ISSN 1725-5244

Uradni list Evropske unije

C 128

Slovenska izdaja

Informacije in objave

Zvezek 52

6. junij 2009

Obvestilo št. | Vsebina | Stran

SL

(Nadaljevanje na naslednji strani)

SL

I

(Resolucije, priporočila in mnenja)

MNENJA

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV

Mnenje Evropskega nadzornika za varstvo podatkov o končnem poročilu Kontaktne skupine na visoki ravni EU-ZDA za izmenjavo informacij ter varstvo zasebnosti in osebnih podatkov

(2009/C 128/01)

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV JE –

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

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

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

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 ter zlasti člena 41 te uredbe –

SPREJEL NASLEDNJE MNENJE:

I. UVOD – OZADJE ZA PRIPRAVO TEGA MNENJA

1. Predsedstvo Sveta Evropske unije je 28. maja 2008 obvestilo Coreper, da je Kontaktna skupina na visoki ravni EU-ZDA (*EU-US High Level Contact Group*; v nadaljnjem besedilu: HLCG) za izmenjavo informacij ter varstvo zasebnosti in osebnih podatkov pripravila končno poročilo za vrh EU 12. junija 2008, ki je bilo objavljeno 26. junija 2008 ([1]).

2. V njem so opredeljena skupna načela varstva zasebnosti in osebnih podatkov, ki predstavljajo prvi korak k izmenjavi informacij z Združenimi državami v okviru preprečevanja terorizma in hudih mednarodnih kaznivih dejanj.

3. Predsedstvo Sveta v svojem obvestilu sporoča, da so dobrodošle vse zamisli glede nadaljnjega ukrepanja na podlagi navedenega poročila, zlasti pa odzivi na priporočila iz predloga, ki se nanašajo na nadaljnje ravnanje. ENVP na ta poziv odgovarja z izdajo tega mnenja, ki temelji na trenutnem stanju, kolikor je to znano javnosti, in ne vpliva na nobeno prihodnje stališče, ki bi ga utegnil zavzeti ob upoštevanju razvoja dogodkov v zvezi s tem vprašanjem.

4. ENVP ugotavlja, da se je okolje, v katerem je delovala HLCG, spremenilo zlasti po 11. septembru 2001: obseg izmenjave podatkov med ZDA in EU je večji in poteka v okviru mednarodnih sporazumov oziroma prek drugih instrumentov; med njimi sta sporazuma Europola in Eurojusta z Združenimi državami pa tudi sporazumi o PNR in zadeva „SWIFT“, v zvezi s katero je med uradniki EU in ZDA prišlo do izmenjave pisem zaradi uvedbe minimalnih jamstev glede varstva podatkov ([2]).

([1]) Dokument Sveta št. 9831/08, ki je (v angleškem jeziku) na voljo na spletni povezavi http://ec.europa.eu/justice_home/fsj/privacy/news/docs/report_02_07_08_en.pdf

([2]) — Sporazum med Združenimi državami Amerike in Evropskim policijskim uradom z dne 6. decembra 2001 ter Dodatni sporazum med Europolom in ZDA o izmenjavi osebnih podatkov in z njimi povezanih informacij (v angleškem jeziku), objavljen na spletnih straneh Europola;
— Sporazum med Združenimi državami Amerike in Eurojustom o pravosodnem sodelovanju z dne 6. novembra 2006, objavljen na spletnih straneh Europola;
— Sporazum med Evropsko unijo in Združenimi državami Amerike o obdelavi in posredovanju podatkov iz evidence podatkov o potnikih (PNR) s strani letalskih prevoznikov ministrstvu Združenih držav za domovinsko varnost (MDV) (Sporazum PNR iz leta 2007), podpisan v Bruslju, 23. julija 2007 in v Washingtonu, 26. julija 2007, UL L 204, 4.8.2007, str. 18;
— Izmenjava pisem med pristojnimi organi ZDA in EU o programu nadzora nad financiranjem terorizma z dne 28. junija 2007.

5. EU se poleg tega pogaja in dogovarja o podobnih instrumentih za izmenjavo osebnih podatkov z drugimi tretjimi državami. Nedaven primer je Sporazum med Evropsko unijo in Avstralijo o obdelavi in posredovanju podatkov iz evidence podatkov o potnikih (PNR) Evropske unije s strani letalskih prevoznikov avstralski carinski službi ([3]).

6. Glede na navedeno je videti, da vedno več organov pregona iz tretjih držav zahteva informacije o osebnih podatkih, ne samo iz konvencionalnih vladnih zbirk podatkov, pač pa tudi iz drugih zbirk, zlasti tistih v zasebnem sektorju.

7. ENVP tudi opozarja na še en pomemben element, namreč da je vprašanje prenosa osebnih podatkov v tretje države v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah obravnavano v okvirnem sklepu Sveta o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah ([4]), ki naj bi bil verjetno sprejet pred koncem leta 2008.

8. Predvidevamo lahko, da bo ta čezatlantska izmenjava vse intenzivnejša in da se bodo informacije kmalu izmenjavale tudi med drugimi sektorji, v katerih se obdelujejo osebni podatki. Dialog o t. i. čezatlantskem kazenskem pregonu je ob upoštevanju navedenega sicer dobrodošel, hkrati pa gre za občutljivo vprašanje. Dobrodošel je zato, ker bi lahko omogočil preglednejšo izmenjavo podatkov, ki je že v teku ali se šele pripravlja. Obenem pa je to vprašanje tudi občutljivo, saj bi lahko tak okvir upravičil množične prenose podatkov na tem področju, tj. na področju kazenskega pregona, kjer imajo ti prenosi še posebej resne posledice za posameznike, in na katerem so zato še toliko bolj potrebni zanesljivi zaščitni ukrepi in jamstva ([5]).

9. V naslednjem poglavju tega mnenja sta obravnavana trenutno stanje in možnosti za nadaljnje ukrepanje. Poglavje III je osredotočeno na področje uporabe in naravo instrumenta, ki bi omogočil izmenjavo informacij. V poglavju IV tega mnenja so s splošnega vidika preučena pravna vprašanja v zvezi z vsebino morebitnega sporazuma, tj. temami, kot so pogoji za oceno ravni varstva, ki ga zagotavljajo Združene države, poglavje pa bo posvečeno tudi vprašanju uporabe regulativnega okvira EU kot merila za oceno navedene ravni zaščite. Isto poglavje vsebuje tudi seznam osnovnih zahtev, ki bi jih bilo treba vključiti v tak sporazum. V poglavju V mnenja pa je analiza načel v zvezi z zasebnostjo, ki so priložena poročilu.

([3]) UL L 213, 8.8.2008, str. 49.

([4]) Okvirni sklep Sveta o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah, različica z dne 24. junija 2008, ki je na voljo na povezavi http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=sl&DosId=193371

([5]) Več o nujni potrebi po jasnem pravnem okviru v poglavjih III in IV tega mnenja.

II. TRENUTNO STANJE IN MOREBITNO NADALJNJE UKREPANJE

10. Ocena ENVP o trenutnem stanju je naslednja: pri določanju skupnih standardov za izmenjavo informacij ter varstvo zasebnosti in osebnih podatkov je bil dosežen določen napredek.

11. Toda morebiten sporazum med EU in ZDA še ni dokončno pripravljen, potrebna bodo dodatna prizadevanja. Tudi poročilo HLCG navaja številna odprta vprašanja, od katerih je najpomembnejše tisto v zvezi s pravnim varstvom. Še vedno ni razrešeno nesoglasje glede potrebnega obsega sodnega varstva ([6]). Drugih pet odprtih vprašanj je navedenih v poglavju 3 poročila. ENVP pa meni, da je še mnogo drugih vprašanj, ki še niso razrešena, na primer vprašanje o področju uporabe in naravi instrumenta za izmenjavo informacij.

12. Glede na to, da je poročilo bolj naklonjeno zavezujočemu sporazumu – in ENVP je istega mnenja –, je še toliko bolj potrebna preudarnost. Sporazuma ne bo mogoče skleniti brez nadaljnjih skrbnih in poglobljenih priprav.

13. ENVP pa tudi meni, da bi moral biti sporazum sklenjen v okviru Lizbonske pogodbe, če bo ta seveda začela veljati, saj ne bi dopustila nobenega pravnega dvoma o tem, kje poteka ločnica med posameznimi stebri EU. Poleg tega bi bila v celoti zagotovljena sodelovanje Evropskega parlamenta in pravosodni nadzor Sodišča.

14. V teh razmerah bi bilo v prihodnje najbolje oblikovati časovni načrt za nekoliko morebitno kasnejšo sklenitev sporazuma. V časovni načrt bi lahko vključili naslednje elemente:

— navodila in časovni okvir glede nadaljevanja dela HLCG (ali katere koli druge skupine);

— v začetni fazi razprava in morebitni dogovor o temeljnih vprašanjih kot sta področje uporabe in narava sporazuma;

— podrobnejša opredelitev načel varstva podatkov na podlagi enotnega razumevanja teh temeljnih vprašanj;

— sodelovanje zainteresiranih strani v različnih fazah postopka;

— obravnava vprašanja institucionalnih ovir na evropski strani.

([6]) Stran 5, točka C poročila.

III. **PODROČJE UPORABE IN NARAVA INSTRUMENTA ZA IZMENJAVO INFORMACIJ**

15. ENVP meni, da je jasna opredelitev področja uporabe in narave morebitnega instrumenta, vključno z načeli varstva podatkov, ključnega pomena in prvi korak pri nadaljnjem razvoju takšnega instrumenta.

16. V zvezi s področjem uporabe bi bilo treba odgovoriti na naslednja pomembna vprašanja:

— kdo so akterji na področju kazenskega pregona in na drugih področjih;

— kaj natančno pomeni kazenski pregon ter njegova povezava z drugimi nameni, kot je državna varnost, ali natančneje kontrola na meji ter javno zdravje;

— na kakšen način bi lahko instrument vključili v zamisel o globalnem čezatlantskem območju varnosti.

17. Z opredelitvijo narave instrumenta bi bilo treba razjasniti naslednja vprašanja:

— v okviru katerega stebra bodo tekla pogajanja o instrumentu, če bo to potrebno;

— ali bo instrument za EU in ZDA zavezujoč,

— ali bo imel instrument neposreden učinek, glede na to, da vsebuje pravice in obveznosti za posameznike, ki jih je mogoče uveljaviti pred pravosodnim organom;

— ali bo izmenjavo informacij omogočal že sam instrument ali bo v njem določen sklop minimalnih standardov za tovrstno izmenjavo, ki naj bi jih dopolnili specifični sporazumi;

— kakšna bo povezava med navedenim instrumentom in instrumenti, ki so že v veljavi – ali jih bo moral upoštevati, nadomestiti ali dopolnjevati?

III. 1. **Področje uporabe instrumenta**

Akterji

18. Čeprav v poročilu HLCG nikjer ni jasno in natančno navedeno, kaj vse naj bi sodilo v področje uporabe bodočega instrumenta, je iz v njem navedenih načel mogoče sklepati, da naj bi predvidoma zajemalo prenose med zasebnimi in javnimi akterji ([7]) ter javnimi organi.

([7]) Glej predvsem poglavje 3 poročila, tj. o odprtih vprašanjih v zvezi s čezatlantskimi odnosi, in sicer točko 1 o doslednosti v zvezi z obveznostmi zasebnih subjektov pri prenosu podatkov.

— Prenosi med zasebnimi in javnimi akterji

19. ENVP se strinja s smiselnostjo uporabe bodočega instrumenta za prenose med zasebnimi in javnimi akterji. Oblikovanje takega instrumenta poteka na podlagi zahtev po informacijah v lasti zasebnih subjektov, ki jih je v zadnjih letih vložila ameriška stran. ENVP ugotavlja, da z vidika kazenskega pregona zasebni akterji dejansko sistematično postajajo vir informacij tako v EU kot na mednarodni ravni ([8]). Zadeva SWIFT je predstavljala pomemben precedens – organi kazenskega pregona tretje države so zahtevali, da jim zasebna družba sistematično pošilja podatke v neprečiščeni obliki ([9]). Na isti način letalske družbe zbirajo in pošiljajo podatke iz PNR. ENVP je že v mnenju o osnutku okvirnega sklepa o evropskem sistemu PNR podvomil o zakonitosti tega trenda ([10]).

20. Za previdnost pri vključevanju prenosov med zasebnimi in javnimi akterji v področje uporabe bodočega instrumenta sta še dva dodatna razloga.

21. Vključitev bi lahko imela nezaželen učinek na ozemlju EU. ENVP je resno zaskrbljen, da bi – če bi bilo mogoče podatke zasebnih podjetij (kot so finančne ustanove) načeloma prenašati v tretje države – to lahko močno vplivalo na zahteve o tem, da bi bili isti podatki dostopni tudi organom kazenskega pregona v EU. Primer takšnega nezaželenega razvoja dogodkov je sistem PNR: vse skupaj se je začelo z zbiranjem neobdelanih podatkov o potnikih v neprečiščeni obliki s strani ZDA, nato pa naj bi se to začelo dogajati tudi v EU ([11]), kljub temu, da ni bilo jasno dokazano, ali je tak sistem v resnici potreben in sorazmeren.

22. ENVP pa je v mnenju o predlogu Komisije glede sistema PNR na ravni EU izpostavil tudi vprašanje o tem, kateri okvir za varstvo podatkov (prvi ali tretji steber) naj bi veljal za pogoje sodelovanja med javnimi in zasebnimi akterji: ali bi bilo treba pravila utemeljiti s tem, kdo je upravljavec podatkov (zasebni sektor), ali s predvidenim namenom (kazenski pregon)? Če so zasebni akterji primorani obdelovati osebne podatke za namene kazenskega pregona,

([8]) V zvezi s tem glej Mnenje ENPV z dne 20. decembra 2007 o osnutku predloga okvirnega sklepa Sveta o uporabi evidence podatkov o potnikih (PNR) za namene kazenskega pregona, UL C 110, 1.5.2008, str. 1. „Običajno so dejavnosti kazenskega pregona jasno ločene od dejavnosti zasebnega sektorja, pri čemer naloge kazenskega pregona opravljajo posebej temu namenjeni organi, zlasti policija, zasebni subjekti pa so od primera do primera naprošeni, da tem organom pregona pošljejo osebne podatke. Sedaj obstaja tendenca, da bi k sodelovanju za namene kazenskega pregona sistematično pritegnili zasebne subjekte […].“

([9]) Glej Mnenje 10/2006 Delovne skupine za varstvo podatkov iz člena 29 z dne 22. novembra 2006 o obdelavi osebnih podatkov s strani Združenja za svetovne finančne telekomunikacije med bankami (SWIFT – *Society for Worldwide Interbank Financial Telecommunication*), WP 128.

([10]) Mnenje z dne 20. decembra 2007, op. cit.

([11]) Glej predlog okvirnega sklepa Sveta o uporabi evidence podatkov o potnikih (PNR) za namene kazenskega pregona, naveden v opombi 8, o katerem Svet trenutno razpravlja.

je ločnica med prvim in tretjim stebrom vse prej kot jasna. S tem v zvezi je zato pomembno opozoriti, da je generalni pravobranilec Bot v nedavnem mnenju glede zadeve v zvezi s hrambo podatkov ([12]) predlagal jasno razlikovanje v takih primerih ter dodal, da takšna ločnica vsekakor ni nespremenljiva in da je lahko v določenih primerih videti, kot da je postavljena umetno. ENVP tudi ugotavlja, da sodba Sodišča v zvezi s PNR ([13]) ne odgovarja popolnoma na vprašanje o veljavnem pravnem okviru. Dejstvo, da direktiva 95/46/ES ne zajema določenih dejavnosti, še ne pomeni tudi, da je mogoče te dejavnosti urejati v okviru tretjega stebra. Posledično lahko glede veljavnega prava nastane pravna praznina, to pa v vsakem primeru povzroči pravno negotovost v zvezi s pravnimi jamstvi, ki jih imajo na voljo posamezniki, na katere se nanašajo osebni podatki.

23. ENVP zato poudarja, da je treba zagotoviti, da z bodočim instrumentom in splošnimi načeli varstva podatkov ne bo mogoče upravičiti čezatlantskega prenosa osebnih podatkov med zasebnimi in javnimi subjekti. Ta prenos lahko postane del bodočega instrumenta le pod naslednjimi pogoji:

— v bodočem instrumentu je določeno, da je tak prenos dovoljen le, če se izkaže, da je dejansko nujno potreben za specifičen namen, o čemer se odloča od primera do primera;

— prenos je zavarovan s strogimi zaščitnimi ukrepi za varstvo podatkov (kot je opisano v tem mnenju).

ENVP poleg tega opozarja na negotovi položaj glede veljavnega okvira za varstvo podatkov, zato se močno zavzema, da prenos osebnih podatkov med zasebnimi in javnimi subjekti glede na trenutno stanje prava EU v nobenem primeru ne bi bil vključen v področje uporabe novega instrumenta.

— Prenosi med javnimi organi

24. Ker ni natančno znano, kakšen naj bi bil obseg izmenjave informacij, bi bilo treba kot prvi korak v okviru prizadevanj za skupni instrument razjasniti predvideno področje uporabe takšnega instrumenta. Še zlasti so nerazjasnjena vprašanja v zvezi z naslednjim:

— kar zadeva zbirke podatkov v EU, ali naj bi bil instrument usmerjen predvsem na centralizirane zbirke podatkov, ki jih (delno) upravlja EU, kot sta npr. zbirki Europola in Eurojusta, oziroma na decentralizirane zbirke podatkov, ki jih upravljajo države članice, ali na ene in druge;

— področje uporabe instrumenta zajema tudi medsebojno povezana omrežja, ali se bodo torej predvidena jamstva nanašala na podatke, ki si jih izmenjujejo države članice oziroma agencije v EU in v ZDA;

— ali naj bi instrument zajemal samo izmenjavo med zbirkami podatkov na področju kazenskega pregona (policija, sodstvo, morebiti carina) ali tudi med drugimi zbirkami podatkov kot so zbirke davčnih podatkov;

— ali naj bi instrument vključeval tudi zbirke podatkov organov za nacionalno varnost oziroma ali naj bi tem organom omogočal dostop do zbirk podatkov organov za kazenski pregon na ozemlju druge pogodbenice (iz EU v ZDA in obratno);

— ali naj bi instrument omogočal prenos podatkov od primera do primera ali pa naj bi bil dostop do obstoječih zbirk podatkov trajne narave. Zadnja domneva bi nedvomno sprožila vprašanja glede sorazmernosti, kar je natančneje preučeno v točki 3 poglavja V.

Namen: kazenski pregon

25. Tudi opredelitev namena morebitnega sporazuma ni popolnoma jasna. Iz uvoda poročila pa tudi prvega načela iz priloge k poročilu je jasno razvidno, da gre za izmenjavo v namene kazenskega pregona; več o tem v poglavju IV tega mnenja. ENVP je že ugotovil, da je glede na te izjave videti, da bo izmenjava podatkov osredotočena na zadeve v okviru tretjega stebra, vendar se sprašuje, ali ni to le prvi korak k obsežnejši izmenjavi informacij. Zdi se jasno, da namen „javne varnosti“ iz poročila vključuje tudi boj proti terorizmu, organiziranemu kriminalu in drugim kaznivim dejanjem. Toda, ali to pomeni, da naj bi bila dovoljena tudi izmenjava podatkov zaradi drugih javnih interesov, kot so npr. morebitna tveganja za javno zdravje?

26. ENVP priporoča omejitev namena na natančno določeno obdelavo podatkov ter utemeljitev političnih odločitev, na podlagi katerih je prišlo do takšne opredelitve pomena.

([12]) Mnenje generalnega pravobranilca Bota z dne 14. oktobra 2008, Irska proti Evropskemu parlamentu in Svetu (zadeva 301/06), odstavek 108.

([13]) Sodba Sodišča z dne 30. maja 2006, Evropski parlament proti Svetu Evropske unije (C–317/04) in Komisiji Evropskih skupnosti (C–318/04), združeni zadevi C–317/04 in C–318/04, Zbirka odločb, (2006), stran I–4721.

Globalno čezatlantsko območje varnosti

27. Na širše področje uporabe tega poročila bi bilo treba gledati z vidika globalnega čezatlantskega območja varnosti, o katerem je razpravljala t. i. skupina za prihodnost notranjih zadev ([14]). V poročilu te skupine, ki je bilo objavljeno junija 2008, je v določeni meri poudarjena zunanja razsežnost politike na področju notranjih zadev. Zavzema se za to, da bi se morala Evropska unija do leta 2014 odločiti glede političnega cilja o vzpostavitvi evroatlantskega območja sodelovanja na področju svobode, varnosti in pravice z Združenimi državami. Takšno sodelovanje bi torej preseglo namen varnosti v strogem pomenu besede in bi vključevalo vsaj tematiko iz sedanjega naslova IV PES kot so priseljevanje, vizumi, azil in sodelovanje v civilnih zadevah. Vprašati se je treba, v kakšni meri bi se sporazum o osnovnih načelih varstva podatkov, kot je tisti iz poročila HLCG, lahko uporabil oziroma bi se moral uporabiti kot podlaga za izmenjavo podatkov na tako širokem področju.

