši način zaščite temeljne pravice do varstva podatkov in nadaljnjega zbliževanja na notranjem trgu.

Krepitev pravic posameznikov

174. ENVP podpira Sporočilo glede krepitve pravic posameznikov. Predlaga naslednje:

— v zakonodajo bi lahko vključili načelo preglednosti. Vendar je še pomembnejše okrepiti sedanje določbe, ki obravnavajo preglednost (kot sta sedanja člena 10 in 11 Direktive 95/46/ES),

— v splošni akt je treba uvesti določbo o obveščanju o kršitvah varstva osebnih podatkov, ki razširja obveznost, ki je v spremenjeni direktivi o e-zasebnosti veljala le za nekatere ponudnike, na vse upravljavce podatkov,

— pojasniti je treba omejitve glede privolitve. Razmisliti je treba o razširitvi primerov, v katerih je potrebna izrecna privolitev, in sprejeti dodatna pravila za privolitev v spletnem okolju,

— uvesti je treba dodatne pravice, kot sta prenosljivost podatkov in pravica biti pozabljen, zlasti za storitve informacijske družbe na svetovnem spletu,

— interese otrok je treba bolje zaščititi z vrsto dodatnih določb, ki so posebej namenjene zbiranju in nadaljnji obdelavi podatkov o otrocih,

— v zakonodajo EU je treba uvesti mehanizme skupinskih tožb za kršenje pravil o varstvu podatkov, da se pooblaščene subjekte pooblasti za vlaganje tožb v imenu skupin posameznikov.

Okrepitev obveznosti organizacij/upravljavcev

175. Novi okvir mora vsebovati spodbude za upravljavce podatkov, da bi ti v svoje poslovne postopke proaktivno uvajali ukrepe za varstvo podatkov. ENVP predlaga uvedbo splošnih določb o odgovornosti in „vgrajeni zasebnosti“. Uvesti je treba tudi določbo o shemah potrjevanja zaupnosti.

Globalizacija in pravo, ki se uporablja

176. ENVP podpira ambiciozna prizadevanja v okviru mednarodne konference pooblaščencev za varstvo osebnih podatkov, usmerjena v razvoj tako imenovanih „madridskih standardov“ z namenom njihovega vključevanja v zavezujoč akt in po možnosti uvedbe medvladne konference. ENVP poziva Komisijo, da v zvezi s tem sprejme konkretne ukrepe v tesnem sodelovanju z OECD in Svetom Evrope.

177. Novi pravni akt mora pojasniti merila za določanje prava, ki se uporablja. Zagotoviti je treba, da se podatki, ki se obdelujejo zunaj meja EU, ne izognejo pravni pristojnosti EU, če obstaja utemeljen zahtevek za uporabo prava EU. Če bi bil pravni okvir uredba, bi se v vseh državah članicah uporabljala enaka pravila, določanje prava, ki se uporablja (v EU), pa bi imelo manjši pomen.

178. ENVP v celoti podpira cilj zagotovitve enotnejšega in skladnejšega pristopa v razmerju do tretjih držav in mednarodnih organizacij. V pravni akt je treba vključiti zavezujoča poslovna pravila.

Policija in pravosodje

179. Celovit akt, v katerega sta vključena policija in pravosodje, lahko ponudi posebna pravila, v katerih se ustrezno upoštevajo posebnosti tega sektorja, v skladu z izjavo št. 21, ki je priložena k Lizbonski pogodbi. Uvesti je treba posebne zaščitne ukrepe, da se posameznikom, na katere se nanašajo podatki, zagotovi dodatno varstvo na področju, na katerem je obdelava osebnih podatkov po naravi bolj moteča.

180. Novi pravni okvir bi moral biti čim bolj jasen, preprost in dosleden. Izogibati se je treba različnim ureditvam, ki se uporabljajo na primer za Europol, Eurojust, SIS in Prümsko pogodbo. ENVP razume, da bo treba usklajevanje pravil iz različnih sistemov opraviti natančno in postopno.

Organi za varstvo podatkov in sodelovanje med njimi

181. ENVP v celoti podpira cilj Komisije glede proučitve vprašanja statusa organov za varstvo podatkov ter glede okrepitve njihove neodvisnosti, sredstev in izvršilnih pooblastil. Priporoča naslednje:

— v novem pravnem aktu je treba uzakoniti osnovni pojem neodvisnosti organov za varstvo podatkov, kot ga je opredelilo Sodišče Evropske unije,

— v zakonodaji je treba navesti, da se organom za varstvo podatkov zagotovijo zadostna sredstva,

— organom je treba zagotoviti usklajena pooblastila v zvezi s preiskovanjem in sankcioniranjem.

182. ENVP predlaga nadaljnje izboljšave v delovanju delovne skupine iz člena 29, vključno z njeno neodvisnostjo in infrastrukturo. Delovni skupini je treba zagotoviti tudi zadostna sredstva in okrepljen sekretariat.

183. ENVP predlaga, da se okrepi svetovalna vloga delovne skupine z uvedbo obveznosti, ki od organov za varstvo podatkov in Komisije zahteva, da *dosledno upoštevajo mnenja in skupna stališča*, ki jih sprejme delovna skupina. ENVP ne podpira uvedbe zavezujočega učinka stališč delovne skupine, zlasti zaradi neodvisnega statusa posameznih organov za varstvo podatkov. Priporoča, da Komisija v novi pravni akt uvede posebne določbe za okrepitev sodelovanja z ENVP.

184. ENVP poziva Komisijo, da čim prej sprejme stališče glede vprašanja nadzora organov EU in velikih informacijskih sistemov, pri čemer je treba upoštevati, da morajo vsi nadzorni organi izpolnjevati nujna merila glede neodvisnosti, zadostnih sredstev in izvršilnih pooblastil, ter zagotoviti, da se ustrezno upoštevajo vidiki na ravni EU. ENVP podpira model „usklajenega nadzora“.

Izboljšave v sedanjem sistemu:

185. ENVP poziva Komisijo, da:

— še naprej spremlja skladnost držav članic z Direktivo 95/46/ES in, kjer je to potrebno, uporabi svoja pooblastila iz člena 258 PDEU,

— spodbuja izvrševanje na nacionalni ravni in usklajevanje izvrševanja,

— zagotovi, da so načela varstva podatkov proaktivno vključena v nove predpise, ki lahko vplivajo, neposredno ali posredno, na varstvo podatkov,

— si dejavno prizadeva za nadaljnje sodelovanje med različnimi udeleženci na mednarodni ravni.

V Bruslju, 14. januarja 2011

Peter HUSTINX

Evropski nadzornik za varstvo podatkov