28. Do leta 2014 naj bi bil stebrni ustroj ukinjen in v EU se bo za varstvo podatkov uporabljala samo ena pravna podlaga (glede na Lizbonsko pogodbo naj bi bil to člen 16 Pogodbe o delovanju Evropske unije). Ne glede na usklajeno *urejanje* varstva podatkov na ravni EU pa to še ne pomeni, da bi bil *prenos* kakršnih koli osebnih podatkov, ne glede na njegov namen, upravičen s sklenitvijo kakršnega koli sporazuma s tretjo državo. Za posebna področja, kot je kazenski pregon, bo morda treba jamstva glede varstva podatkov prilagoditi, odvisno od načina obdelave podatkov oziroma pogojev take obdelave. ENVP priporoča, da se pri pripravi bodočega instrumenta upoštevajo posledice teh različnih vidikov.

III.2. **Narava sporazuma**

Evropski institucionalni okvir

29. Vsaj na kratki rok je ključnega pomena, da se določi, v okviru katerega stebra bodo tekla pogajanja o navedenem instrumentu, zlasti zato, ker bo taka ureditev vplivala na notranji regulativni okvir za varstvo podatkov. Bo to okvir znotraj prvega stebra – v bistvu gre za direktivo 95/46/ES in njeno posebno ureditev za prenos podatkov v tretje države – ali pa okvir znotraj tretjega stebra, v katerem je za prenose v tretje države predvidena nekoliko manj stroga ureditev? ([15])

30. Instrument naj bi bil sicer namenjen predvsem kazenskemu pregonu, kljub temu pa je v poročilu HLCG omenjeno tudi zbiranje podatkov, s katerimi upravljajo zasebni akterji; tudi namene zbiranja si je mogoče razlagati v širšem smislu, ki ne zajema izključno varnosti, pač pa tudi vprašanja v zvezi s priseljevanjem in nadzorom mej, po možnosti pa tudi javno zdravje. Ob upoštevanju teh dvomov bi bilo veliko bolje počakati na uskladitev stebrov v okviru zakonodaje EU, kakor je predvideno v Lizbonski pogodbi, in šele nato oblikovati jasno pravno podlago za pogajanja ter točno določiti, kakšna je pri tem vloga evropskih institucij, zlasti Evropskega parlamenta in Komisije.

Zavezujoči značaj instrumenta

31. Določiti bi bilo treba, ali naj bi razprave zaključili z memorandumom o soglasju ali s kakšnim drugim nezavezujočim instrumentom, ali naj bi po njihovem zaključku sklenili zavezujoč mednarodni sporazum.

32. Poročilo je bolj naklonjeno zavezujočemu sporazumu, s čimer se strinja tudi ENVP. Meni namreč, da je uraden zavezujoč sporazum nepogrešljiv predpogoj za kakršen koli prenos podatkov izven EU, ne glede na namen izmenjave. / to, zakaj se podatki izmenjujejo. Prenosa podatkov v tretjo državo si ni mogoče zamisliti brez posebnega (zavezujočega) pravnega okvira z ustreznimi pogoji in zaščitnimi ukrepi. Povedano drugače: memorandum o soglasju ali drug nezavezujoč instrument sicer lahko koristno usmerja pogajanja glede nadaljnjih zavezujočih sporazumov, vendar nikakor ne more nadomestiti zavezujočega sporazuma.

Neposredni učinek

33. Določbe navedenega instrumenta bi morale biti v enaki meri zavezujoče za ZDA, EU in njene države članice.

34. Prav tako bi bilo treba zagotoviti, da bodo posamezniki lahko na podlagi dogovorjenih načel uveljavljali svoje pravice, zlasti glede pravnega varstva. ENVP meni, da bi lahko to najlažje dosegli tako, če bi bistvene določbe instrumenta oblikovali tako, da bodo imele neposreden učinek za prebivalce Evropske unije in se bo nanje mogoče sklicevati tudi pred sodiščem. V instrumentu je torej treba jasno navesti, kakšen bo neposredni učinek določb mednarodnega sporazuma, ter določiti pogoje za njegov prenos v notranjo evropsko in nacionalno zakonodajo in s tem poskrbeti za učinkovitost ukrepov.

Razmerje do drugih pravnih instrumentov

35. Bistvenega pomena je tudi, v kakšni meri se sporazum uporablja kot samostojen instrument oziroma ali ga je treba v posameznih primerih dopolniti z nadaljnjimi sporazumi o specifičnih izmenjavah podatkov. Dejansko je vprašljivo, ali so lahko v enem sporazumu, ki vsebuje en sam sklop standardov, ustrezno zajete številne posebnosti

([14]) Poročilo neformalne svetovalne skupine na visoki ravni za prihodnost evropske politike na področju notranjih zadev „Svoboda, varnost, zasebnost – evropske notranje zadeve v odprtem svetu“, junij 2008, na voljo na naslovu register.consilium.europa.eu

([15]) Glej člena 11 in 13 okvirnega sklepa Sveta o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah iz točke 7 tega mnenja.

obdelave podatkov v tretjem stebru. Še bolj je dvomljivo, ali bi smel brez dodatnih razprav in zaščitnih ukrepov *omogočati* vsesplošen prenos osebnih podatkov, ne glede na namen prenosa oziroma naravo zadevnih podatkov. Poleg tega za sporazume s tretjimi državami ni nujno, da so trajni, saj se lahko nanašajo na specifične nevarnosti, mogoče pa jih je tudi ponovno preučiti oziroma vanje vključiti klavzule o časovni omejitvi veljavnosti. Če pa bi, po drugi strani, v zavezujočem instrumentu imeli skupne minimalne standarde, bi lahko ti olajšali vse nadaljnje razprave glede prenosa osebnih podatkov v zvezi s specifičnimi zbirkami podatkov oziroma postopki obdelave.

36. ENVP je zato bolj kot samostojnemu sporazumu naklonjen oblikovanju sklopa minimalnih meril varstva podatkov, ki bi jih v posameznih primerih dopolnili z dodatnimi specifičnimi določbami, tako kot je predlagano v poročilu HLCG. Te dodatne specifične določbe so predpogoj za prenos podatkov v posameznih primerih, kar bo spodbudilo usklajeno ukrepanje v zvezi z varstvom podatkov.

Uporaba glede na obstoječe instrumente

37. Preučiti bi bilo treba tudi, kako bi se morebiten splošen sporazum uporabljal skupaj z obstoječimi sporazumi, sklenjenimi med EU in ZDA. Poudariti je treba, da ti veljavni sporazumi niso enako zavezujoči – zlasti gre za sporazum o PNR (ki nudi večjo pravno varnost), sporazuma z Europolom in Eurojustom oziroma izmenjavo pisem v zvezi z zadevo SWIFT ([16]). Ali bi novi splošni okvir dopolnil te obstoječe instrumente oziroma bi ti ostali nespremenjeni, saj bi se novi okvir uporabljal le za druge, bodoče izmenjave osebnih podatkov? ENVP meni, da bi zaradi pravne doslednosti potrebovali usklajen sklop pravil, ki bi veljala za obstoječe in bodoče zavezujoče instrumente za prenos podatkov ter jih dopolnjevala.

38. Prednost uporabe splošnega sporazuma za obstoječe instrumente bi bila okrepitev njihove zavezujoče narave. To bi bilo še zlasti dobrodošlo pri instrumentih, ki niso pravno zavezujoči, kot je npr. izmenjava pisem v zvezi z zadevo SWIFT, saj bi morali upoštevati sklop splošnih načel v zvezi z zasebnostjo.

IV. **SPLOŠNA PRAVNA OCENA**

39. V tem poglavju bo preučeno, kako oceniti raven varstva v določenem okviru oziroma instrumentu, vključno z vprašanjem meril, ki naj bi se pri tem uporabljala, ter potrebnimi osnovnimi zahtevami.

([16]) Glej opombo št. 2.

Ustrezna raven varstva

40. ENVP meni, da bi moralo biti jasno, da bi morali z bodočim instrumentom predvsem določiti, da bo prenos osebnih podatkov v Združene države mogoč le, če bodo oblasti v ZDA zanje zagotovile ustrezno raven varstva (in obratno).

41. ENVP meni, da bi lahko samo z dejanskim preskusom ustreznosti zagotovili ustrezna jamstva glede varstva osebnih podatkov, toda splošni okvirni sporazum, katerega področje uporabe bi bilo tako široko, kot je predlagano v poročilu HLCG, bi težko prestal dejanski preskus ustreznosti. Splošni sporazum bi lahko obveljal za ustreznega le, če bi se izkazalo, da so ustrezni tudi specifični sporazumi, sklenjeni za vsak primer posebej.

42. Ugotavljanje ravni varstva v tretjih državah je dokaj običajno, zlasti za Evropsko komisijo: ustreznost je v okviru prvega stebra ena od zahtev, ki jih je treba izpolniti za prenos. Ugotavljala se je ob različnih priložnostih, na podlagi specifičnih meril iz člena 25 direktive 95/46, potrjena pa je bila s sklepi Evropske komisije ([17]). V okviru tretjega stebra tak sistem ni izrecno predviden; merjenje ustreznosti varstva je predpisano le v posebnih okoliščinah iz členov 11 in 13 (še nesprejetega) okvirnega sklepa o varstvu podatkov ([18]) in je prepuščeno državam članicam.

43. V sedanjem primeru to ugotavljanje ustreznosti posega v namen kazenskega pregona, tovrstne razprave pa Komisija izvaja pod nadzorom Sveta. Ozadje je tu drugačno od ocenjevanja načel varnega pristana ali ustreznosti kanadske zakonodaje; v večji meri je povezano z nedavnimi pogajanji v zvezi s PNR z ZDA in Avstralijo v pravnem okviru tretjega stebra. Načela HLCG pa so bila omenjena tudi v povezavi s programom za odpravo vizumov, ki se nanaša na meje in priseljevanje in s tem na vprašanja v okviru prvega stebra.

44. ENVP priporoča, da bi v okviru bodočega instrumenta morale vse ugotovitve v zvezi z ustreznostjo temeljiti na izkušnjah, pridobljenih na teh različnih področjih, ter predlaga nadaljnjo opredelitev izraza „ustreznost“, in

([17]) Odločbe Komisije o ustreznosti ravni varstva osebnih podatkov v tretjih državah, vključno z Argentino, Kanado, Švico, Združenimi državami ter otoki Guernsey, Man in Jersey, so (v angleškem jeziku) na voljo na povezavi http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

([18]) Omejeno na prenos podatkov, ki jih država članica pridobi od pristojnih organov druge države članice, v tretjo državo ali mednarodni organizaciji.

sicer na podlagi podobnih meril, kot so bila uporabljena v predhodnih ugotovitvah o ustreznosti.

Medsebojno priznavanje – vzajemnost

45. Drugi element ravni varstva se nanaša na medsebojno priznavanje sistemov EU in ZDA. V zvezi s tem je v poročilu HLCG navedeno, da bi si bilo treba prizadevati za medsebojno priznanje učinkovitosti sistemov zasebnosti in varstva podatkov za področja, ki jih zajemajo ta načela ([19]), ter poskrbeti za enakovredno in vzajemno uporabo zakonodaje o zasebnosti in varstvu osebnih podatkov.

46. ENVP meni, da je medsebojno priznavanje (ali vzajemnost) očitno mogoče le, če je zagotovljena ustrezna raven varstva. Povedano drugače, z bodočim instrumentom bi bilo treba določiti usklajeno minimalno raven varstva (z ugotavljanjem ustreznosti, ob upoštevanju potrebe po specifičnih sporazumih za vsak primer posebej), saj bi bilo mogoče vzajemnost priznavati le ob tem predpogoju.

47. Najprej je pri tem treba upoštevati vzajemnost vsebinskih določb v zvezi z varstvom podatkov. ENVP meni, da bi moral sporazum ta pojem obravnavati tako, da bi bilo na eni strani zagotovljeno, da se pri obdelavi podatkov na ozemlju EU (in ZDA) dosledno upoštevajo tovrstni domači predpisi, po drugi strani pa bi bilo treba poskrbeti, da bi pri obdelavi v državi, ki ni država, od koder podatki izvirajo, in v okviru področja uporabe sporazuma upoštevali načela varstva podatkov, tako kot so zapisana v sporazumu.

48. Drugi element predstavlja vzajemnost pravnih sredstev. Zagotoviti bi bilo treba, da imajo evropski državljani v primerih, ko se podatki, povezani z njimi, obdelujejo v Združenih državah, na voljo ustrezna pravna sredstva (ne glede na predpise, ki veljajo za tako obdelavo), Evropska unija in njene države članice pa morajo zagotoviti enake pravice ameriškim državljanom.

49. Tretji element je vzajemnost pri dostopu organov kazenskega pregona do osebnih podatkov. Če bi določen instrument omogočil organom Združenih držav dostop do podatkov, ki izvirajo iz Evropske unije, bi po načelu vzajemnosti to pomenilo, da bi morali enak dostop do podatkov z izvorom v ZDA imeti tudi organi EU. Vzajemnost ne sme vplivati na učinkovitost varstva posameznika, na katerega se nanašajo osebni podatki, kar je tudi predpogoj, da se lahko organom kazenskega pregona omogoči čezatlantski dostop/dostop do „čezatlantskih“ podatkov. Konkretno to pomeni, da

— organom Združenih držav ne bi smel biti dovoljen neposreden dostop do podatkov na ozemlju EU (in obratno). Omogočen bi moral biti samo posreden dostop oziroma dostop po sistemu „push“;

— dostop bi morali nadzorovati organi za varstvo podatkov ter sodni organi v državi, kjer poteka obdelava podatkov;

— organi Združenih držav bi morali pri dostopu do zbirk podatkov v EU upoštevati vsebinske določbe o varstvu podatkov (glej zgoraj) ter posamezniku, na katerega se nanašajo osebni podatki, zagotoviti popolno pravno varstvo.

Natančnost instrumenta

50. Specifikacija pogojev ocenjevanja (ustreznost, enakovrednost, vzajemno priznavanje) je ključnega pomena, saj določa natančnost vsebine, pravno varnost in učinkovitost varstva. Vsebina bodočega instrumenta mora biti natančno določena.

51. Jasno bi moralo biti tudi, da bo moral tudi vsak nadaljnji specifični sporazum vsebovati podrobne in popolne zaščitne ukrepe za varstvo podatkov posameznika, v zvezi s katerim naj bi si izmenjali podatke. Kot je omenjeno že v točkah 35 in 36 tega mnenja, bi samo takšna dvojna mera konkretnih načel varstva podatkov zagotovila dobro ujemanje splošnih in specifičnih sporazumov.

Oblikovanje modela za druge tretje države

52. Posebno pozornost si zasluži vprašanje, v kakšni meri bi lahko sporazum z ZDA uporabljali kot model za druge tretje države. ENVP ugotavlja, da je v navedenem poročilu skupine za prihodnost notranjih zadev poleg ZDA kot strateški partner EU navedena tudi Rusija. Kolikor bodo načela nevtralna in v skladu s temeljnimi zaščitnimi ukrepi EU, bi bila lahko ustrezen primer navedenega. Sporazuma pa zaradi specifičnih lastnosti, povezanih z npr. pravnim okvirom države prejemnice ali namenom prenosa, ne bi bilo mogoče prenesti popolnoma brez težav. Podobno odločilno vlogo bo imelo tudi stanje demokracije v tretjih državah; prepričati bi se bilo treba, da bodo dogovorjena načela v tretjih državah tudi dejansko zajamčena in se bodo izvajala.

Merila za ocenjevanje ravni varstva

53. Implicitna oziroma eksplicitna ustreznost bi morala biti zagotovljena v skladu z mednarodnim in evropskim pravnim okvirom ter zlasti skladno s skupno dogovorjenimi zaščitnimi ukrepi za varstvo podatkov iz smernic Združenih narodov, konvencije Sveta Evrope št. 108 ter

([19]) Poglavje A. Zavezujoč mednarodni sporazum, str. 8.

dodatnega protokola k njej, smernic OECD, osnutka okvirnega sklepa o varstvu podatkov in direktive 95/46/ES (kar zadeva prvi steber) ([20]). Vsi ti instrumenti vsebujejo podobna načela, ki širše gledano veljajo za osrednji element varovanja osebnih podatkov.

54. Glede na učinek morebitnega sporazuma kot je npr. tisti, predviden v poročilu HLCG, je še toliko bolj pomembno, da so navedena načela ustrezno upoštevana. Instrumenta, ki bi zajemal celotni sektor *kazenskega pregona* v tretji državi, zaenkrat namreč še nimamo. Za obstoječe odločbe o ustreznosti v okviru prvega stebra ter sporazume s tretjimi državami v okviru tretjega stebra EU (Europol, Eurojust) velja, da se ponavadi navezujejo na specifičen prenos podatkov, s predlaganim instrumentom pa bi bilo mogoče zajeti mnogo širše področje, če upoštevamo, kako obsežen naj bi bil predvideni namen prenosa (preprečevanje kaznivih dejanj, državna in javna varnost, varovanje meja), ter pomanjkanje podatkov o tem, koliko zbirk podatkov naj bi instrument zajemal.

Temeljne zahteve

55. Pogoji, ki jih je treba upoštevati pri prenosu osebnih podatkov v tretje države, so bili oblikovani v delovnem dokumentu Delovne skupine iz člena 29 ([21]). Vsi sporazumi o minimalnih načelih v zvezi z zasebnostjo bi morali prestati preskus skladnosti in s tem zagotoviti učinkovitost zaščitnih ukrepov za varstvo podatkov.

— Vsebina: načela v zvezi z varstvom podatkov bi morala zagotavljati visoko raven zaščite ter izpolnjevati standarde v skladu z načeli EU. Podrobnejša analiza 12 načel iz poročila HLCG s tega vidika sledi v poglavju V tega mnenja.

— Specifičnost: pravila in postopki bi morali biti – glede na naravo sporazuma ter zlasti v primeru uradnih mednarodnih sporazumov – dovolj podrobni, da bi jih bilo mogoče učinkovito izvajati.

— Nadzor: zaradi zagotavljanja skladnosti z dogovorjenimi pravili bi bilo treba vzpostaviti specifične notranje (revizije) in zunanje mehanizme nadzora (pregledi), ki bi bili v enaki meri dostopni obema stranema, ki sta sklenili sporazum. Nadzor vključuje mehanizme za zagotavljanje skladnosti na makro ravni, kot so skupni mehanizmi pregleda, ter na mikro ravni, kot je pravno varstvo posameznika.

56. Poleg teh treh osnovnih zahtev bi bilo treba posebno pozornost nameniti tudi posebnostim obdelave osebnih podatkov v okviru kazenskega pregona, saj gre za področje, kjer lahko pride do določenega omejevanja temeljnih pravic. Zato bi bilo treba sprejeti zaščitne ukrepe, da bi s tem ublažili omejitev pravic posameznika, zlasti ob upoštevanju naslednjih vidikov in glede na to, kakšen je njihov vpliv na posameznika:

— preglednost: informacije in dostop do osebnih podatkov je mogoče v okviru kazenskega pregona omejiti, npr. zaradi diskretnosti preiskav. V EU se ta omejitev temeljnih pravic sicer običajno ublaži z vzpostavitvijo dodatnih mehanizmov (pri tem pogosto sodelujejo neodvisni organi za varstvo podatkov), treba pa je zagotoviti, da bodo podobni mehanizmi nadomestil na voljo tudi ob prenosu informacij v tretjo državo;

— pravno varstvo: iz prej navedenih razlogov bi morali imeti posamezniki pravico do alternativnih možnosti za zaščito svojih pravic, zlasti prek neodvisnih nadzornih organov in pred sodiščem;

— hramba podatkov: utemeljitev za obdobje hrambe podatkov včasih ni dovolj jasna, da pa to ne bi vplivalo na učinkovito uveljavljanje pravic posameznikov, na katere se nanašajo podatki, oziroma nadzornih organov, je treba sprejeti ustrezne ukrepe;

([20]) — Smernice Združenih narodov o računalniških datotekah o osebnih podatkih, ki jih je 14. decembra 1990 sprejela Generalna skupščina, na voljo na povezavi www.unhchr.ch/html/menu3/b/71.htm
— Konvencija Sveta Evrope z dne 28. januarja 1981 o varstvu posameznikov glede na avtomatsko obdelavo podatkov, na voljo na povezavi http://www.conventions.coe.int/treaty/en/Treaties/html/108.htm
— Smernice OECD o varovanju zasebnosti in čezmejnem prenosu osebnih podatkov, sprejete 23. septembra 1980, na voljo na povezavi www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html
— Osnutek okvirnega sklepa Sveta o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah, na voljo na povezavi http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=sl&DosId=193371
— Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov, UL L 281, 23.11.1995, str. 31.

([21]) Delovni dokument z dne 24. julija 1998 o prenosih podatkov v tretje države ter uporabi členov 25 in 26 direktive EU o varstvu podatkov; WP12.

— odgovornost organov kazenskega pregona: mehanizmi nadzora, ki jih vzpostavijo posamezne ali institucionalne zainteresirane strani, nikakor ne morejo veljati za celovite, če ni zagotovljena učinkovita preglednost. Še vedno je ključnega pomena, da ima takšen nadzor trdno podlago, in sicer zaradi občutljivosti podatkov ter prisilnih ukrepov, ki jih je mogoče sprejeti zoper posameznike na podlagi obdelave podatkov. Odgovornost je odločilna pri nacionalnih mehanizmih nadzora države prejemnice, pa tudi v okviru možnosti za pregled v državi oziroma regiji izvora podatkov. Takšni mehanizmi pregleda so predvideni v specifičnih sporazumih, kot je sporazum o PNR, ENVP pa močno priporoča, da bi jih vključili tudi v splošni instrument.

V. **ANALIZA NAČEL**

Uvod

57. V tem poglavju je analiziranih 12 načel iz dokumenta HLCG, in sicer z naslednjega vidika:

— iz teh načel je razvidno, da imata ZDA in EU v zvezi z njimi določena skupna stališča, saj so podobna načelom iz konvencije št. 108;

— toda le načelni sporazum ni dovolj. Pravni instrument bi moral biti dovolj zavezujoč, da bi ga upoštevale vse strani;

— ENVP obžaluje, da načelom ni priložen tudi obrazložitveni memorandum;

— preden se lotimo opisa načel, bi bilo treba nedvoumno zagotoviti, da si obe strani na enak način razlagata uporabljeno formulacijo, na primer kar zadeva pojem „osebni podatek“ ali pojem posameznikov, ki uživajo varstvo. V tem pogledu bi bilo zato priporočljivo oblikovati opredelitve.

1. Opredelitev namena

58. Prvo načelo s seznama v poročilu HLCG je, da se osebni podatki obdelujejo za zakonite namene kazenskega pregona. Kakor je bilo že navedeno, za Evropsko unijo to pomeni preprečevanje, odkrivanje, preiskavo oziroma pregon kaznivih dejanj. Kar pa zadeva ZDA, kazenski pregon ne zajema le kaznivih dejanj, pač pa vključuje tudi namene varovanja meja, javne varnosti in državne varnosti. Ni znano, kakšne bodo posledice takšnega razlikovanja med nameni pregona v EU in v ZDA. Čeprav je v poročilu navedeno, da se ti nameni v praksi sicer lahko v veliki meri ujemajo, je odločilnega pomena natančna informacija o tem, v kakšnem obsegu se ti nameni *ne* ujemajo. Na področju kazenskega pregona je treba ob upoštevanju vpliva ukrepov na posameznike strogo upoštevati načelo omejitve namena, navedeni namen pa mora biti jasen in omejen. Glede na vzajemnost, ki je predvidena v poročilu, se zdi, da je ključnega pomena tudi zbliževanje teh namenov. Na kratko, treba je pojasniti, kako naj bi si razlagali to načelo.

2. Celovitost/kakovost podatkov

59. ENVP pozdravlja določbo o natančnih, ustreznih, pravočasnih in popolnih osebnih podatkih, ki so potrebni za zakonito obdelavo. Takšno načelo je osnovni pogoj za učinkovito obdelavo podatkov.

3. Nujnost/sorazmernost

60. Navedeno načelo jasno povezuje zbrane informacije ter nujnost teh informacij za dosego namena v okviru kazenskega pregona, kakor je določen z zakonom, ta pravna podlaga pa je potrebna zato, da se zagotovi zakonitost obdelave. ENVP ugotavlja, da je pravna varnost zaradi te določbe sicer res boljša, vendar pa pravna podlaga za takšno obdelavo izvira iz prava tretje države, ki samo po sebi ne more biti zakonita podlaga za prenos osebnih podatkov ([22]). Glede na poročilo HLCG je mogoče sklepati, da pravo tretje države, tj. Združenih držav, načeloma velja za legitimno. Toda upoštevati je treba – če lahko na tem mestu sploh uporabimo tako utemeljitev –, da v Združenih državah, ki sicer veljajo za demokratično državo, isti sistem ne bi bil veljaven in ga ne bi bilo mogoče prenesti na odnose z drugimi tretjimi državami.

61. Skladno s prilogo k poročilu HLCG mora biti vsak prenos osebnih podatkov ustrezen, nujen in primeren. ENVP poudarja, da obdelava, če naj bo sorazmerna, ne sme biti preveč moteča, uskladiti pa bi bilo treba tudi načine obdelave ter pri tem upoštevati pravice in interese posameznikov, na katere se nanašajo osebni podatki.

62. Dostop do informacij bi morali omogočiti za vsak primer posebej, odvisno od praktičnih potreb v okviru specifične preiskave. Stalen dostop organov kazenskega pregona tretjih držav do zbirk podatkov v EU bi bil nesorazmeren

([22]) Glej zlasti člen 7(c) in (e) Direktive 95/46/ES. Delovna skupina iz člena 29 je v svojem mnenju št. 6/2002 z dne 24. oktobra 2002 o prenosu očitnih informacij o potnikih in drugih podatkov s strani letalskih družb Združenim državam izjavila, da se ne zdi sprejemljivo, da bi bil na podlagi enostranske odločitve tretje države, ki jo ta sprejme zaradi lastnega javnega interesa, omogočen rutinski, vsesplošen prenos podatkov, ki so zavarovani z navedeno direktivo.

in nezadostno utemeljen. ENVP opozarja, da izmenjava podatkov tudi v okviru veljavnih sporazumov te vrste, tj. sporazuma o PNR, temelji na specifičnih okoliščinah in se izvaja le v omejenem časovnem obdobju ([23]).

63. Zato bi bilo treba določiti tudi obdobje hrambe podatkov: podatke bi morali hraniti le toliko časa, dokler so potrebni za predvideni specifičen namen. Če pa v zvezi z navedenim namenom niso več potrebni, bi jih bilo treba izbrisati. ENVP močno nasprotuje vzpostavitvi podatkovnih skladišč, v katerih bi hranili informacije o osebah, ki sicer niso ničesar osumljene, za primer, če bi te podatke morda potrebovali kdaj v prihodnosti.

4. Varnost podatkov

64. V načelih so oblikovani ukrepi in postopki za varovanje podatkov proti zlorabi, predelavi in drugemu tveganju, vsebujejo pa tudi določbo o omejevanju dostopa le na pooblaščene osebe, za kar ENVP meni, da je zadovoljivo.

65. Navedeno načelo bi bilo mogoče dopolniti še z določbo o tem, da se vodi evidenca o osebah, ki imajo dostop do podatkov, saj bi s tem okrepili učinkovitost zaščitnih ukrepov za omejitev dostopa in preprečili zlorabo podatkov.

66. Pri kršitvah na področju varnosti bi bilo poleg tega treba predvideti vzajemno obveščanje: prejemniki v ZDA in v EU, ki so prejeli nezakonito razkrite podatke, bi morali o tem obvestiti tudi druge prejemnike. To bo prispevalo k večji odgovornosti za varno obdelavo podatkov.

5. Posebne vrste osebnih podatkov

67. ENVP meni, da je načelo o prepovedi obdelave občutljivih podatkov precej oslabljeno zaradi izjeme, ki takšno obdelavo dovoljuje v primeru, če so v notranjem pravu predvideni ustrezni zaščitni ukrepi. Vsakršno odstopanje od načela o prepovedi je treba prav zaradi občutljivosti tovrstnih podatkov ustrezno in natančno utemeljiti s seznamom namenov in okoliščin, v okviru katerih je navedene vrste občutljivih podatkov mogoče obdelovati, ter navesti, kateri upravljavci podatkov smejo obdelovati takšne vrste podatkov. Kar zadeva zaščitne ukrepe, ki naj bi jih sprejeli, ENVP meni, da občutljivih podatkov ne bi smeli uporabljati kot razlog za začetek preiskave. Na voljo bi bili lahko v posebnih okoliščinah, vendar le v obliki dodatnih informacij o posamezniku, na katerega se nanašajo osebni podatki in ki je že v postopku preiskave. Besedilo načela bi moralo vsebovati izčrpen seznam teh zaščitnih ukrepov in pogojev.

6. Odgovornost

68. V točkah 55 in 56 tega mnenja je navedeno, da je treba zagotoviti učinkovito odgovornost javnih subjektov, ki obdelujejo osebne podatke, v sporazumu pa je treba poskrbeti tudi za ustrezna zagotovila v zvezi s to odgovornostjo. To je še toliko bolj pomembno ob upoštevanju premajhne preglednosti, ki jo običajno povezujemo z obdelavo osebnih podatkov pri kazenskem pregonu. Določba o odgovornosti javnih subjektov, ki je navedena v prilogi, vendar brez kakršnega koli nadaljnjega pojasnila o vrstah in posledicah take odgovornosti, ne predstavlja zadostnega jamstva. ENVP priporoča, da se takšno pojasnilo navede v besedilu instrumenta.

7. Neodvisen in učinkovit nadzor

69. ENVP v celoti podpira vključitev določbe o zagotavljanju neodvisnega in učinkovitega nadzora, za kar naj bi poskrbel en ali več javnih nadzornih organov. Meni, da bi bilo treba razjasniti, kako naj bi si to neodvisnost razlagali, zlasti glede tega, od koga so ti organi neodvisni in komu poročajo. V zvezi s tem je treba vzpostaviti merila, v katerih bi bilo treba upoštevati institucionalno in funkcionalno neodvisnost glede na izvršilne in zakonodajne organe. ENVP opozarja, da gre za bistven element zagotavljanja učinkovite skladnosti z dogovorjenimi načeli. Prav tako so, kakor je bilo že navedeno, ključnega pomena intervencijska in izvršilna pooblastila teh organov, kar zadeva odgovornost javnih subjektov, ki obdelujejo osebne podatke. Posamezniki, na katere se nanašajo osebni podatki, bi morali biti dobro seznanjeni z obstojem in pristojnostmi teh organov, kar bi jim omogočilo uveljavljanje njihovih pravic, zlasti v primerih, ko je za obdelavo pristojnih več organov.

70. ENVP poleg tega priporoča, da bi v bodoči instrument vključili tudi mehanizem sodelovanja med nadzornimi organi.

8. Individualni dostop in popravek

71. Za dostop in popravek so v okviru kazenskega pregona potrebna specifična jamstva. ENVP v tem pogledu pozdravlja načelo, ki določa, da imajo posamezniki možnost oziroma bi morali imeti možnost popravka in/ali izbrisa svojih osebnih podatkov ter da imajo oziroma bi morali imeti za to na voljo potrebna sredstva. Vendar pa še ni popolnoma jasno, koga vse zajema opredelitev posameznika (zavarovati bi bilo treba vse posameznike,

([23]) Ta sporazum bo prenehal veljati in učinkovati sedem let od dne podpisa, razen če se pogodbenici dogovorita, da ga bosta nadomestili.

na katere se nanašajo osebni podatki, ne samo državljane zadevne države), niso pa znani tudi pogoji, na podlagi katerih bi lahko posamezniki ugovarjali obdelavi njihovih podatkov. Natančneje bi bilo treba določiti t. i. „po potrebi“, ko bi bil ugovor mogoč ali ne. Posamezniki, na katere se nanašajo osebni podatki, morajo biti seznanjeni s tem, v kakšnih okoliščinah, tj. odvisno od vrste organa, vrste preiskave oziroma glede na druga merila, bodo lahko uveljavljali svoje pravice.

72. Če obdelavi ni mogoče ugovarjati neposredno, z utemeljenimi razlogi, bi moralo biti na voljo posredno preverjanje preko neodvisnega organa, pristojnega za nadzor obdelave.

9. Preglednost in obvestilo

73. ENVP ponovno poudarja, kako pomembna je učinkovita preglednost; posameznikom naj bi omogočila uveljavljanje njihovih pravic ter prispevala k splošni odgovornosti javnih subjektov, ki obdelujejo osebne podatke. Podpira pripravljeni osnutek načel in zlasti vztraja pri potrebi po splošnem *in* posameznem obveščanju posameznika, kar je razvidno iz načela v točki 9 priloge.

74. Toda v poročilu je v poglavju 2, A. B (dogovorjena načela) navedeno, da lahko v ZDA preglednost vključuje objavo individualnega obvestila v Zveznem registru in/ali razkritje v sodnem postopku. Jasno bi bilo treba določiti, da objava v uradnem listu ni zadostno jamstvo, da bo posameznik, na katerega se nanašajo osebni podatki, ustrezno obveščen. ENVP poleg potrebe po individualnem obvestilu opozarja tudi na to, da morajo biti informacije na voljo v takšni obliki in jeziku, ki sta posamezniku, na katerega se nanašajo osebni podatki, razumljiva.

10. Pravna sredstva

75. Da bi posamezniku zagotovili učinkovito uveljavljanje njegovih pravic, mu mora biti omogočeno, da lahko vloži pritožbo pri neodvisnem organu za varstvo osebnih podatkov oziroma mora imeti pravico do pravnega sredstva pred neodvisnim in nepristranskim sodiščem, obe možnosti morata biti enako dostopni.

76. Neodvisni organi za varstvo podatkov so potrebni zato, ker v okviru kazenskega pregona, ki je lahko za posameznika precej nerazumljiv, zagotavljajo prožno in cenejšo pomoč. Navedeni organi lahko pomagajo tudi pri uveljavljanju pravic v imenu posameznikov, na katere se nanašajo osebni podatki, če ti zaradi izjem ne morejo neposredno dostopati do svojih osebnih podatkov.

77. Dostop do pravosodnega sistema je dodatno in nepogrešljivo jamstvo, da lahko posamezniki, na katere se nanašajo osebni podatki, poiščejo pravno varstvo pri organu iz druge veje demokratičnega sistema in ne pri javnih institucijah, ki dejansko obdelujejo njihove osebne podatke. Evropsko sodišče ([24]) je takšno učinkovito pravno sredstvo pred sodiščem razglasilo kot bistveno, da se posamezniku zagotovi učinkovita zaščita njegove pravice; predstavlja namreč izraz splošnega načela prava Skupnosti, ki izhaja iz skupnih ustavnih tradicij držav članic in je potrjeno v členih 6 in 13 Evropske konvencije za varstvo človekovih pravic in temeljnih svoboščin. Pravno sredstvo je izrecno predvideno tudi v členu 47 Listine Evropske unije o temeljnih pravicah ter v členu 22 Direktive 95/46/ES brez poseganja v kakršna koli upravnopravna sredstva.

11. Avtomatizirane posamezne odločitve

78. ENVP pozdravlja odločbo o ustreznih zaščitnih ukrepih pri avtomatizirani obdelavi osebnih podatkov. Ugotavlja, da bi enotno razumevanje besedne zveze „znatne škodljive posledice za zadevne interese posameznika“ pripomoglo k jasnejšim pogojem za uporabo tega načela.

12. Nadaljnji prenos

79. Nekateri pogoji v zvezi z nadaljnjimi prenosi so nejasni. Zlasti v primerih, ko mora nadaljnji prenos potekati v skladu z mednarodnimi sporazumi in dogovori med državo pošiljateljico in državo prejemnico, bi bilo treba natančno določiti, ali se to nanaša na sporazume med državama, med katerima je bil izveden prvi prenos, ali med državama, ki sta vključeni v nadaljnji prenos. ENVP meni, da bi moral biti sporazum v vsakem primeru sklenjen med državama, med katerima je bil izveden prvi prenos.

80. ENVP poleg tega ugotavlja, da je opredelitev izraza „zakoniti javni interesi“, ki omogoča nadaljnji prenos, zelo široka. Še vedno ni jasno, v kakšni meri se nanaša na javno varnost, razširitev prenosov pri kršitvah etike ali v zakonsko urejenih poklicih v okviru kazenskega pregona pa se zdi neutemeljeno in pretirano.

VI. **SKLEPNE UGOTOVITVE**

81. ENVP pozdravlja skupna prizadevanja oblasti EU in ZDA na področju kazenskega pregona, kjer je varstvo podatkov bistvenega pomena. Kljub temu pa vztraja, da gre za kompleksno zadevo, zlasti kar zadeva točno področje uporabe in naravo, zato jo je treba skrbno in natančno analizirati. Podrobno bi bilo treba preučiti,

([24]) Zadeva 222/84 *Johnston* (1986) Recueil 1651; zadeva 222/86 *Heylens* (1987) Recueil 4097; zadeva C-97/91 *Borelli* (1992), Recueil I-6313.

kakšen bi bile lahko posledice čezatlanskega instrumenta za varstvo podatkov za veljavni pravni okvir in državljane.

82. ENVP poziva k večji jasnosti in konkretnejšim določbam, zlasti v zvezi z naslednjimi vidiki:

— razjasnitev narave instrumenta, ki bi moral biti pravno zavezujoč, da bi lahko zagotovil zadostno pravno varnost;

— temeljito ugotavljanje ustreznosti na podlagi bistvenih zahtev glede vsebine, specifičnosti in nadzora predvidenega sistema. ENVP meni, da bi splošni instrument lahko za ustreznega obveljal le, če bi se za ustrezne izkazali tudi specifični sporazumi, sklenjeni za vsak primer posebej;

— določeno področje uporabe z jasno in enotno opredelitvijo zadevnih namenov kazenskega pregona;

— natančna opredelitev načinov za vključitev zasebnih subjektov v sisteme prenosov podatkov;

— skladnost z načelom sorazmernosti, iz katerega sledi, da izmenjava podatkov poteka za vsak primer posebej, glede na konkretne potrebe;

— močni nadzorni mehanizmi in mehanizmi pravnih sredstev, ki so na voljo posameznikom, na katere se nanašajo osebni podatki, vključno z upravnopravnimi in pravnimi sredstvi;

— učinkoviti ukrepi, s katerimi se zagotavlja uveljavljanje pravic vseh posameznikov, na katere se nanašajo osebni podatki, ne glede na njihovo državljanstvo;

— sodelovanje neodvisnih organov za varstvo podatkov, zlasti pri nadzoru in pomoči posameznikom, na katere se nanašajo osebni podatki.

83. ENVP vztraja, da bi bilo treba oblikovanju načel posvetiti dovolj časa, saj bodo sprejete rešitve sicer nezadostne, njihov učinek na varstvo podatkov pa ravno nasproten od zaželenega. Na tej točki bi bilo najbolje oblikovati časovni načrt za nekoliko kasnejšo sklenitev morebitnega sporazuma.

84. ENVP tudi poziva k večji preglednosti v postopku oblikovanja načel varstva podatkov. Demokratična razprava o instrumentu je mogoča le s sodelovanjem vseh zainteresiranih strani, tudi Evropskega parlamenta, saj bo instrument le na ta način pridobil ustrezno podporo in priznanje.

V Bruslju, 11. novembra 2008

Peter HUSTINX

Evropski nadzornik za varstvo podatkov

Mnenje Evropskega nadzornika za varstvo podatkov o sporočilu Komisije Evropskemu parlamentu, Svetu in Evropskemu ekonomsko-socialnemu odboru – Za evropsko strategijo na področju e-pravosodja

(2009/C 128/02)

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV JE –

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

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

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

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

SPREJEL NASLEDNJE MNENJE:

I. UVOD

1. Sporočilo Komisije Evropskemu parlamentu, Svetu in Evropskemu ekonomsko-socialnemu odboru – Za evropsko strategijo na področju e-pravosodja (v nadaljnjem besedilu: sporočilo) je bilo sprejeto 30. maja 2008. ENVP v skladu s členom 41 uredbe (ES) št. 45/2001 predstavlja svoje mnenje.

2. Namen sporočila je predlagati strategijo na področju e-pravosodja, ki naj bi povečala zaupanje državljanov v evropsko območje pravice. Glavni cilj e-pravosodja naj bi bil po vsej Evropi povečati učinkovitost pravosodja v korist državljanov. Ukrepi Evropske unije naj bi državljanom omogočili dostop do informacij, pri čemer morajo biti odpravljene jezikovne, kulturne in pravne ovire zaradi različnosti sistemov. Sporočilu sta priložena osnutek akcijskega načrta in časovni razpored različnih projektov.

3. To mnenje ENVP zadeva tiste dele sporočila, ki se nanašajo na obdelavo osebnih podatkov, varstvo zasebnosti na področju elektronskih komunikacij in prosti pretok podatkov.

[1] UL L 281, 23.11.1995, str. 31.
[2] UL L 8, 12.1.2001, str. 1.

II. OZADJE IN OKVIR

4. Svet PNZ je junija 2007 [3] opredelil več prednostnih nalog pri razvoju e-pravosodja:

— vzpostavitev evropskega vmesnika, portala e-pravosodja;

— vzpostavitev pogojev za povezovanje različnih registrov, kot so kazenske evidence, registri plačilne nesposobnosti, trgovinski in poslovni registri ter zemljiške knjige;

— začetek priprav za uporabo IKT pri postopku za evropski plačilni nalog;

— večja uporaba tehnologije za videokonference v čezmejnih postopkih, predvsem pri pridobivanju dokazov;

— razvoj podpornih orodij za prevajanje in tolmačenje.

5. Delo na področju e-pravosodja je od takrat nenehno napredovalo. Po mnenju Komisije je treba prednost dati operativnim projektom in decentraliziranim strukturam ter hkrati zagotoviti usklajevanje na evropski ravni in uporabiti obstoječe pravne instrumente, pri čemer je treba njihovo učinkovitost izboljšati s pomočjo računalniških orodij. Projekt e-pravosodja [4] je podprl tudi Evropski parlament.

6. Komisija dosledno spodbuja uporabo sodobne informacijske tehnologije na civilno- pa tudi kazenskopravnem področju. Tako so bili razviti instrumenti, kot je evropski plačilni nalog. Komisija že od leta 2003 upravlja „portal“ Evropske pravosodne mreže v civilnih in gospodarskih zadevah, ki je državljanom na voljo v 22 jezikih. Prav tako je zasnovala in vzpostavila evropski pravosodni atlas. To so predhodniki prihodnjega evropskega okvira za e-pravosodje. Na kazenskopravnem področju Komisija razvija mehanizem, ki naj bi omogočil izmenjavo informacij iz kazenskih evidenc držav članic [5]. Poleg tega sistema za varno komunikacijo z nacionalnimi organi ni razvila samo Komisija, temveč tudi Eurojust.

[3] Dok. 10393/07 JURINFO 21.
[4] Glej osnutek poročila Evropskega parlamenta, Odbor za pravne zadeve.
[5] Glej zlasti sistem ECRIS, o katerem govorimo v nadaljevanju.

7. Z e-pravosodjem naj bi ustvarili več možnosti, da bi v prihodnjih letih konkretizirali evropsko pravosodje za državljane. Komisija je sprejela sporočilo o e-pravosodju, da bi tako začrtala splošno strategijo za to pomembno področje. V sporočilu so določena objektivna merila za določitev prednostnih nalog, zlasti za prihodnje projekte na evropski ravni, tako da bi konkretne rezultate dosegli v doglednem času.

8. V delovnem dokumentu služb Komisije, tj. spremnem dokumentu k sporočilu s povzetkom ocene učinka, je predstavljeno tudi ozadje ([6]). Pri pripravi poročila o oceni učinka so upoštevali odziv držav članic, pravosodnih organov, pravosodnih delavcev, državljanov in gospodarstvenikov, z ENVP pa se niso posvetovali. V poročilu o oceni učinka so kot najprimernejšo za reševanje problemov označili možnost, ki združuje evropsko razsežnost in nacionalne sposobnosti. To možnost so izbrali tudi v sporočilu. Strategija bo usmerjena v uporabo videokonference, vzpostavitev portala e-pravosodje, izboljšanje prevajalskih orodij z razvojem spletnih orodij za samodejno prevajanje, izboljšanje komuniciranja med pravosodnimi organi, boljše povezave med nacionalnimi evidencami in spletna orodja za evropske postopke (na primer evropski plačilni nalog).

9. ENVP podpira to usmeritev. Na splošno podpira vsestranski pristop k e-pravosodju. Strinja se, da je treba izboljšati tri stvari: dostopnost sodnega varstva, sodelovanje med evropskimi pravosodnimi organi in učinkovitost samega pravosodnega sistema. Ta pristop vključuje več institucij in oseb:

— države članice, ki so najbolj odgovorne za zagotavljanje učinkovitih pravosodnih sistemov, vrednih zaupanja;

— Evropsko komisijo v vlogi varuha pogodb;

— pravosodne organe držav članic, ki potrebujejo boljša orodja za komuniciranje zlasti v čezmejnih postopkih;

— pravosodne delavce, državljane in podjetja, ki se vsi zavzemajo za večjo uporabo računalniških orodij, da bi našli boljše rešitve za svoje potrebe na področju pravosodja.

10. Sporočilo se tesno navezuje na predlog sklepa Sveta o vzpostavitvi Evropskega informacijskega sistema kazenskih evidenc (ECRIS), o katerem je ENVP 16. septembra 2008 izdal mnenje ([7]). Predlog je podprl, vendar je treba upoštevati več pripomb. ENVP je predvsem poudaril, da bi bila potrebna dodatna jamstva glede varstva podatkov, saj trenutno ni celovitega tovrstnega pravnega okvira na področju sodelovanja policijskih in pravosodnih organov. Zato je poudaril, da je treba učinkovito nadzirati varstvo podatkov v sistemu, pri čemer bi morali sodelovati organi držav članic in Komisije, ki zagotavlja skupno komunikacijsko infrastrukturo.

11. Izpostaviti bi bilo treba predvsem ta priporočila iz mnenja:

— zahteva po visoki ravni varstva podatkov kot predpogoju za izvajanje sprejetih ukrepov;

— jasna določitev odgovornosti Komisije za skupno infrastrukturo sistema ter uporabe uredbe (ES) št. 45/2001, s čimer bi zagotovili večjo pravno varnost;

— prav tako bi morala biti Komisija – in ne države članice – odgovorna za programsko opremo za povezovanje, tako da bi bila izmenjava bolj učinkovita in nadzor nad sistemom boljši;

— samodejno prevajanje bi bilo treba jasno opredeliti in omejiti, tako da bi zagotovili vzajemno poznavanje kaznivih dejanj brez poseganja v kakovost posredovanih informacij.

12. Ta priporočila bi bilo treba upoštevati tudi pri analizi sporočila.

III. **IZMENJAVA INFORMACIJ, PREDVIDENA V SPOROČILU**

13. E-pravosodje sega na zelo raznolika področja in med drugim vključuje tudi uporabo informacijsko-komunikacijske tehnologije v pravosodju v Evropski uniji ter celo vrsto vprašanj, kot so projekti učinkovitejšega obveščanja strank v postopku, na primer s podatki o pravosodnih sistemih, zakonodaji in sodni praksi, objavljenimi na spletu, s sistemi elektronskega komuniciranja med strankami

([6]) Delovni dokument služb Komisije – Spremni dokument k Sporočilu Svetu, Evropskemu parlamentu in Evropskemu socialno-ekonomskemu odboru „Za evropsko strategijo na področju e-pravosodja“ – Povzetek ocene učinka, 30.5.2008, SEC(2008) 1944.

([7]) Glej mnenje ENVP o vzpostavitvi Evropskega informacijskega sistema kazenskih evidenc (ECRIS) na podlagi člena 11 okvirnega sklepa 2008/XX/PNZ; na voljo (v angleškem jeziku) na spletni strani ENVP, www.edps.europa.eu pod naslovom „consultation“ in nato „opinions“, „2008“.

in sodišči ter uvedba popolnoma elektronskih postopkov. Sem spadajo tudi evropski projekti, kot je uporaba elektronskih orodij za snemanje obravnav, in projekti izmenjave informacij ali povezovanja.

14. Kljub temu raznolikemu področju uporabe ENVP ugotavlja, da bodo zajeti podatki o kazenskih postopkih in o sistemih civilnega in gospodarskega pravosodja, ne pa tudi o sistemih upravnega sodstva. Prav tako bo vzpostavljena povezava s kazenskim in civilnim atlasom, ne pa tudi z upravnim atlasom, čeprav bi bilo morda koristneje, da bi imeli državljani in podjetja dostop do sistemov upravnega sodstva, tj. upravnega prava in pritožbenega postopka. Zagotoviti bi bilo treba tudi povezavo z Združenjem državnih svetov. Te dopolnitve bi lahko bile koristnejše za državljane, ki iščejo pot skozi gozd, ki ga pogosto predstavlja upravno pravo z vsemi različnimi sodišči, saj bi jih bolje seznanjale s sistemi upravnega sodstva.

15. ENVP zato predlaga, da se v e-pravosodje vključijo tudi upravni postopki. Kot del te nove sestavine bi bilo treba začeti projekte e-pravosodja, s katerimi bi zagotovili opaznejšo vlogo pravil o varstvu podatkov pa tudi nacionalnih organov za varstvo podatkov, zlasti pri vrstah podatkov, ki se obdelujejo v okviru e-pravosodja. To bi bilo v skladu s t. i. londonsko pobudo, ki so jo organi za varstvo podatkov sprožili novembra 2006 z namenom „obveščanja o varstvu podatkov in izboljšanja njegove učinkovitosti".

IV. **NOVI OKVIRNI SKLEP O VARSTVU PODATKOV V OKVIRU POLICIJSKEGA IN PRAVOSODNEGA SODELOVANJA V KAZENSKIH ZADEVAH**

16. Zaradi večje izmenjave informacij med pravosodnimi organi, predvidene v sporočilu, je uporaba pravnega okvira za varstvo podatkov še pomembnejša. ENVP v zvezi s tem ugotavlja, da je Svet Evropske unije 27. novembra, to je tri leta po prvem predlogu Komisije, sprejel okvirni sklep o varstvu podatkov v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah ([8]). Ta novi zakonodajni akt bo poleg določb za varstvo podatkov v „prvem stebru" iz direktive 95/46/ES zagotovil tudi splošni pravni okvir za varstvo podatkov za zadeve iz „tretjega stebra".

17. ENVP pozdravlja ta pravni akt kot prvi opazni korak proti varstvu podatkov v okviru policijskega in pravosodnega sodelovanja. Vendar pa končno besedilo ne zagotavlja v celoti zadovoljive ravni varstva podatkov. Okvirni sklep namreč zajema le policijske in pravosodne podatke, izmenjane med državami članicami, organi in sistemi EU, ne pa tudi domačih podatkov. Sprejeti okvirni sklep prav tako ne določa obveznosti razlikovanja med različnimi kategorijami posameznikov, na katere se nanašajo podatki, kot so osumljenci, storilci kaznivih dejanj, priče in žrtve, s čimer bi zagotovili ustreznejša varovala pri obdelovanju njihovih podatkov. Nadalje ni v celoti skladen z direktivo 95/46/ES, zlasti pri omejitvi namenov, za katere so osebni podatki lahko nadalje obdelani. Niti ne predvideva neodvisne skupine ustreznih nacionalnih organov in organov EU za varstvo podatkov, ki bi lahko poskrbela za večjo usklajenost organov za varstvo podatkov ter znatno prispevala k enotni uporabi okvirnega sklepa.

18. Posledica tega bi bila, da bi hkrati z močnim prizadevanjem za razvoj skupnih sistemov čezmejne izmenjave osebnih podatkov še vedno obstajale razlike v pravilih za obdelovanje teh podatkov in za uveljavljanje pravic državljanov v različnih državah EU.

19. ENVP še enkrat poudarja, da sta poleg drugih ukrepov, predvidenih za pospešitev čezmejne izmenjave osebnih podatkov pri kazenskem pregonu, bistveni tudi visoka raven varstva podatkov v policijskem in pravosodnem sodelovanju ter skladnost z direktivo 95/46/ES. Ne le zato, ker je pravica državljanov, da se spoštuje njihova temeljna pravica varstva osebnih podatkov, temveč tudi zato, ker morajo organi kazenskega pregona zagotoviti izmenjavo kakovostnih podatkov, kar potrjuje tudi priloga sporočila o povezovanju kazenskih evidenc, zaupanje med organi v različnih državah in nazadnje tudi pravno veljavnost dokazov, pridobljenih s čezmejno izmenjavo.

20. ENVP zato spodbuja institucije EU, da ta elementa izrecno upoštevajo ne samo pri izvajanju ukrepov, predvidenih v sporočilu, temveč tudi zato, da bi čim prej začeli razmišljati o novih izboljšavah pravnega okvira varstva podatkov pri kazenskem pregonu.

V. **PROJEKTI E-PRAVOSODJA**

Orodja e-pravosodja na evropski ravni

21. ENVP priznava, da je izmenjava osebnih podatkov bistvena, če želimo ustvariti območje svobode, varnosti in pravice, zato podpira predlog strategije za e-pravosodje. Vendar hkrati poudarja, da je pri tem treba varovati podatke. Varstvo podatkov dejansko ni zgolj pravna obveznost, ampak tudi ključni element za uspeh predvidenih sistemov, npr. kakovost izmenjave podatkov. Enako velja tudi za

([8]) Še ni bil objavljen v UL.

institucije in organe, saj morajo poskrbeti za varstvo, ko obdelujejo podatke, pa tudi ko pripravljajo nove politike. Pravila in načela je treba uporabljati in upoštevati v praksi, še zlasti pri zasnovi in vzpostavljanju informacijskih sistemov. Varstvo zasebnosti in podatkov sta v bistvu „glavna dejavnika za uspeh“ cvetoče in uravnotežene informacijske družbe. Zato je smiselno, da se začne vanju vlagati čim prej.

22. ENVP v zvezi s tem poudarja, da v sporočilu ni predvidena osrednja evropska podatkovna zbirka, in je zadovoljen, da je bila prednost dana decentraliziranim strukturam. ENVP spominja, da je izdal mnenji o ECRIS ([9]) in o prümski pobudi ([10]). V mnenju o ECRIS je zapisal, da decentralizirana struktura preprečuje dodatno podvajanje osebnih podatkov v osrednji podatkovni zbirki. V mnenju o prümski pobudi pa je svetoval, da je treba med razpravo o povezovanju podatkovnih zbirk ustrezno upoštevati razsežnost sistema. Treba bi bilo uvesti predvsem specifične formate za sporočanje podatkov, na primer prošnje za izpis podatkov iz kazenske evidence, posredovane po spletu, ter pri tem upoštevati tudi jezikovne razlike. Prav tako bi bilo treba nenehno nadzirati točnost izmenjanih podatkov. Te elemente bi bilo treba upoštevati tudi pri pobudah na podlagi strategije za e-pravosodje.

23. Evropska komisija namerava prispevati k okrepitvi in razvoju orodij za e-pravosodje na evropski ravni ter pri tem tesno sodelovati z državami članicami in drugimi partnerji. Še naprej bo podpirala prizadevanja držav članic, vendar namerava tudi sama razviti vrsto računalniških orodij za boljšo interoperabilnost sistemov, lažji dostop javnosti do sodnega varstva in boljšo komunikacijo med pravosodnimi organi ter velike ekonomije obsega na evropski ravni. Kar zadeva interoperabilnost programske opreme, ki jo uporabljajo države članice, slednjim ni treba vsem uporabljati iste opreme (čeprav bi bila to najbolj praktična rešitev), vendar pa mora biti v celoti interoperabilna.

24. ENVP priporoča, da bi morali pri medsebojni povezljivosti in interoperabilnosti sistemov ustrezno upoštevati načelo omejitve namena ter za podlago uporabiti standarde varstva podatkov (zasnovano za varstvo zasebnosti – *privacy by design*). Vsako interakcijo med različnimi sistemi bi bilo treba natančno zabeležiti. Interoperabilnost ne bi smela nikoli omogočiti organu, ki ni pooblaščen za dostop ali uporabo določenih podatkov, da pridobi dostop prek drugega informacijskega sistema. ENVP znova poudarja, da interoperabilnost sama po sebi ne bi smela biti opravičilo za izogibanje načelu omejitve namena ([11]).

25. Zelo pomembno je tudi zagotoviti, da večja čezmejna izmenjava osebnih podatkov poteka pod povečanim nadzorom in ob boljšem sodelovanju med organi za varstvo podatkov. ENVP je že v mnenju z dne 29. maja 2006 o okvirnem sklepu o izmenjavi podatkov iz kazenskih evidenc ([12]) poudaril, da predlagani okvirni sklep ne bi smel obravnavati le sodelovanja med osrednjimi organi, temveč tudi sodelovanje med različnimi pristojnimi organi za varstvo podatkov. To je sedaj še pomembnejše, kajti med pogajanji o nedavno sprejetem okvirnem sklepu o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja ([13]), je bila črtana določba o vzpostavitvi delovne skupine, ki bi združevala organe EU za varstvo podatkov in usklajevala njihove dejavnosti v zvezi z obdelavo podatkov v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah. Zato bi bilo treba poskrbeti za ustrezne mehanizme učinkovitega usklajevanja med organi za varstvo podatkov, da bi zagotovili učinkovit nadzor in dobro kakovost čezmejne izmenjave podatkov iz kazenskih evidenc ([14]). Pri teh mehanizmih bi morali upoštevati tudi dejstvo, da je za nadzor nad infrastrukturo omrežja s-TESTA pristojen ENVP ([15]). Navedene mehanizme, ki bi jih lahko razvili v tesnem sodelovanju z organi za varstvo podatkov, bi lahko dopolnila orodja za e-pravosodje.

26. V točki 4.2.1 sporočila je poudarjeno, da naj izmenjava podatkov iz kazenskih evidenc ne bi potekala samo v okviru pravosodnega sodelovanja, ampak naj bi zajemala tudi druge cilje, npr. dostop do določenih zaposlitev. ENVP poudarja, da je treba pri vsakršni obdelavi osebnih podatkov v namene, ki so drugačni kot tisti, zaradi katerih so bili podatki zbrani, upoštevati specifične pogoje iz veljavne zakonodaje o varstvu podatkov. Predvsem bi

([9]) Glej opombo 4, točka 18.
([10]) UL C 89, 10.4.2008, str. 4.
([11]) UL C 91, 19.4.2006, str. 53. Glej tudi pripombe ENVP v zvezi s sporočilom Komisije o interoperabilnosti evropskih zbirk podatkov (Bruselj, 10. marec 2006).
([12]) UL C 313, 20.12.2006, str. 26.
([13]) Glej poglavje IV.
([14]) Glej mnenje ENVP o ECRIS, točke 8, 37 in 38.
([15]) S tem v zvezi glej točki 27 in 28.

smela biti nadaljnja obdelava osebnih podatkov dovoljena le zaradi uresničevanja ciljev iz zakonodaje Skupnosti o varstvu podatkov ([16]) ter pod pogojem, da je ta nadaljnja obdelava določena z zakonodajnimi ukrepi.

27. V sporočilu je v zvezi s povezovanjem kazenskih evidenc navedeno, da bo Komisija v okviru priprav na začetek veljavnosti okvirnega sklepa o izmenjavi podatkov iz kazenskih evidenc opravila dve študiji izvedljivosti ter na tej podlagi usmerjala projekt in izmenjavo podatkov razširila tudi na državljane tretjih držav, ki so bili obsojeni zaradi kaznivih dejanj. Leta 2009 bo Komisija vsem državam članicam dobavila programsko opremo, namenjeno hitri izmenjavi kazenskih evidenc. Ta referenčni sistem bo skupaj z omrežjem s-TESTA za izmenjavo podatkov omogočil vzpostavitev ekonomije obsega, saj bo državam članicam prihranjeno delo na področju razvoja, projekt pa bo tako mogoče tudi lažje upravljati.

28. ENVP zato pozdravlja uporabo omrežja s-TESTA, ki se je pri izmenjavi podatkov izkazalo za zanesljivo, ter priporoča, da se natančno določijo statistični dejavniki v zvezi s predvidenimi sistemi za izmenjavo podatkov; pri tem naj bi v ustrezni meri upoštevali tudi potrebo po zagotovitvi nadzora nad varstvom podatkov. Statistični podatki bi lahko na primer izrecno vsebovali elemente, kot je število zahtev za dostop do osebnih podatkov ali popravek teh podatkov, podatke o trajanju in celovitosti postopka posodabljanja, podatke o statusu oseb z dostopom do teh podatkov ter podatke o kršitvah varnosti. Statistični podatki in na njih temelječa poročila bi morali biti poleg tega v celoti na razpolago pristojnim organom za varstvo podatkov.

Samodejno prevajanje in podatkovna zbirka o prevajalcih

29. Samodejno prevajanje je koristen instrument in bo verjetno prispevalo k boljšemu vzajemnemu razumevanju zadevnih akterjev v državah članicah; ne bi pa smelo vplivati na kakovost izmenjanih informacij, zlasti kadar se te uporabljajo pri sprejemanju odločitev, ki imajo za zadevne osebe pravni učinek. ENVP opozarja, da je treba jasno opredeliti in omejiti uporabo samodejnega prevajanja. Če se pri posredovanju informacij, ki niso bile pravilno predhodno prevedene, uporabi samodejno prevajanje, npr. pri dodatnih komentarjih ali specifikacijah za posamezne primere, lahko to vpliva na kakovost posredovanih informacij ter posledično na odločitve, sprejete na osnovi teh informacij, in bi moralo biti zato načeloma izključeno ([17]).

([16]) Glej zlasti člen 13 direktive 95/46 in člen 20 uredbe (ES) št. 45/2001.

([17]) Glej točki 39 in 40 mnenja ENVP o ECRIS.

ENVP predlaga, naj Komisija upošteva to priporočilo pri ukrepih, sprejetih na podlagi sporočila.

30. Poročilo predstavlja poskus vzpostavitve podatkovne zbirke o sodnih prevajalcih in tolmačih, kar naj bi pripomoglo h kakovostnejšim prevodom in tolmačenju na tem področju. ENVP ta načrt odobrava, vendar opozarja, da bodo za navedeno podatkovno zbirko veljali zadevni predpisi o varstvu podatkov. Zlasti če bodo v zbirki tudi podatki o oceni uspešnosti prevajalcev, jo bodo morda morali pristojni organi za varstvo podatkov predhodno preveriti.

Za evropski akcijski načrt na področju e-pravosodja

31. V točki 5 sporočila je poudarjeno, da mora biti jasno določeno, kakšne so odgovornosti Komisije, držav članic oziroma drugih akterjev v okviru pravosodnega sodelovanja. Komisija bo v splošni vlogi koordinatorja spodbujala izmenjavo praks ter skrbela za oblikovanje, urejanje in usklajevanje informacij na portalu e-pravosodja. Poleg tega si bo še naprej prizadevala za povezljivost kazenskih evidenc in bo neposredno odgovorna za civilnopravno omrežje, hkrati pa še naprej podpirala kazenskopravnega. Države članice bodo morale posodabljati informacije o svojih pravosodnih sistemih, navedene na spletnih straneh e-pravosodja. Drugi akterji so civilnopravna in kazenskopravna omrežja ter Eurojust, ki bodo v tesnem sodelovanju s Komisijo poskrbeli za orodja, ki naj bi omogočila učinkovitejše pravosodno sodelovanje, predvsem orodja za samodejno prevajanje in varen sistem izmenjave. Sporočilu sta priložena osnutek akcijskega načrta in časovni razpored različnih projektov.

32. ENVP s tem v zvezi poudarja, da po eni strani nimamo osrednje evropske podatkovne zbirke in neposreden dostop do nacionalnih podatkovnih zbirk kazenskih evidenc drugih držav članic ni predviden, po drugi strani pa so na nacionalni ravni osrednji organi držav članic tisti, ki prevzemajo vso odgovornost. Države članice so v okviru tega mehanizma odgovorne za delovanje nacionalnih podatkovnih zbirk in za učinkovito izmenjavo. Ni pa jasno, ali so odgovorne tudi za programsko opremo za povezovanje. Komisija bo vsem državam članicam dobavila programsko opremo, namenjeno hitri izmenjavi kazenskih evidenc. Izmenjava podatkov bo istočasno potekala prek tega referenčnega sistema ter v omrežju s-TESTA.

33. Kot razume ENVP, naj bi podobne sisteme uporabljali tudi pri drugih podobnih pobudah na področju e-pravosodja, pri čemer bi bila Komisija odgovorna za skupno infrastrukturo, čeprav v sporočilu to ni izrecno navedeno.

Predlaga, da se zaradi pravne varnosti ta odgovornost pojasni v ukrepih, sprejetih na podlagi sporočila.

Projekti e-pravosodja

34. V prilogi je seznam vrste projektov, ki naj bi jih razvili v naslednjih petih letih. Prvi projekt, razvoj spletnih strani e-pravosodja, se nanaša na portal e-pravosodja. Izvesti bi bilo treba študijo izvedljivosti in oblikovati portal. Poleg tega bi bilo treba zagotoviti upravljanje in spletne informacije v vseh jezikih EU. Drugi in tretji projekt se nanašata na povezovanje kazenskih evidenc; pri projektu 2 gre za povezovanje nacionalnih kazenskih evidenc, v okviru projekta 3 pa naj bi bil vzpostavljen evropski register državljanov tretjih držav, ki so bili obsojeni zaradi kaznivih dejanj, in sicer na podlagi študije izvedljivosti in po predložitvi zakonodajnega predloga. ENVP ugotavlja, da zadnjega projekta ni več v delovnem programu Komisije, ter se sprašuje, ali je Komisija spremenila načrte glede predvidenih projektov, ali pa je bil ta specifični projekt samo preložen na poznejši čas.

35. V sporočilu so našteti tudi trije projekti na področju elektronskih izmenjav ter trije projekti v zvezi s pomočjo za prevajanje. Začel se bo pilotni projekt za postopno zbiranje gradiva za primerjalni večjezični pravni slovar. Drugi zadevni projekti se nanašajo na oblikovanje dinamičnih obrazcev, s katerimi naj bi bila opremljena evropska zakonodajna besedila, ter spodbujanje pravosodnih organov k uporabi videokonferenc. V okviru forumov e-pravosodja bodo organizirana letna srečanja o tematiki e-pravosodja in izvajalo se bo usposabljanje pravosodnih delavcev za pravosodno sodelovanje. ENVP predlaga, da bi bilo treba na takih srečanjih in v okviru navedenega usposabljanja v ustrezni meri upoštevati zakonodajo in prakso glede varstva podatkov.

36. V prilogi so torej predvidena raznovrstna evropska orodja, ki naj bi olajšala izmenjavo informacij med akterji iz različnih držav članic. Pomembno vlogo bo pri tem igral portal e-pravosodja, za katerega bo največji del odgovornosti nosila Komisija.

37. Skupni imenovalec številnih od teh orodij bo v tem, da bodo informacije in osebne podatke izmenjevali oziroma z njimi upravljali različni akterji na nacionalni ravni in na ravni EU, ki bodo morali uresničevati obveznosti v zvezi z varstvom podatkov ter ravnati v skladu z navodili nadzornih organov, ustanovljenih na podlagi direktive 95/46/ES oziroma uredbe (ES) št. 45/2001. ENPV je že v mnenju o informacijskem sistemu za notranji trg (IMI) [18] pojasnil, da je ključnega pomena učinkovito in celovito zagotoviti ravnanje v skladu s pravili o varstvu podatkov.

38. Po eni strani to pomeni, da mora biti jasno določeno, kdo je odgovoren za obdelavo osebnih podatkov v teh sistemih, po drugi pa, da se ustrezni mehanizmi usklajevanja, zlasti glede nadzora, vzpostavijo, kadarkoli je potrebno.

39. Uporaba novih tehnologij je eden izmed temeljev pobud v zvezi z e-pravosodjem: povezovanje nacionalnih registrov, razvoj elektronskega podpisa, varna omrežja, virtualne platforme za izmenjavo ter pogostejša raba videokonferenc bodo v naslednjih letih ključni elementi pobud v zvezi z e-pravosodjem.

40. Vprašanja v zvezi z varstvom podatkov je zato treba upoštevati takoj, ko je to mogoče, in jih vključiti v predvidena orodja. Zlasti pomembna sta struktura sistema in izvajanje ustreznih varnostnih ukrepov. Z vključitvijo pristopa „zasnovano za varstvo zasebnosti“ v ustrezne pobude e-pravosodja bi omogočili učinkovito upravljanje osebnih podatkov ter zagotovili usklajenost z načeli varstva podatkov in varno izmenjavo podatkov med različnimi organi.

41. ENVP poleg tega opozarja, da tehnoloških orodij ne bi smeli uporabljati le za zagotavljanje izmenjave informacij, pač pa bi morali z njimi tudi izboljšati pravice zadevnih oseb. V tem pogledu ENVP pozitivno ocenjuje sporočilo, saj je v njem navedena možnost, da bi lahko državljani zaprosili za svoje podatke iz kazenske evidence preko spleta in sicer v jeziku po lastni izbiri [19]. S tem v zvezi tudi opozarja, da je v mnenju o predlogu Komisije o izmenjavi kazenskih evidenc podprl možnost, da zadevna oseba od osrednjega organa države članice zahteva podatke o svoji kazenski evidenci, če prosilec je oziroma je bil prebivalec ali državljan zaprošene države članice ali države članice prosilke. ENVP je tudi predlagal, da bi na področju koordinacije sistemov socialne varnosti organ, ki je bliže zadevni osebi, deloval kot organ „vse na enem mestu“. Zato spodbuja Komisijo, naj si še naprej prizadeva

[18] UL C 270, 25.10.2008, str. 1.
[19] Glej str. 6 sporočila.

za razvoj tehnoloških orodij ter predvsem za spletni dostop, kar bi državljanom omogočilo boljši pregled nad njihovimi osebnimi podatki, tudi kadar zamenjajo več držav članic.

VI. **SKLEPI**

42. ENVP podpira sedanji predlog za vzpostavitev e-pravosodja in priporoča, da se upoštevajo naslednje pripombe iz tega mnenja:

— nedavno sprejeti okvirni sklep o varstvu osebnih podatkov na področju policijskega in pravosodnega sodelovanja v kazenskih zadevah bi bilo treba skupaj z njegovimi pomanjkljivostmi upoštevati ne le pri izvajanju ukrepov, predvidenih v sporočilu, temveč tudi zato, da bi čimprej začeli razmišljati o novih izboljšavah pravnega okvira varstva podatkov pri kazenskem pregonu;

— upravni postopki v zvezi z e-pravosodjem. Začeti bi bilo treba projekte e-pravosodja, ki so del te nove sestavine, ter z njimi zagotoviti opaznejšo vlogo pravil o varstvu podatkov ter nacionalnih organov za varstvo podatkov, zlasti pri vrstah podatkov, ki se obdelujejo v okviru projektov e-pravosodja;

— prednost bi bilo treba dati decentralizirani strukturi;

— pri medsebojni povezljivosti in interoperabilnosti sistemov bi bilo treba ustrezno upoštevati načelo omejitve namena;

— jasno bi bilo treba določiti odgovornosti vseh akterjev, ki bodo sodelovali pri obdelavi osebnih podatkov v predvidenih sistemih, ter vzpostaviti mehanizme za učinkovito medsebojno usklajevanje organov za varstvo podatkov;

— pri obdelavi osebnih podatkov v druge namene, kot so tisti, za katere so bili zbrani, bi bilo treba zagotoviti izpolnjevanje specifičnih pogojev iz veljavne zakonodaje o varstvu podatkov;

— jasno bi bilo treba opredeliti in omejiti samodejno prevajanje ter s tem zagotoviti vzajemno poznavanje kaznivih dejanj brez poseganja v kakovost posredovanih informacij;

— pojasniti bi bilo treba, kakšna je odgovornost Komisije za skupne sisteme, kot je omrežje s-TESTA;

— kar zadeva uporabo novih tehnologij, bi bilo treba zagotoviti, da se vprašanja v zvezi z varstvom podatkov upoštevajo takoj, ko je to mogoče, ter si prizadevati za razvoj tehnoloških orodij, ki bi državljanom omogočila boljši pregled nad njihovimi osebnimi podatki, tudi kadar zamenjajo več držav članic.

V Bruslju, 19. decembra 2008

Peter HUSTINX

Evropski nadzornik za varstvo podatkov

Osnutek mnenja Evropskega nadzornika za varstvo podatkov o predlogu direktive Evropskega parlamenta in Sveta o uveljavljanju pravic pacientov na področju čezmejnega zdravstvenega varstva

(2009/C 128/03)

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV JE –

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

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

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

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 teh podatkov ter zlasti člena 41 Uredbe,

ob upoštevanju prošnje za mnenje v skladu s členom 28(2) Uredbe (ES) št. 45/2001, ki je bila ENVP poslana 2. julija 2008 –

SPREJEL NASLEDNJE MNENJE:

I. UVOD

Predlog direktive o uveljavljanju pravic pacientov na področju čezmejnega zdravstvenega varstva

1. Komisija je 2. julija 2008 sprejela predlog direktive Evropskega parlamenta in Sveta o uveljavljanju pravic pacientov na področju čezmejnega zdravstvenega varstva (v nadaljnjem besedilu: predlog) [1]. Komisija je predlog poslala ENVP, da bi se z njim posvetovala v skladu s členom 28(2) Uredbe (ES) št. 45/2001.

2. Namen predloga je vzpostaviti okvir Skupnosti za zagotavljanje čezmejnega zdravstvenega varstva znotraj EU v tistih primerih, v katerih se oskrba, ki jo pacienti iščejo, izvaja v drugi državi članici in ne v njihovi matični državi. Ta je oblikovan okrog treh področij:

— vzpostavitve skupnih načel v vseh zdravstvenih sistemih EU z jasno opredelitvijo pristojnosti držav članic;

— razvoja posebnega okvira za čezmejno zdravstveno varstvo, ki zagotavlja jasnost glede pravic pacientov do zdravstvenega varstva v drugi državi članici;

— spodbujanja sodelovanja EU na področju zdravstvenega varstva na področjih, kot so priznavanje zdravniških receptov, izdanih v drugih državah, evropske referenčne mreže, ocenjevanje zdravstvene tehnologije, zbiranje podatkov ter kakovost in varnost.

3. Cilji tega okvirnega sklepa so dvojni: zagotoviti dovolj jasnosti o pravicah do povračila stroškov za zdravstveno varstvo v drugi državi članici in zagotoviti, da so pri čezmejni oskrbi izpolnjene potrebne zahteve za visokokakovostno, varno in učinkovito zdravstveno varstvo.

4. Izvajanje čezmejnega sistema zdravstvenega varstva zahteva izmenjavo ustreznih osebnih podatkov, povezanih z zdravjem (v nadaljnjem besedilu: zdravstveni podatki) pacientov, med pooblaščenimi organizacijami in zdravstvenimi delavci različnih držav članic. Ti podatki so občutljivi in zanje veljajo strožja pravila o varstvu podatkov, kakor so določena v členu 8 Direktive 95/46/ES o posebnih vrstah podatkov.

Posvetovanje z ENVP

5. ENVP pozdravlja posvetovanje glede tega vprašanja in dejstvo, da je to posvetovanje navedeno v preambuli predloga v skladu s členom 28 Uredbe (ES) št. 45/2001.

6. Prvič se je zgodilo, da poteka formalno posvetovanje z ENVP o predlogu direktive na področju zdravstvenega varstva. Zato so v tem mnenju nekatere opombe širšega obsega in se nanašajo na splošna vprašanja varstva osebnih podatkov v sektorju zdravstvenega varstva, ki bi se lahko upoštevala pri drugih ustreznih pravnih instrumentih (zavezujočih ali nezavezujočih).

[1] COM(2008) 414 konč. Upoštevajte, da je bilo istega dne sprejeto dopolnilno sporočilo o okviru Skupnosti o uveljavljanju pravic pacientov na področju čezmejnega zdravstvenega varstva (COM(2008) 415 konč.). Ker pa je sporočilo precej splošne narave, se je ENVP odločil osredotočiti na predlagano direktivo.

7. ENVP želi že na začetku izraziti podporo pobudam za izboljšanje pogojev za čezmejno zdravstveno varstvo. Ta predlog je treba dejansko razumeti v okviru splošnega programa ES za izboljšanje zdravja državljanov v informacijski družbi. Druge pobude v zvezi s tem so predvidena direktiva in sporočilo Komisije o darovanju in presaditvi človeških organov [1], priporočilo o medobratovalnosti elektronskih zdravstvenih zapisov [2] in predvideno sporočilo o telemedicini [3]. ENVP pa je zaskrbljen zaradi dejstva, da vse te sorodne pobude niso tesno povezane in/ali medsebojno povezane na področju zasebnosti in varnosti podatkov, saj je tako težje sprejeti enoten pristop do varstva podatkov v zdravstvenem varstvu, zlasti kar zadeva uporabo novih tehnologij IKT. V sedanjem predlogu na primer ni navedenega sklica na ustrezno razsežnost o varstvu podatkov iz sporočila EK, čeprav je telemedicina izrecno omenjena v uvodni izjavi 10 predlagane direktive. Poleg tega ni zagotovljene povezave z vprašanji zasebnosti, ki so obravnavana v ustreznem priporočilu Komisije, čeprav so elektronski zdravstveni zapisi možen način čezmejnega sporočanja zdravstvenih podatkov [4]. To daje vtis, da splošna perspektiva zasebnosti v zdravstvenem varstvu še vedno ni jasno opredeljena, v nekaterih primerih pa je sploh ni.

8. To je očitno tudi v sedanjem predlogu, za katerega ENVP obžaluje, da posledic varstva podatkov ne obravnava konkretno. Seveda je mogoče najti sklicevanja na varstvo podatkov, a so večinoma zelo splošni in ne odražajo ustrezno specifičnih potreb glede zasebnosti in zahtev čezmejnega zdravstvenega varstva.

9. ENVP želi poudariti, da enoten in trden pristop do varstva podatkov v vseh predlaganih instrumentih o zdravstvenem varstvu ne bo le zagotovil temeljnih pravic državljanov do varstva njihovih podatkov, ampak bo prispeval tudi k nadaljnjemu razvoju čezmejnega zdravstvenega varstva v EU.

II. VARSTVO PODATKOV V ČEZMEJNEM ZDRAVSTVENEM VARSTVU

Splošno ozadje

10. Najpomembnejši cilj Evropske skupnosti je vzpostaviti notranji trg, območje brez notranjih meja, v katerem je zagotovljen prosti pretok blaga, oseb, storitev in kapitala. Omogočanje, da se državljani lažje gibajo in prebivajo v drugih državah članicah, iz katerih ne prihajajo, ima seveda za posledico vprašanja, povezana z zdravstvenim varstvom. Zato se je Sodišče v devetdesetih letih v okviru notranjega trga soočalo z vprašanji o možnem povračilu zdravstvenih izdatkov, ki so nastali v drugi državi članici. Sodišče je priznalo, da svoboda opravljanja storitev, kakor je določena v členu 49 Pogodbe ES, vključuje svobodo oseb, da gredo na zdravljenje v drugo državo članico [5]. Zato pacientov, ki so želeli izkoristiti čezmejno zdravstveno varstvo, ni bilo več mogoče obravnavati drugače od državljanov njihove države izvora, ki so prejeli isto zdravljenje in pri tem niso prestopili meje.

11. Te sodbe Sodišča so bistvo sedanjega predloga. Ker sodna praksa Sodišča temelji na posameznih zadevah, je namen sedanjega predloga izboljšati jasnost, da bi zagotovili splošnejše in učinkovitejše uveljavljanje svobode prejemanja in opravljanja zdravstvenih storitev. Vendar pa je, kakor je že bilo omenjeno, predlog tudi del bolj velikopoteznega programa z namenom izboljšanja zdravja državljanov v informacijski družbi, kjer EU vidi velike možnosti za izboljšanje čezmejnega zdravstvenega varstva z uporabo informacijske tehnologije.

12. Zaradi jasnih razlogov je določanje pravil za čezmejno zdravstveno varstvo občutljivo vprašanje. Dotika se občutljivega področja, na katerem so države članice vzpostavile različne nacionalne sisteme, na primer glede zavarovanja in povračila stroškov ali organizacije infrastrukture zdravstvenega varstva, vključno z omrežji in aplikacijami za podatke o zdravstvenem varstvu. Čeprav je zakonodaja Skupnosti v sedanjem predlogu osredotočena na *čezmejno* zdravstveno varstvo, bodo pravila vsaj vplivala na način organizacije nacionalnih sistemov zdravstvenega varstva.

13. Izboljšanje pogojev za čezmejno zdravstveno varstvo bo koristilo državljanom. Hkrati pa bo vsebovalo tudi določena tveganja za državljane. Rešiti bo treba precej praktičnih težav, ki so značilne za čezmejno sodelovanje med ljudmi iz različnih držav, ki govorijo različne jezike. Ker je dobro zdravje odločilnega pomena za vsakega državljana, je treba izključiti vsakršno tveganje napačne komunikacije in posledične zmote. Ni treba poudariti, da krepitev čezmejnega zdravstvenega varstva v kombinaciji z uporabo

[1] Napovedana v delovnem programu Komisije.

[2] Priporočilo Komisije z dne 2. julija 2008 o čezmejni medobratovalnosti sistemov za vodenje elektronskih zdravstvenih zapisov (notificirano pod dokumentarno številko C(2008) 3282), UL L 190, 18.7.2008, str. 37.

[3] Napovedano v delovnem programu Komisije.

[4] V zvezi s tem veliko pove dejstvo, da v sporočilu iz opombe 1 ni sklica na zasebnost ali varstvo podatkov, namen tega sporočila pa je vzpostaviti okvir Skupnosti za uveljavljanje pravic pacientov v čezmejnem zdravstvenem varstvu.

[5] Glej zadevo 158/96, *Kohll*, (1998) ZOdl. I-1931, odst. 34. Med drugim glej tudi zadevo C-157/99, *Smits and Peerbooms* (2001) ZOdl. I-5773 in zadevo C-385/99, *Müller-Fauré and Van Riet* (2003) ZOdl. I-12403.

novosti informacijske tehnologije v veliki meri vpliva na varstvo osebnih podatkov. Zaradi učinkovitejše in zato vse večje izmenjave zdravstvenih podatkov, vse večjih razdalj med zadevnimi ljudmi in primeri ter različnih nacionalnih zakonov o izvajanju pravil o varstvu podatkov se postavljajo vprašanja o varnosti podatkov in pravni varnosti.

Varstvo zdravstvenih podatkov

14. Poudariti je treba, da so zdravstveni podatki posebna kategorija podatkov, ki zasluži višjo stopnjo varstva. Kakor je nedavno navedlo Evropsko sodišče za človekove pravice v okviru člena 8 Evropske konvencije o varstvu človekovih pravic: „Varstvo osebnih podatkov, zlasti medicinskih, je temeljnega pomena za uveljavitev pravice določene osebe do spoštovanja njene zasebnosti in družinskega življenja, kar zagotavlja člen 8 Konvencije“ ([1]). Pred pojasnitvijo strožjih pravil za obdelavo zdravstvenih podatkov, ki so določena v Direktivi 95/46/ES, je treba nekaj besed najprej nameniti izrazu „zdravstveni podatki“.

15. Direktiva 95/46/ES ne vsebuje izrecne opredelitve zdravstvenih podatkov. Običajno se uporablja široka razlaga, ki pogosto opredeljuje zdravstvene podatke kot „osebne podatke, ki so jasno in tesno povezani z opisom zdravstvenega stanja osebe“ ([2]). V tem smislu zdravstveni podatki običajno zajemajo medicinske podatke (npr. zdravniške napotnice in recepti, poročila medicinskih pregledov, laboratorijski testi, rentgenske slike itd.), pa tudi administrativne in finančne podatke, ki se nanašajo na zdravje (npr. dokumenti o sprejemu v bolnišnico, številka socialnega zavarovanja, urniki zdravniških obiskov, računi za opravljanje storitev zdravstvenega varstva itd.). Opozoriti je treba, da se včasih za navedbo podatkov, povezanih z zdravjem, poleg izraza „zdravstveni podatki“ ([3]) uporablja tudi izraz „medicinski podatki“ ([4]). V tem mnenju se uporablja izraz „zdravstveni podatki“.

16. Uporabna opredelitev pojma „zdravstveni podatki“ je v standardu ISO 27799: „vse informacije, ki se nanašajo na fizično ali psihično zdravje posameznika ali opravljanje zdravstvenih storitev za posameznika in ki lahko zajemajo: (a) informacije o registraciji posameznika za opravljanje zdravstvenih storitev; (b) informacije o plačilih ali upravičenosti do zdravstvenega varstva posameznika; (c) število, znak ali posebnost, dodeljeno posamezniku za njegovo edinstveno identifikacijo v zdravstvene namene; (d) vse informacije o posamezniku, zbrane v času izvajanja zdravstvenih storitev za posameznika; (e) informacije, pridobljene iz testiranja ali preiskav dela telesa ali telesnih snovi, ter (f) identifikacijo osebe (zdravstvenega delavca) kot izvajalca storitev zdravstvenega varstva za posameznika“.

17. ENVP se močno zavzema za sprejetje posebne opredelitve izraza „zdravstveni podatki“ v okviru sedanjega predloga, ki bi se v prihodnosti lahko uporabljala tudi v drugih ustreznih zakonodajnih besedilih ES (glej oddelek III spodaj).

18. Člen 8 Direktive 95/46/ES določa pravila za obdelavo posebnih vrst podatkov. Ta pravila so strožja od tistih za obdelavo drugih podatkov iz člena 7 Direktive 95/46/ES. To je vidno že v členu 8(1), ki izrecno navaja, da države članice med drugim prepovejo obdelavo podatkov v zvezi z zdravjem. V naslednjih odstavkih tega člena je navedenih več izjem iz te prepovedi, a so ožje kot podlaga za obdelavo običajnih podatkov iz člena 7. Prepoved se na primer ne uporablja, če je posameznik, na katerega se podatki nanašajo, dal svojo *izrecno* privolitev (člen 8(2)(a)), v nasprotju z *nedvoumno* privolitvijo iz člena 7(a) Direktive 95/46/ES. Poleg tega lahko zakon države članice določa, da v nekaterih primerih tudi privolitev posameznika, na katerega se podatki nanašajo, ne more odpraviti prepovedi. Tretji odstavek člena 8 je namenjen izključno obdelavi podatkov v zvezi z zdravjem. V skladu s tem odstavkom se prepoved iz prvega odstavka ne uporablja, kadar se podatki obdelujejo za potrebe preventivne medicine, zdravstvene diagnoze, za zagotovitev oskrbe, ali zdravljenja, ali vodenje zdravstvenih služb in kadar te podatke obdeluje zdravstveni delavec na podlagi nacionalne zakonodaje ali pravil, ki jih sprejmejo pristojni nacionalni organi glede dolžnosti poklicne molčečnosti, ali druga oseba, ki je prav tako zavezana enaki dolžnosti molčečnosti.

19. Člen 8 Direktive 95/46/ES zelo poudarja dejstvo, da morajo države članice zagotoviti ustrezne ali primerne zaščitne ukrepe. Člen 8(4) na primer državam članicam dovoljuje, da določijo dodatne izjeme od prepovedi za obdelavo občutljivih podatkov zaradi javnega interesa bistvenega pomena, vendar ob zagotovitvi ustreznih zaščitnih ukrepov. To na splošno poudarja odgovornost držav članic, da posebno pozornost namenijo obdelavi občutljivih podatkov, kot so podatki v zvezi z zdravjem.

Varstvo zdravstvenih podatkov v čezmejnih primerih

Deljene pristojnosti med državami članicami

20. Države članice se morajo še posebej zavedati pravkar omenjene pristojnosti, kar zadeva vprašanje čezmejne izmenjave podatkov. Kakor je navedeno zgoraj, čezmejna izmenjava zdravstvenih podatkov povečuje tveganje za netočno ali nelegalno obdelavo podatkov. Seveda ima to lahko velike negativne posledice za posameznika, na katerega se podatki nanašajo. V ta postopek sta vključeni tako država članica zdravstvenega zavarovanja (kjer

([1]) Glej EKČP, 17. julij 2008, *I proti Finski* (vloga št. 20511/03), odstavek 38.

([2]) Glej delovni dokument Delovne skupine iz člena 29 o obdelavi osebnih podatkov, povezanih z zdravjem, v elektronskih zdravstvenih zapisih, februar 2007, WP 131, odstavek II.2. Glej tudi širok pomen „osebnih podatkov“: Delovna skupina iz člena 29, mnenje 4/2007 o pojmu osebnih podatkov, WP 136.

([3]) Standard ISO 27799:2008 „ Zdravstvena informatika – Upravljanje informacijske varnosti v zdravstvu z uporabo standarda ISO/IEC 27002“.

([4]) Svet Evrope, priporočilo št. R(97)5 o varstvu medicinskih podatkov.

je pacient zavarovana oseba) kot tudi država članica zdravljenja (kjer se zdravstveno varstvo dejansko izvaja) in zato delita to pristojnost.

21. Varnost zdravstvenih podatkov je v tem smislu pomembno vprašanje. V nedavnem zgoraj navedenem primeru je Evropsko sodišče za človekove pravice velik pomen pripisalo zaupnosti zdravstvenih podatkov: „Spoštovanje zaupnosti zdravstvenih podatkov je ključno načelo v pravnih sistemih vseh držav pogodbenic Konvencije. Zato je bistveno, da se ne le spoštuje pomen zasebnosti pacienta, ampak tudi ohrani njegovo ali njeno zaupanje v medicinski poklic in zdravstvene službe na splošno". ([1])

22. Pravila o varstvu podatkov iz Direktive 95/46/ES nadalje zahtevajo, da mora država članica zdravstvenega zavarovanja pacientu zagotoviti ustrezne, pravilne in najnovejše informacije o pošiljanju njegovih osebnih podatkov v drugo državo članico in hkrati zagotoviti zanesljiv prenos podatkov v to državo članico. Država članica zdravljenja mora zagotoviti tudi zanesljiv sprejem teh podatkov in ustrezno stopnjo varnosti, kadar se podatki res obdelujejo, v skladu s svojo nacionalno zakonodajo o varstvu podatkov.

23. ENVP želi, da bi bile deljene pristojnosti držav članic v predlogu jasne, ob tem pa je treba upoštevati tudi elektronsko sporočanje podatkov, zlasti v okviru novih aplikacij IKT, kakor je navedeno v nadaljevanju.

Elektronsko sporočanje zdravstvenih podatkov

24. Izboljšanje čezmejne izmenjave zdravstvenih podatkov običajno poteka z uporabo informacijske tehnologije. Čeprav bi se izmenjava podatkov v čezmejnem sistemu zdravstvenega varstva lahko še vedno izvedla v papirni obliki (npr. pacient se preseli v drugo državo članico in s seboj prinese vse svoje pomembne zdravstvene podatke, kot so laboratorijske preiskave, zdravniške napotnice itd.), je namesto tega jasno viden namen uporabe elektronskih sredstev. Elektronsko sporočanje zdravstvenih podatkov bodo podpirali informacijski sistemi zdravstvenega varstva, ki so že ali še bodo vzpostavljeni v državah članicah (v bolnišnicah, na klinikah itd.), pa tudi uporaba novih tehnologij, kot so aplikacije za elektronske zdravstvene zapise (ki bodo verjetno delovale prek spleta), in druga orodja, kot so zdravstvene kartice pacientov in zdravnikov. Seveda je možna tudi kombinirana uporaba izmenjave v papirnati in elektronski obliki, odvisno od sistemov zdravstvenega varstva držav članic.

25. Aplikaciji e-zdravje in telemedicina, ki bosta spadali v področje uporabe predlagane direktive, bosta izključno odvisni od izmenjave elektronskih zdravstvenih podatkov (npr. življenjski znaki, podobe itd.), običajno skupaj z drugimi obstoječimi elektronskimi informacijski sistemi zdravstvenega varstva v državi članici zdravljenja in zdravstvenega zavarovanja. To zajema sisteme, ki delujejo tako na podlagi odnosa pacient-zdravnik (npr. spremljanje in diagnostika na daljavo), kot tudi na podlagi odnosa zdravnik-zdravnik (npr. teleposvetovanje med zdravstvenimi delavci za strokovne nasvete glede posameznih primerov zdravstvenega varstva). Druge bolj specifične aplikacije zdravstvenega varstva, ki podpirajo splošno čezmejno izvajanje zdravstvenega varstva, bi lahko bile odvisne tudi izključno od elektronske izmenjave podatkov, npr. elektronski zdravniški recept (e-recept) ali elektronska napotnica (e-napotnica), kar se v nekaterih državah članicah že izvaja na nacionalni ravni ([2]).

Zaskrbljujoča področja pri čezmejni izmenjavi zdravstvenih podatkov

26. Ob upoštevanju navedenih pomislekov skupaj z obstoječimi razlikami med zdravstvenimi sistemi držav članic in vse hitrejšega razvoja aplikacij e-zdravja, se glede varstva osebnih podatkov v čezmejnem zdravstvenem varstvu pojavljata dve glavni zaskrbljujoči področji: (a) različne stopnje varnosti, ki jih države članice lahko uporabljajo za varstvo osebnih podatkov (v smislu tehničnih in organizacijskih ukrepov), in (b) vključitev zasebnosti v aplikacije e-zdravja, zlasti pri novostih. Poleg tega bi bilo morda posebno pozornost treba nameniti drugim vidikom, kot je sekundarna uporaba zdravstvenih podatkov, zlasti na področju pridobivanja statističnih podatkov. Ta vprašanja so nadalje preučena v preostanku tega oddelka.

Varnost podatkov v državah članicah

27. Kljub dejstvu, da se direktivi 95/46/ES in 2002/58/ES enako uporabljata v Evropi, se razlaga in izvajanje določenih delov lahko razlikuje med državami članicami, zlasti na področjih, kjer so pravne določbe na splošno prepuščene državam članicam. V tem smislu je glavno področje, ki se mora obravnavati, varnost obdelave, tj. ukrepi (tehnični in organizacijski), ki jih države članice sprejmejo za zagotovitev varnosti zdravstvenih podatkov.

([1]) EKČP, 17. julij 2008, *I proti Finski* (vloga št. 20511/03), odstavek 38.

([2]) Poročilo e-zdravje v evropskem raziskovalnem prostoru, na poti k vzpostavitvi evropskega raziskovalnega prostora za e-zdravje (*Towards the Establishment of a European eHealth Research Area*), Evropska komisija, informacijska družba in mediji, marec 2007, http://ec.europa.eu/information_society/activities/health/docs/policy/ehealth-era-full-report.pdf

28. Čeprav je strogo varstvo zdravstvenih podatkov pristojnost vseh držav članic, trenutno ni splošno sprejete opredelitve „ustrezne“ stopnje varnosti za zdravstveno varstvo v EU, ki bi se lahko uporabljala v primeru čezmejnega zdravstvenega varstva. Tako lahko na primer bolnišnico v eni državi članici obvezujejo predpisi o varstvu, uvedeni na nacionalni ravni, da sprejme posebne varnostne ukrepe (kot npr. opredelitev politike varstva in kodeksov ravnanja, posebna pravila za zunanje izvajalce in uporabo zunanjih pogodbenih partnerjev, revizijske zahteve itd.), medtem ko tega v drugi državi članici ni. Ta nedoslednost bi lahko vplivala na čezmejno izmenjavo podatkov, zlasti kadar je ta v elektronski obliki, saj ni mogoče zagotoviti, da so podatki zaščiteni (s tehničnega in organizacijskega vidika) na enaki stopnji med različnimi državami članicami.

29. Zato je na tem področju potrebna nadaljnja uskladitev v smislu opredelitve skupnega svežnja varnostnih zahtev za zdravstveno varstvo, ki ga morajo na splošno sprejeti izvajalci storitev zdravstvenega varstva držav članic. Ta potreba je zagotovo skladna s splošno potrebo po opredelitvi skupnih načel v zdravstvenih sistemih EU, kakor je navedeno v predlogu.

30. To je treba urediti na splošen način, brez uvedbe posebnih tehničnih rešitev za države članice, a vendar z določitvijo podlage za vzajemno priznavanje in sprejemanje npr. na področjih opredelitve politike varstva, identifikacije in avtentifikacije pacientov ter zdravstvenih delavcev itd. Kot načrt pri takem poskusu bi se lahko uporabili obstoječi evropski in mednarodni standardi (npr. ISO in CEN) glede zdravstvenega varstva in varnosti, pa tudi široko sprejeti in pravno utemeljeni tehnični pojmi (npr. elektronski podpisi) ([1]).

31. ENVP podpira zamisel uskladitve varnosti v zdravstvenem varstvu na ravni EU in meni, da mora Komisija pripraviti ustrezne spodbude že v okviru sedanjega predloga (glej oddelek III spodaj).

Zasebnost v aplikacijah e-zdravja

32. Zasebnost in varnost morata biti vključeni v oblikovanje in izvajanje katerega koli sistema zdravstvenega varstva, zlasti aplikacij e-zdravja, kakor je omenjeno v tem predlogu („zasebnost pri oblikovanju“). Ta nesporna zahteva je že dobila podporo v drugih ustreznih političnih dokumentih ([2]), tako splošnih kot tistih, ki se nanašajo na zdravstveno varstvo ([3]).

33. V okviru medobratovalnosti e-zdravja, opisanega v predlogu, je treba še enkrat poudariti pojem „zasebnost pri oblikovanju“ kot podlago za vse predvidene novosti. Ta pojem se nanaša na več različnih ravni: organizacijsko, semantično in tehnično.

— Na organizacijski ravni je treba zasebnost upoštevati v opredelitvi potrebnih postopkov za izmenjavo zdravstvenih podatkov med organizacijami zdravstvenega varstva držav članic. To lahko neposredno vpliva na vrsto izmenjave in obseg prenosa podatkov (npr. uporaba identifikacijskih številk namesto pravih imen pacientov, če je to mogoče).

— Na semantični ravni je treba zahteve glede zasebnosti in varnosti vključiti v nove standarde in sisteme, npr. v opredelitev predloge za elektronske zdravniške recepte, saj je to obravnavano v predlogu. Tako bi se lahko nadgradili tehnični standardi na tem področju, npr. standardi o zaupnosti podatkov in digitalnem podpisu, in obravnavale potrebe, značilne za zdravstveno varstvo, kot je avtentifikacija usposobljenih zdravstvenih delavcev glede na njihovo vlogo.

— Na tehnični ravni morajo strukture sistemov in aplikacije za uporabnike prilagoditi tehnologije za varovanje zasebnosti ob izvajanju omenjene semantične opredelitve.

34. ENVP meni, da bi področje elektronskih zdravniških receptov lahko služilo kot začetna točka za vključitev zahtev glede zasebnosti in varnosti že v začetni fazi razvoja (glej oddelek III spodaj).

Drugi vidiki

35. Dodatni vidik, ki bi se lahko preučil v okviru čezmejne izmenjave zdravstvenih podatkov, je sekundarna uporaba zdravstvenih podatkov, zlasti uporaba podatkov za statistične namene, kakor je že določeno v sedanjem predlogu.

36. Kakor je že bilo omenjeno v točki 18, člen 8(4) Direktive 95/46 predvideva možnost sekundarne uporabe zdravstvenih podatkov. Vendar se ta nadaljnja obdelava lahko opravi le zaradi „javnega interesa bistvenega pomena“ in morajo zanjo veljati „ustrezni zaščitni ukrepi“, določeni v nacionalni zakonodaji, ali pa se opravi na podlagi odločitve nadzornega organa ([4]). Poleg tega se v primeru obdelave statističnih podatkov, kakor je tudi omenjeno v mnenju ENVP o predlagani uredbi o statističnih podatkih Skupnosti

([1]) Direktiva 1999/93/ES Evropskega parlamenta in Sveta z dne 13. decembra 1999 o okviru Skupnosti za elektronski podpis (UL L 13, 19.1.2000, str. 12–20).

([2]) Raziskave in tehnološki razvoj ENVP in EU, strateški dokument, ENPV, april 2008, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/08-04-28_PP_RTD_EN.pdf

([3]) Priporočilo Komisije z dne 2. julija 2008 o čezmejni medobratovalnosti sistemov za vodenje elektronskih zdravstvenih zapisov (notificirano pod dokumentarno številko C(2008) 3282), UL L 190, 18.7.2008, str. 37.

([4]) Glej tudi uvodno izjavo 34 Direktive 95/46/ES. Glede te točke glej tudi mnenje Delovne skupine iz člena 29 o elektronskih zdravstvenih zapisih, omenjeno v opombi 8 na str. 16.

v zvezi z javnim zdravjem ter zdravjem in varnostjo pri delu ([1]), pojavlja dodatno tveganje zaradi različnih pomenov, ki jih lahko imata pojma „zaupnost“ in „varstvo podatkov“ pri uporabi zakonodaje o varstvu podatkov na eni strani in zakonodaje o statistiki na drugi.

37. ENVP želi poudariti zgornje elemente v okviru sedanjega predloga. Vključiti je treba bolj izrecne sklice na zahteve glede varstva podatkov, kar zadeva nadaljnjo uporabo zdravstvenih podatkov (glej oddelek III spodaj).

III. **NATANČNA ANALIZA PREDLOGA**

Določbe predloga o varstvu podatkov

38. Predlog vključuje številne sklice na varstvo podatkov in zasebnost v različnih delih dokumenta; natančneje:

— uvodna izjava (3) med drugim navaja, da je treba direktivo izvajati in uporabljati ob ustreznem upoštevanju pravic do zasebnega življenja in varstva osebnih podatkov;

— uvodna izjava (11) govori o temeljni pravici do zasebnosti, kar zadeva obdelavo osebnih podatkov, in zaupnosti, kot dveh operativnih načelih, ki sta skupni zdravstvenim sistemom v Skupnosti;

— uvodna izjava (17) opisuje pravico do varstva osebnih podatkov kot temeljno pravico posameznikov, ki bi jo bilo treba zaščititi, pri tem pa se v prvi vrsti osredotočiti na pravico posameznika do dostopa do zdravstvenih podatkov (tudi v okviru čezmejnega zdravstvenega varstva), kakor je določeno v Direktivi 95/46/ES,

— člen 3, ki določa razmerje med direktivo in drugimi določbami Skupnosti, se v odstavku 1 sklicuje na direktivi 95/46/ES in 2002/58/ES;

— člen 5 o pristojnostih države članice zdravljenja v odstavku 1(f) kot eno od teh pristojnosti določa zaščito pravice do zasebnosti v skladu z nacionalnimi ukrepi o izvajanju direktiv 95/46/ES in 2002/58/ES;

— člen 6 o zdravstvenem varstvu v drugi državi članici v odstavku 5 poudarja pravico do dostopa pacientov do svojih zdravstvenih kartotek, če potujejo v drugo državo članico z namenom prejemanja zdravstvenega varstva ali poiskati zdravstveno varstvo, zagotovljeno v drugi državi članici, zopet v skladu z nacionalnimi ukrepi o izvajanju direktiv 95/46/ES in 2002/58/ES;

— člen 12 o nacionalnih kontaktnih službah za čezmejno zdravstveno varstvo v odstavku 2(a) navaja, da morajo biti te kontaktne službe med drugim odgovorne za zagotavljanje in posredovanje informacij pacientom o jamstvih glede varstva osebnih podatkov v drugi državi članici;

— člen 16 o e-zdravju določa, da morajo ukrepi za doseganje medobratovalnosti sistemov informacijske in komunikacijske tehnologije upoštevati temeljno pravico do varstva osebnih podatkov v skladu z zakonodajo, ki se uporablja;

— nazadnje je v členu 18(1) med drugim omenjeno, da mora biti zbiranje podatkov za namene statistike in spremljanja opravljeno v skladu z nacionalno zakonodajo in zakonodajo Skupnosti o varstvu osebnih podatkov.

39. ENVP pozdravlja dejstvo, da je bilo varstvo podatkov upoštevano pri oblikovanju besedila predloga in da se poskuša prikazati splošna potreba po zasebnosti v okviru čezmejnega zdravstvenega varstva. Vendar pa so obstoječe določbe predloga o varstvu podatkov bodisi preveč splošne ali pa se nanašajo na pristojnosti držav članic precej selektivno in nedosledno:

— zlasti uvodni izjavi (3) in (11) skupaj s členom 3(1)(a), členom 16 in členom 18(1) dejansko obravnavajo splošni pravni okvir za varstvo podatkov (zadnja dva v okviru e-zdravja in zbiranja statističnih podatkov, a brez določanja posebnih zahtev glede zasebnosti);

— kar zadeva pristojnosti držav članic, je omenjen splošni sklic v členu 5(1)(f);

— uvodna izjava (17) in člen 6(5) določata natančnejše sklice na pravico pacientov do dostopa v državi članici zdravljenja;

— nazadnje člen 12(2)(a) vsebuje določbo o pravici pacientov do informacij v državi članici zdravstvenega zavarovanja (prek delovanja nacionalnih kontaktnih služb).

Poleg tega, kakor je že bilo omenjeno v uvodnem delu tega mnenja, ni povezave in/ali sklica na vidike zasebnosti iz drugih pravnih instrumentov ES (zavezujočih ali ne) na področju zdravstvenega varstva, zlasti kar zadeva uporabo novih aplikacij IKT (kot so telemedicina ali elektronski zdravstveni zapisi).

([1]) UL C 295, 7.12.2007, str. 1.

40. Čeprav je zasebnost običajno navedena kot zahteva pri čezmejnem zdravstvenem varstvu, na ta način še vedno nimamo splošne podobe, tako v smislu obveznosti držav članic kot tudi v smislu podrobnosti, uvedenih s čezmejno naravo opravljanja storitev zdravstvenega varstva (v nasprotju z opravljanjem storitev nacionalnega zdravstvenega varstva). Natančneje:

— pristojnosti držav članic niso prikazane celovito, saj so nekatere obveznosti (pravica do dostopa in informacij) poudarjene – vendar v različnih delih predloga – medtem ko so druge popolnoma izpuščene, kot je varnost obdelave;

— pomisleki glede nedoslednosti držav članic pri varnostnih ukrepih in potrebe po uskladitvi varnosti zdravstvenih podatkov na evropski ravni v okviru čezmejnega zdravstvenega varstva niso niti omenjeni;

— vključitev zasebnosti v aplikacije e-zdravja ni omenjena; tudi v primeru e-recepta to ni ustrezno izraženo.

41. Poleg tega se pomisleki pojavljajo glede člena 18, ki obravnava zbiranje podatkov za namene statistike in spremljanja. Prvi odstavek se nanaša na „statistične *in druge dodatne podatke*“, nato pa v množini govori o „namenih spremljanja“ in navaja področja, ki spadajo v te namene spremljanja, tj. izvajanje čezmejnega zdravstvenega varstva, zagotovljena oskrba, izvajalci in pacienti, stroški in rezultati. V tem že precej nejasnem okviru je naveden sklic na zakonodajo o varstvu podatkov, vendar pa niso določene posebne zahteve za nadaljnjo uporabo podatkov, povezanih z zdravjem, kakor je določeno v členu 8(4) Direktive 95/46/ES. Poleg tega drugi odstavek vsebuje brezpogojno obveznost prenosa velike količine podatkov Komisiji vsaj vsako leto. Ker ni izrecno navedena ocena potrebe po tem prenosu, se zdi, da je zakonodajalec Skupnosti že sam določil potrebo po teh prenosih Komisiji.

Priporočila ENVP

42. Da bi se ustrezno odzval na navedene elemente, je ENVP pripravil številna priporočila v obliki petih osnovnih korakov za spremembe, kakor je opisano v nadaljevanju.

Korak 1 – opredelitev zdravstvenih podatkov

43. Člen 4 opredeljuje osnovne izraze v predlogu. ENVP močno priporoča, da se v tem členu uvede opredelitev zdravstvenih podatkov. Uporabiti je treba široko razlago zdravstvenih podatkov, kakor je opisana v oddelku II tega mnenja (točki 14 in 15).

Korak 2 – uvedba posebnega člena o varstvu podatkov

44. ENVP tudi močno priporoča, da se v predlog uvede poseben člen o varstvu podatkov, ki bi lahko jasno in razumljivo določil splošno razsežnost politike. Ta člen mora (a) opisati pristojnosti držav članic zdravstvenega zavarovanja in zdravljenja, med drugim vključno s potrebo po varnosti obdelave, in (b) opredeliti glavna področja za nadaljnji razvoj, tj. uskladitev varnosti in vključitev zasebnosti v e-zdravje. Za ta vprašanja se lahko pripravijo posebne določbe (v predlaganem členu), kakor je opisano v korakih 3 in 4 spodaj.

Korak 3 – posebna določba o uskladitvi varnosti

45. Na podlagi spremembe iz koraka 2 ENVP priporoča, naj Komisija sprejme mehanizem za opredelitev splošno sprejemljive stopnje varnosti podatkov zdravstvenega varstva na nacionalni ravni, pri čemer je treba upoštevati obstoječe tehnične standarde na tem področju. To se mora odražati v predlogu. Izvajanje bi bilo možno z uporabo postopka v odboru, saj je to že opisano v členu 19 in velja za druge dele predloga. Poleg tega bi se lahko uporabili dodatni instrumenti za pripravo ustreznih smernic, pri čemer bi bile vključene vse zadevne zainteresirane strani, kot sta Delovna skupina iz člena 29 in ENVP.

Korak 4 – vključitev zasebnosti v predlogo za e-recept

46. Člen 14 o priznavanju zdravniških receptov, izdanih v drugi državi članici, določa razvoj predloge za zdravniški recept na ravni Skupnosti, ki podpira medobratovalnost e-receptov. Ta ukrep se sprejme s postopkom v odboru, saj je tako določeno v členu 19(2) predloga.

47. ENVP priporoča, naj predlagana predloga za e-recept vključuje zasebnost in varnost, tudi pri zelo osnovni semantični opredelitvi te predloge. To mora biti izrecno omenjeno v členu 14(2)(a). Tudi tu je bistvenega pomena vključenost ustreznih zainteresiranih strani. V zvezi s tem želi biti ENVP obveščen o nadaljnjih ukrepih, sprejetih glede tega vprašanja s predlaganim postopkom v odboru, in biti vanje vključen.

Korak 5 – nadaljnja uporaba zdravstvenih podatkov za namene statistike in spremljanja

48. Da bi preprečili nesporazume, ENVP poziva k pojasnitvi pojma „drugi dodatni podatki“ v členu 18(1). Nadalje je treba člen spremeniti v smislu, da se bo bolj izrecno skliceval na zahteve za nadaljnjo uporabo zdravstvenih podatkov, kakor je določeno v členu 8(4) Direktive 95/46/ES. Poleg tega je treba za obveznost prenosa podatkov Komisiji iz drugega odstavka oceniti potrebo po takšnih prenosih za namene zakonitosti, ki so ustrezno določeni vnaprej.

IV. **ZAKLJUČKI**

49. ENVP želi izraziti podporo pobudam za izboljšanje pogojev za čezmejno zdravstveno varstvo. Vendar pa izraža pomisleke glede dejstva, da pobude ES v zvezi z zdravstvenim varstvom niso vedno dobro medsebojno usklajene kar zadeva uporabo IKT, zasebnost in varnost, saj je tako težje sprejeti enoten pristop do varstva podatkov v zdravstvenem varstvu.

50. ENVP pozdravlja dejstvo, da je v trenutnem predlogu vključeno sklicevanje na zasebnost. Potrebne pa so številne spremembe, kakor je pojasnjeno v oddelku III tega mnenja, da bi določili jasne zahteve, tako za države članice zdravljenja kot tudi za države članice zdravstvenega zavarovanja, pa tudi da bi ustrezno obravnavali razsežnost varstva podatkov v čezmejnem zdravstvenem varstvu.

— V člen 4 je treba vključiti opredelitev zdravstvenih podatkov, ki bo zajemala vse osebne podatke, ki so lahko jasno in tesno povezani z opisom zdravstvenega stanja osebe. To mora načeloma zajemati medicinske podatke, pa tudi administrativne in finančne podatke v zvezi z zdravjem.

— Močno se priporoča uvedba posebnega člena o varstvu podatkov. Ta člen mora jasno določiti splošno podobo, opisati pristojnosti držav članic zdravstvenega zavarovanja in zdravljenja ter opredeliti glavna področja za nadaljnji razvoj, tj. uskladitev varnosti in vključitev zasebnosti, zlasti v aplikacije e-zdravja.

— Priporoča se, naj Komisija v okviru tega predloga sprejme mehanizem za opredelitev splošno sprejemljive stopnje varnosti podatkov zdravstvenega varstva na nacionalni ravni, pri čemer je treba upoštevati obstoječe tehnične standarde na tem področju. Spodbujati je treba tudi dodatne in/ali dopolnilne pobude, ki vključujejo vse zadevne zainteresirane strani, Delovno skupino iz člena 29 in ENVP.

— Priporoča se, naj se pojem „zasebnost pri oblikovanju“ vključi v predlagano predlogo Skupnosti za e-recept (tudi na semantični ravni). To bi moralo biti izrecno omenjeno v členu 14(2)(a). ENVP želi biti obveščen o nadaljnjih ukrepih, sprejetih glede tega vprašanja s predlaganim postopkom v odboru, in biti vanje vključen.

— Priporoča se, da se natančneje opredeli ubeseditev člena 18 in vključi bolj izrecni sklic na posebne zahteve glede nadaljnje uporabe podatkov v zvezi z zdravjem, kakor je določeno v členu 8(4) Direktive 95/46/ES.

V Bruslju, 2. decembra 2008

Peter HUSTINX

Evropski nadzornik za varstvo podatkov

Drugo mnenje Evropskega nadzornika za varstvo podatkov o pregledu Direktive 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah)

(2009/C 128/04)

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV JE –

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

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

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

ob upoštevanju Direktive 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij.

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 teh podatkov ter zlasti člena 41 Uredbe –

SPREJEL NASLEDNJE MNENJE:

I. UVOD

Ozadje

1. Evropska komisija je 13. novembra 2007 sprejela predlog, ki med drugim spreminja direktivo o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij, ponavadi naslovljeno Direktiva o zasebnosti in elektronskih komunikacijah [1] (v nadaljnjem besedilu predlog ali predlog Komisije). ENVP je 10. aprila 2008 sprejel mnenje o predlogu Komisije, v katerem je navedel priporočila za njegovo izboljšanje, s tem pa tudi sam poskušal zagotoviti, da bodo predlagane spremembe omogočile kar se da učinkovito varstvo zasebnosti in osebnih podatkov posameznikov (prvo mnenje ENVP) [2].

2. ENVP je ugodno ocenil predlog Komisije za vzpostavitev obveznega sistema za uradno obveščanje v primeru kršitev varnosti, v okviru katerega bodo morala podjetja uradno obvestiti posameznike, če bodo njihovi osebni podatki ogroženi. Poleg tega je tudi pohvalil novo določbo, ki omogoča pravnim osebam (kot so združenja za varstvo potrošnikov in ponudniki internetnih storitev), da ukrepajo proti pošiljateljem neželene pošte, kar je, poleg obstoječih, dodatni instrument za ukrepanje proti temu pojavu.

3. V razpravah, ki so potekale v Evropskem parlamentu pred prvo obravnavo, je ENVP predstavil nadaljnje nasvete oziroma pripombe glede nekaterih vprašanj, ki so se pojavila v poročilih odborov Evropskega parlamenta, pristojnih za pregled Direktive o univerzalni storitvi [3] in Direktive o zasebnosti in elektronskih komunikacijah (pripombe) [4]. V njih je obravnaval predvsem vprašanja, ki se nanašajo na obdelavo podatkov o prometu in varovanje pravic intelektualne lastnine.

4. Evropski parlament (EP) je 24. septembra 2008 sprejel zakonodajno resolucijo o direktivi o zasebnosti in elektronskih komunikacijah (prva obravnava) [5]. ENVP je pozitivno ocenil več sprememb EP, ki so bile sprejete v skladu z navedenim mnenjem in pripombami ENVP, med njimi vključitev ponudnikov storitev informacijske družbe (podjetij, ki delujejo preko spleta) v obveznosti v zvezi z uradnim obveščanjem o kršitvah varnosti. ENVP je tudi ugodno ocenil spremembo, ki omogoča pravnim in fizičnim osebam ukrepanje v primeru kršitev katerih

[1] Pregled Direktive o zasebnosti in elektronskih komunikacijah je del širšega postopka, katerega cilj je ustanovitev organa EU za telekomunikacijske storitve, pregled direktiv 2002/21/ES, 2002/19/ES, 2002/20/ES, 2002/22/ES in 2002/58/ES ter pregled Uredbe (ES) št. 2006/2004 (v nadaljnjem besedilu pregled telekomunikacijskega svežnja).

[2] Mnenje z dne 10. aprila 2008 o predlogu direktive, ki med drugim o spreminja Direktivo 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah), UL C 181, 18.7.2008, str. 1.

[3] Direktiva 2002/22/ES o univerzalni storitvi in pravicah uporabnikov v zvezi z elektronskimi komunikacijskimi omrežji in storitvami (Direktiva o univerzalnih storitvah) (UL L 108, 24.4.2002, str. 51).

[4] Pripombe ENVP v zvezo z izbranimi vprašanji na podlagi poročila odbora IMCO o pregledu Direktive 2002/22/ES (univerzalna storitev) in Direktive 2002/58/ES (Direktiva o zasebnosti in elektronskih komunikacijah), 2. september 2008. Na voljo na spletni strani: www.edps.europa.eu

[5] Zakonodajna resolucija Evropskega parlamenta z dne 24. septembra 2008 o predlogu direktive Evropskega parlamenta in Sveta o spremembi Direktive 2002/22/ES o univerzalni storitvi in pravicah uporabnikov v zvezi z elektronskimi komunikacijskimi omrežji in storitvami, Direktive 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij in Uredbe (ES) št. 2006/2004 o sodelovanju na področju varstva potrošnikov (COM(2007) 698 – C6-0420/2007 – 2007/248(COD).

koli določb direktive o zasebnosti in elektronskih komunikacijah (in ne samo kršitev določb o neželeni pošti, kot je predlagala Komisija). Po prvi obravnavi v Parlamentu je Komisija pripravila spremenjeni predlog Direktive o zasebnosti in elektronskih komunikacijah (v nadaljnjem besedilu spremenjeni predlog) ([6]).

5. Svet je 27. novembra 2008 dosegel politično soglasje o pregledu predpisov o svežnju predlogov o telekomunikacijah, med katerimi je tudi Direktiva o zasebnosti in elektronskih komunikacijah, ki bo predstavljeno kot skupno stališče Sveta (skupno stališče) ([7]). To stališče, ki bo v skladu s členom 251(2) Pogodbe o ustanovitvi Evropske skupnosti posredovano EP, lahko vključuje tudi spremembe, ki jih je predlagal slednji.

Splošno mnenje o skupnem stališču

6. Svet je spremenil bistvene elemente predloga in hkrati ni sprejel več sprememb, ki jih je predlagal EP. Čeprav je skupno stališče Sveta zagotovo tudi pozitivno, je ENVP zaskrbljen zaradi njegove vsebine, zlasti zato, ker vanj niso vključene nekatere pozitivne spremembe, ki so jih predlagali EP, Komisija (v spremenjenem predlogu), ENVP in evropski organi za varstvo podatkov v okviru razprav Delovne skupine iz člena 29 ([8]).

7. Nasprotno, določbe v spremenjenem predlogu Komisije in spremembah EP, ki ščitijo državljane, so v kar nekaj primerih znatno oslabljene ali črtane. Raven varstva posameznikov, kakor je predlagana v skupnem stališču, je tako precej nižja. ENVP je zato pripravil drugo mnenje, saj upa, da bodo v nadaljnji obravnavi Direktive o zasebnosti in elektronskih komunikacijah sprejete nove spremembe, ki bodo ponovno zaščitile državljane.

8. V drugem mnenju se je ENVP osredotočil na nekaj glavnih pomislekov in ni ponovil vseh pripomb, ki jih je navedel v mnenju iz decembra 2005 in so še vedno utemeljene. V njem obravnava zlasti:

— določbe o uradnem obveščanju o kršitvah varnosti;

— področje uporabe Direktive o zasebnosti in elektronskih komunikacijah v zasebnih in v javno dostopnih zasebnih omrežjih;

— obdelavo podatkov o prometu iz varnostnih razlogov;

— možnost, da pravne osebe ukrepajo v primeru kršitev direktive o zasebnosti in elektronskih komunikacijah.

9. Pri obravnavi navedenih vprašanj je ENVP analiziral skupno stališče Sveta in ga primerjal s predlaganimi spremembami EP in spremenjenim predlogom Komisije. V mnenje so vključena priporočila, ki naj bi racionalizirala določbe Direktive o zasebnosti in elektronskih komunikacijah in pomagala zagotoviti, da bo direktiva še naprej ustrezno varovala zasebnost in osebne podatke posameznikov.

II. **DOLOČBE O URADNEM OBVEŠČANJU O KRŠITVAH VARNOSTI**

10. ENVP podpira sprejetje določb o sistemu za uradno obveščanje v primeru kršitev, ki bo zagotavljal, da bodo organi in posamezniki obveščeni, če bodo njihovi osebni podatki ogroženi ([9]). Ta obvestila naj bi omogočila posameznikom, da ublažijo morebitno škodo zaradi ogroženosti. Poleg tega bo obveznost obveščanja o kršitvah spodbudila podjetja, da bodo izboljšala varstvo podatkov in okrepila odgovornost glede osebnih podatkov, s katerimi razpolagajo.

11. Pristopi treh institucij – Komisije v spremenjenem predlogu, Evropskega parlamenta v prvi obravnavi in Sveta v skupnem stališču – v zvezi z obravnavanim sistemom za uradno obveščanje se razlikujejo. Za vsakega od njih so značilni tudi pozitivni vidiki. Kljub temu pa je po mnenju ENVP treba vse tri pristope izboljšati, zato svetuje, naj institucije v zadnjih fazah pred sprejetjem sistema upoštevajo priporočila iz tega mnenja.

([6]) Spremenjeni Predlog direktive Evropskega parlamenta in Sveta o spremembi Direktive 2002/22/ES o univerzalni storitvi in pravicah uporabnikov v zvezi z elektronskimi komunikacijskimi omrežji in storitvami, Direktive 2002/58/ES o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij in Uredbe (ES) št. 2006/2004 o sodelovanju na področju varstva potrošnikov, 6.11.2008, COM(2008) 723 konč.

([7]) Na voljo na spletni strani Sveta.

([8]) Mnenje 2/2008 o pregledu direktive 2002/58/ES o zasebnosti in elektronskih komunikacijah, na voljo na spletni strani Delovne skupine iz člena 29.

([9]) V mnenju je uporabljena beseda „ogroženi“, ki se nanaša na vse kršitve varnosti osebnih podatkov zaradi nenamernega ali nezakonitega uničenja, izgube, spremembe, nepooblaščenega razkritja ali dostopa do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani.

12. Po analizi vseh treh pristopov je ENVP opozoril na pet kritičnih točk, o katerih bo treba še razpravljati: (i) opredelitev kršitve varnosti; (ii) subjekti, za katere velja obveznost uradnega obveščanja (zadevni subjekti); (iii) standard oziroma povod za obveznost obveščanja; (iv) opredelitev subjekta, ki bo odgovoren za odločanje o tem, ali je v določenem primeru kršitve varnosti potrebno obveščanje ali ne; (v) prejemniki obvestila.

Pregled pristopov Komisije, Sveta in EP

13. Evropski parlament, Svet in Komisija so sprejeli različne pristope glede obveščanja o kršitvah varnosti. EP je v prvi obravnavi spremenil prvotni sistem za obveščanje v primeru kršitev, ki ga je predlagala Komisija ([10]). Po mnenju EP obveznost obveščanja ne velja samo za ponudnike javno razpoložljivih elektronskih komunikacijskih storitev (PPECS), ampak tudi za ponudnike storitev informacijske družbe (ISSP). Poleg tega bi bilo treba po mnenju EP o vseh kršitvah varnosti osebnih podatkov obvestiti nacionalni regulativni organ ali pristojne organe (skupaj organe). Če bi organi ugotovili, da gre za *resne* kršitve, bi zahtevali od PPECS in ISSP, naj nemudoma obvestijo zadevno osebo. Če bi kršitve predstavljale takojšnjo in neposredno nevarnost, bi PPECS in ISSP najprej obvestili posameznike in šele nato organe, kar pomeni, da ne bi čakali na njihovo odločitev. Obveznost obveščanja potrošnika ne bi veljala samo za tiste subjekte, ki bi lahko organom dokazali, da „*so bili sprejeti ustrezni tehnični ukrepi*“ za preprečitev dostopa do podatkov nepooblaščenim osebam.

14. Tudi Svet meni, da bi morali biti obveščeni naročniki in organi, vendar le v primerih, če bi kršitve po mnenju *zadevnega* subjekta pomenile *resno* grožnjo za naročnikovo zasebnost (npr. kraja ali goljufija, fizična škoda, veliko ponižanje ali škodovanje ugledu).

15. V spremenjenem predlogu Komisije je ohranjena obveznost, ki jo je sprejel EP, tj. obveznost obveščanja organov o vseh kršitvah. Kljub temu pa je Komisija v spremenjeni predlog, v nasprotju s Parlamentom, vključila odstopanja, kar pomeni, da naj obveznost obveščanja zadevnih posameznikov ne bi veljala v primerih, če PPEC dokaže pristojnemu organu, da (i) ni „*dokaj verjetno*“, da bi posameznik lahko utrpel škodo (gospodarsko izgubo, družbeno škodo ali krajo identitete), ki bi bila posledica teh kršitev, ali da (ii) so bili sprejeti „*ustrezni tehnološki varnostni ukrepi*“ v zvezi s podatki, na katere se nanaša kršitev. Predlog Komisije torej vključuje analizo škode za posamezne kršitve oziroma obvestila o kršitvah.

([10]) To vprašanje je obravnavano zlasti v naslednjih spremembah EP: 187, 124 do 127 ter 27, 21 in 32.

16. Treba je opozoriti, da bi morali po mnenju EP ([11]) in Komisije o obveznosti obveščanja odločati *organi*, ki bi presodili, ali je kršitev resna, oziroma, ali je dokaj verjetno, da bi lahko povzročila škodo posamezniku. Svet, nasprotno, meni, da naj bi to odločitev sprejeli *zadevni subjekti*.

17. Po mnenju Sveta in Komisije naj bi obveznost obveščanja veljala samo za PPECS in ne tudi za ISSP, kot meni Parlament.

Opredelitev kršitve varnosti

18. ENVP z zadovoljstvom ugotavlja, da vsi trije zakonodajni predlogi vključujejo isto opredelitev obveznosti obveščanja v primeru kršitev varnosti, tj. za „*kršitve, ki povzročijo nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani […]*“ ([12]).

19. Kot je razvidno iz tega mnenja, ENVP pozitivno ocenjuje to opredelitev, saj je dovolj široka, da vključuje večino okoliščin, v katerih bi lahko bilo potrebno obveščanje o kršitvah varnosti.

20. Prvič: opredelitev vključuje primere, ko do podatkov *dostopa nepooblaščena* tretja oseba – kot je vdor v računalniški sistem, tj. strežnik, ki vsebuje osebne podatke, in priklic teh podatkov.

21. Drugič: opredelitev vključuje tudi primere, ko so bili osebni podatki izgubljeni ali razkriti, nepooblaščen dostop pa je treba še dokazati. Gre za primere, ko bi osebni podatki lahko bili izgubljeni (CD-romi, ključi USB ali druge prenosne naprave) ali pa so jih redni uporabniki naredili javnosti dostopne (mapa s podatki o zaposlenih, ki je bila nenamerno in začasno dostopna javnosti preko spleta). Ker pogosto ni dokazov o tem, ali so takšni podatki bili v določenem trenutku dostopni nepooblaščenim tretjim osebam oziroma ali so jih te osebe uporabljale, se zdi primerno, da so takšne okoliščine vključene v opredelitev. Zato ENVP priporoča, da opredelitev ostane v tej obliki. ENVP tudi priporoča, da se opredelitev kršitve varnosti vključi v člen 2 Direktive o zasebnosti in elektronskih komunikacijah, ker bi bilo to bolj skladno s celotno strukturo direktive in bi zagotavljalo večjo jasnost.

([11]) Razen v primerih takojšnje in neposredne nevarnosti, v katerih morajo zadevni subjekti najprej obvestiti potrošnika.

([12]) Člen (2) skupnega stališča in spremenjenega predloga ter člen 3.3 iz prve obravnave EP.

Subjekti, za katere bi morala veljati obveznost obveščanja

22. Po mnenju EP naj bi obveznost obveščanja veljala za PPECS in ISSP. Kljub temu pa Svet in Komisija menita, da naj bi obveznost obveščanja posameznikov v primeru, če je bila kršena varnost in bi lahko bili ogroženi njihovi osebni podatki, veljala le za PPECS, kot so podjetja, ki omogočajo telekomunikacijske storitve, in ponudniki dostopa do interneta. Za druge sektorje, kot so spletne banke, spletna trgovina na drobno, spletne zdravstvene storitve in druge, pa naj ne bi veljala. Kot je pojasnjeno v nadaljnjem besedilu, ENVP meni, da je z vidika javnega reda bistveno, da se zagotovi, da bo obveznost obveščanja veljala tudi za ponudnike storitev informacijske družbe, ki vključujejo spletne banke, ponudnike spletnih zdravstvenih storitev itd.

23. Prvič: ENVP meni, da so podjetja, ki zagotavljajo telekomunikacijske storitve, sicer res izpostavljena kršitvam varnosti, in zato mora zanje veljati obveznost obveščanja, kljub temu pa ugotavlja, da velja isto za vse druge vrste podjetij/ponudnikov. Spletni trgovci na drobno, spletne banke in spletne lekarne so ravno tako izpostavljeni kršitvam varnosti kot telekomunikacijska podjetja, če ne še v večji meri. Po preučitvi tveganj je torej mogoče ugotoviti, da obveznosti obveščanja ne bi smeli omejiti na PPECS. Da je potreben širši pristop, dokazujejo tudi izkušnje drugih držav. V Združenih državah so na primer skoraj vse države (več kot 40 v tem trenutku) sprejele zakonodajo glede obveznosti obveščanja o kršitvah varnosti, ki ima širše področje uporabe in torej ne vključuje samo PPECS, ampak vse subjekte, ki razpolagajo z osebnimi podatki.

24. Drugič: drži, da kršitev varnosti osebnih podatkov, ki jih redno obdelujejo PPECS, lahko vpliva na zasebnost posameznikov. Enako pa velja, če ni ta nevarnost še večja, za osebne podatke, ki jih obdelujejo ISSP. Banke in druge finančne institucije gotovo hranijo strogo zaupne informacije (npr. podatke o bančnih računih), ki bi v primeru razkritja lahko bili uporabljeni za krajo identitete. Še zlasti veliko škodo bi lahko posameznikom povzročilo tudi razkritje zelo občutljivih podatkov v zvezi z zdravstvenim stanjem, ki jih hranijo ponudniki spletnih zdravstvenih storitev. Zato si je treba zaradi vrst osebnih podatkov, katerih varnost bi lahko bila ogrožena, prizadevati za širšo veljavnost obveznosti obveščanja o kršitvah varnosti, ki mora vključevati vsaj ISSP.

25. Pri razpravah o razširitvi področja uporabe tega člena, tj. subjektih, za katere naj bi veljala navedena obveznost, so se pojavili nekateri pravni problemi. Zlasti je bilo poudarjeno, da se Direktiva o zasebnosti in elektronskih komunikacijah na splošno nanaša samo na PPECS, kar naj bi preprečevalo, da bi obveznost obveščanja veljala tudi za ISSP.

26. V tej zvezi želi ENVP opozoriti, da: (i) s pravnega vidika ni nikakršnih ovir, da ne bi področje uporabe nekaterih določb direktive razširili, tj. da se ne bi mogle uporabljati tudi za druge subjekte in ne samo za PPECS; zakonodajalec Skupnosti ima pri odločanju o tem popolnoma proste roke, (ii) veljavna Direktiva o zasebnosti in elektronskih komunikacijah že vključuje določbe, ki se nanašajo na subjekte, ki niso PPECS.

27. Primer: člen 13 se ne uporablja samo za PPECS, ampak za vsa podjetja, ki pošiljajo neželena sporočila, ob predhodni zahtevi za potrditev soglasja. Poleg tega člen 5(3) Direktive o zasebnosti in elektronskih komunikacijah, ki med drugim prepoveduje shranjevanje podatkov, kot so piškotki (*cookies*), v terminalski opremi uporabnikov, ne zavezuje samo PPECS, ampak vse subjekte, ki poskušajo shraniti podatke ali pridobiti dostop do podatkov, ki so shranjeni v računalniški opremi posameznikov. Poleg tega je Komisija v tem zakonodajnem postopku predlagala razširitev področja uporabe člena 5(3) na primere, ko se podobne tehnologije (piškotki/vohunska programska oprema) ne prenašajo samo preko elektronskih komunikacijskih sistemov, ampak tudi z vsemi drugimi možnimi metodami (pri prenosu s spleta ali preko zunanjih računalniških shranjevalnih nosilcev, kot so CD-romi, ključi USB, hitri pomnilniki (*flash drives*) itd.) Vsi ti elementi so pomembni in jih je treba ohraniti, v sedanjih razpravah o področju uporabe pa bi jih morali tudi upoštevati kot precedense.

28. Poleg tega sta Komisija in EP, verjetno pa tudi Svet, predlagala vključitev novega člena 6(6)(a), ki se nanaša na subjekte, ki niso PPECS, in je obravnavan v nadaljnjem besedilu.

29. Če upoštevamo vse pozitivne vidike obveznosti uradnega obveščanja o kršitvah varnosti, je zelo verjetno, da bodo državljani pričakovali koristi od tega ukrepa tudi v primeru, če bodo njihove osebne podatke ogrožali ISSP in ne samo v primeru kršitev s strani PPECS. Pričakovanja državljanov ne bodo uresničena, če na primer ne bodo obveščeni v primeru, če bi spletna banka izgubila podatke o njihovem bančnem računu.

30. Če povzamemo: ENVP je prepričan, da bo cilj določb o obveznem uradnem obveščanju v primeru kršitev varnosti bolje uresničen le, če bodo veljale za PPECS in ISSP.

Primeri, v katerih je obvezno uradno obveščanje

31. Kar zadeva povod za obveznost obveščanja, je po mnenju ENVP, kot je dodatno pojasnjeno v nadaljevanju, izmed treh predlogov najprimernejši pristop iz spremenjenega predloga, tj. „*če je dokaj verjetno*“, da bodo kršitve povzročile škodo: Kljub temu pa je treba zagotoviti, da je „škoda“ dovolj široko opredeljena, da zajema vse vidike negativnih posledic na zasebnost ali druge zakonite interese posameznikov. Sicer bi bilo bolje oblikovati novo opredelitev, v skladu s katero bi bilo obveščanje obvezno „*če je dokaj verjetno, da bo kršitev škodovala posameznikom*“.

32. Kot je bilo poudarjeno v prejšnjem delu, EP, Komisija in Svet predlagajo različne pogoje, pod katerimi je treba obvestiti posameznike (imenovane „povod“ ali „standard“). Očitno je, da bo število obvestil, ki jih bodo prejeli posamezniki, v veliki meri odvisno od predvidenih povodov oziroma standardov.

33. Svet in Komisija predlagata, da naj bi bilo obveščanje obvezno, če je kršitev „*resna grožnja za posameznikovo zasebnost*“ (Svet) in če „*je dokaj verjetno, da bi bile zaradi kršitve ogrožene koristi potrošnikov*“ (Komisija). Po mnenju EP naj bi obveščanje posameznikov bilo odvisno od „*resnosti kršitve*“ (tj. obveščanje posameznikov je obvezno, če se oceni, da je kršitev „*resna*“). Če ta pogoj ni izpolnjen, obveščanje ni obvezno ([13]).

34. Po mnenju ENVP je mogoče trditi, da imajo vsi posamezniki, katerih osebni podatki so bili ogroženi, v vseh okoliščinah pravico, da so o tem seznanjeni. Kljub temu pa bi bilo pravilno, da bi preučili, ali jo to ustrezna rešitev glede na druge interese in stališča.

35. Izražen je bil pomislek, da bi neomejena obveznost obveščanja v primerih ogrožanja varnosti osebnih podatkov lahko povzročila pretirano obveščanje in tozadevna „utrujenost“, kar bi povzročilo desenzibilizacijo. Kot je pojasnjeno v nadaljevanju, je ENVP se ENVP s tem argumentom sicer strinja, čeprav želi hkrati tudi poudariti, da ga skrbi možnost pretiranega obveščanja, ki bi bilo lahko dokaz za vsesplošen neuspeh ppostopkov za izboljšanje varnosti.

36. Kot je bilo že pojasnjeno, se ENVP zaveda morebitnih negativnih posledic pretiranega obveščanja in bi želel pomagati zagotoviti, da pravni okvir, ki bo sprejet v zvezi z obveščanjem o kršitvah varnosti, ne bo imel takšnih posledic. Če naj bi posamezniki bili obveščeni o kršitvah tudi v primeru, kadar te ne povzročajo škode ali stiske, bi lahko na koncu spodkopali enega od ključnih ciljev obveznosti obveščanja, saj bi posamezniki lahko, kar je ironija, spregledali obvestila prav v primerih, kjer bi se dejansko morali zavarovati. Zato je zelo pomembno doseči pravilno ravnotežje pri zagotavljanju premišljenega obveščanja, kajti v primeru, če se posamezniki ne bodo odzivali na prejeta obvestila, bo učinkovitost sistemov za obveščanje bistveno manjša.

37. Da bi sprejeli ustrezen standard, ki ne bi povzročil pretiranega obveščanja, je treba razmišljati ne samo o povodu za obveščanje, ampak tudi o drugih dejavnikih, zlasti o opredelitvi kršitve varnosti in informacijah, ki jih je treba sporočiti posamezniku. V tej zvezi ENVP ugotavlja, da glede na to, da je opredelitev kršitve varnosti široka, vsi trije predlogi omogočajo dokaj pogosto obveščanje. Zaskrbljenost zaradi možnosti pretiranega obveščanja je še toliko večja, ker opredelitev kršitve varnosti zajema vse vrste osebnih podatkov. Čeprav je to po mnenju ENVP pravilen pristop (brez omejevanja vrst osebnih podatkov, za katere velja obveznost obveščanja) – v nasprotju z drugimi pristopi, kot npr.v zakonodaji ZDA, kjer so zahtevki osredotočeni na občutljivost informacij – je vseeno dejavnik, ki ga je treba upoštevati.

38. Glede na navedeno in ob upoštevanju različnih spremenljivk, ki jih je treba obravnavati skupaj, bi bilo po mnenju ENVP primerno, da se določi, v katerih primerih je obveščanje obvezno.

39. V predlagani standard, tj. če kršitev pomeni „*resno tveganje za zasebnost*“ ali je „*dokaj verjetno, da bo povzročilo škodo*“, so v obeh primerih vključene na primer družbena škoda ali škoda ugledu in ekonomska izguba. Ta dva standarda naj bi vključevala vidike izpostavljenosti nevarnosti za krajo identitete zaradi razkritja skritih identifikatorjev kot so številke potnih listov, ter razkritje podatkov o zasebnem življenju posameznika. ENVP ugodno ocenjuje ta pristop. Prepričan je, da sistema obveščanja o kršitvah varnosti ne bi mogli v celoti izkoristiti, če bi vključeval samo kršitve, ki povzročijo ekonomsko izgubo.

([13]) Glede odstopanj od tega pravila glej opombo 11.

40. Glede na predlagana standarda ENVP meni, da je boljši predlog Komisije, tj. opredelitev „*dokaj verjetno, da bo povzročilo škodo*“, saj zagotavlja ustreznejšo raven zaščite posameznikov. Bolj verjetno je, da bo obveznost obveščanja potrebna, če je „*dokaj verjetno*“, da bodo kršitve „*povzročile škodo*“ zasebnosti posameznika, kot v primeru, če predstavljajo „*resno grožnjo*“. Če bi se torej omejili samo na kršitve, ki predstavljajo resno grožnjo zasebnosti posameznika, bi bistveno zmanjšali število kršitev, za katere velja obveznost obveščanja. To pa bi PPECS in ISSP zagotovilo pretirana pooblastila pri odločanju glede nujnosti obveščanja, saj je mnogo lažje utemeljiti ugotovitev, da ne obstaja „*resna grožnja*“, kot trditev, da ni „*dokaj verjetno, da bi lahko nastala*“ škoda. Čeprav je seveda treba preprečiti pretirano obveščanje, je v celoti gledano v primeru dvoma treba zavarovati zasebnost posameznikov, ki morajo biti zaščiteni vsaj v primeru, če je dokaj verjetno, da bi lahko kršitev povzročila škodo. Poleg tega bo izraz „*dokaj verjetno*“ v praksi bolj učinkovit, saj zajema subjekte in pristojne organe, ker zahteva objektivno oceno primera in njegovega ozadja.

41. Poleg tega lahko kršitve varnosti osebnih podatkov povzročijo škodo, ki je lahko zelo različna in jo je težko izmeriti. Dejansko lahko razkritje iste vrste podatkov v različnih okoliščinah povzroči določenemu posamezniku veliko škodo, drugega pa ne prizadene v takšni meri. Standard, ki bi določal, da je škoda materialna, pomembna ali resna, ne bi bil primeren. V predlogu Sveta je na primer zahteva, da ima kršitev *resne* posledice za zasebnost posameznika; glede na zahtevo, da mora kršitev imeti „resne“ posledice, s takšnim pristopom ne bi bila zagotovljena ustrezna zaščita posameznikov, hkrati pa bi tudi vplival na objektivnost presoje.

42. Čeprav ENVP meni, kot je bilo že pojasnjeno, da je „*dokaj verjetno, da se povzroči škoda*“ primeren standard za obveznost obveščanja o kršitvah varnosti, se kljub temu boji, da vanj ne bi bili vključeni vsi primeri, za katere velja obveznost obveščanja, tj. vsi primeri, v katerih je dokaj verjetno, da bodo imele kršitve negativne posledice na zasebnost ali druge zakonite pravice posameznikov. Zato bi bilo treba preučiti naslednjo opredelitev primerov, v katerih je potrebna obveznost obveščanja, tj. „*če je dokaj verjetno, da bo kršitev imela negativne posledice za posameznike*“.

43. Takšna opredelitev je primerna tudi z vidika skladnosti z zakonodajo EU o varstvu podatkov. Dejansko so v direktivi o varstvu podatkov velikokrat navedene negativne posledice za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki. Na primer: člen 18 in uvodna izjava 49, ki obravnavata obveznost registracije postopkov obdelave osebnih podatkov pri organih za varstvo podatkov, omogočata državam članicam odstopanje od te obveznosti v primeru, če „*obdelava zelo verjetno ne bo škodljivo vplivala na pravice in svoboščine posameznikov, na katere se osebni podatki nanašajo*“. Podobna določba je uporabljena v členu 16(6) skupnega stališča, njen namen pa je zagotoviti pravnim osebam možnost ukrepanja proti pošiljateljem neželene pošte.

44. Poleg tega bi lahko glede na navedeno tudi pričakovali, da naj bi bili zadevni subjekti in zlasti organi, ki so pristojni za izvajanje zakonodaje o varstvu podatkov, bolje seznanjeni z navedenim standardom, kar bi pripomoglo k lažjemu odločanju glede tega, ali je obveznost obveščanja v posameznem primeru potrebna ali ne.

Subjekt, ki odloča o tem, ali je obveznost obveščanja v primeru kršitve obvezna ali ne

45. Po mnenju EP (razne v primerih neposredne nevarnosti) in v skladu s spremenjenim predlogom Komisije, naj bi o tem, ali je v določenem primeru kršitve zasebnosti obveščanje posameznika obvezno ali ne, odločali organi držav članic.

46. Po mnenju ENVP imajo ti organi pomembno vlogo pri odločanju o tem, ali je obveščanje obvezno, saj v določeni meri jamčijo za pravilno izvajanje zakonov. Takšen sistem bi lahko podjetjem preprečeval, da bi neustrezno ocenila, da kršitev ni škodljiva/resna, in bi se s tem izognila obveznosti obveščanja, čeprav bi bila ta dejansko potrebna.

47. Po drugi strani pa po mnenju ENVP zbuja pomisleke dejstvo, da bi bil sistem, v katerem bi odločali nacionalni organi, nepraktičen in bi ga težko uporabljali oziroma bi se lahko v praksi izkazalo, da je kontraproduktiven. Lahko bi celo povzročil, da bi bili osebni podatki posameznikov slabše zaščiteni.

48. V skladu s tem pristopom bi se dejansko lahko dogajalo, da bi organi za varstvo podatkov prejemali preveliko količino obvestil o kršitvah varnosti in bi zato z veliko težavo pripravljali potrebne ocene. Treba je opozoriti, da morajo organi pri odločanju o tem, ali je v primeru kršitve potrebno obveščanje, zbrati dovolj notranjih informacij, ki so večinoma tehnično zelo kompleksne in jih je treba obdelati zelo hitro. Glede na to, da je takšno ocenjevanje težavno in da imajo nekateri organi omejene vire, bi se po mnenju ENVP lahko zgodilo, da bodo ti organi s težavo izpolnjevali to obveznost in bi lahko v ta namen prerazporejali vire, zadolžene za druge pomembne prednostne naloge. Poleg tega bi takšen sistem pomenil nepotreben pritisk na te organe; če bi sprejeli odločitev, da kršitev ni resna, posamezniki pa bi zaradi nje kljub temu utrpeli škodo, bi se lahko zgodilo, da bi organi morali prevzeti odgovornost.

49. Navedena težava je še dodatno obremenjujoča, če se upošteva, da je ključni dejavnik pri zmanjševanju tveganja, ki ga povzročijo kršitve varnosti, čas. Če organi ne morajo pripraviti ocene v zelo kratkem času in za to potrebujejo dodatni čas, lahko to poveča škodo, ki jo utrpijo posamezniki. Ironija pa je v tem, da bi bi zato lahko ta dodatni ukrep, ki naj bi zagotovil boljšo zaščito posameznikov, te ščitil slabše kot sistemi, ki temeljijo na neposrednem obveščanju.

50. Zato bi bilo po mnenju ENVP bolj primerno, da bi vzpostavili sistem, ki ga predlaga Svet, tj. sistem, v katerem bi zadevni subjekti odločali, ali je obveznost obveščanja potrebna ali ne.

51. Kljub temu pa je treba preprečiti možnost zlorabe, tj. da bi lahko subjekti odklonili obveščanje v primerih, ko je to izrazito potrebno; zato je nadvse pomembno, da se vključijo v nadaljevanju navedeni zaščitni ukrepi za varstvo podatkov.

52. Prvič: obveznost subjektov, da sami odločajo o tem, ali je obveščanje potrebno, mora biti združena z drugo obveznostjo, tj. zahtevo po obveznem obveščanju organov v primeru vseh kršitev, ki ustrezajo predpisanemu standardu. Subjekti bi morali v teh primerih obvestiti organe o kršitvah in razlogih za njihovo odločitev o obvestilu ter vsebini vseh poslanih obvestil.

53. Drugič: organom je treba dejansko zagotoviti nadzorno vlogo. Pri tem jim mora biti omogočena neobvezna preiskava okoliščin kršitve in možnost, da zahtevajo kakršne koli ustrezne ukrepe za izboljšanje ([14]). Poleg obveščanja posameznikov (če še ni bilo izvedeno), bi morala biti vključena tudi možnost, da naložijo subjektom obveznost za sprejetje ukrepov, s katerimi naj bi preprečili nadaljnje kršitve. V tej zvezi bi morali organi imeti učinkovita pooblastila in vire, pa tudi potrebno svobodo pri odločanju o tem, ali je treba v primeru obvestila o kršitvi varnosti ukrepati ali ne. Z drugimi besedami: na ta način bi lahko zagotovili organom možnost izbire in s tem preiskavo velikih in resnično škodljivih kršitev varnosti ter preverjanje in boljšo usklajenost z zakonodajo.

54. Da bi uresničili navedene cilje, ENVP predlaga, da se poleg pooblastil, dodeljenih v skladu s členom 15(a)(3) Direktive o zasebnosti in elektronskih komunikacijah ter Direktive o varstvu podatkov, vključi naslednje besedilo: *„Če naročnik ali zadevni posameznik še ni bil obveščen o kršitvi, lahko pristojni nacionalni organ po preučitvi zadeva zahteva od PPECS ali ISSP, da pošlje obvestilo.“*

55. Poleg tega ENVP priporoča EP in Svetu, naj potrdita obveznost, ki jo predlaga EP (sprememba št. 122, člen 4(1)(a), tj. da morajo subjekti oceniti in presoditi, kakšno tveganje je povezano z njihovimi sistemi in osebnimi podatki, ki jih nameravajo obdelovati. V skladu s to obveznostjo naj bi subjekti pripravili ustrezno in natančno opredelitev zaščitnih ukrepov, ki jih bodo uporabljali in ki naj bi bili na razpolago organom. V primeru kršitve varnosti bo ta obveznost pomagala zadevnim subjektom – in morda tudi organom v vlogi nadzornikov – pri odločanju o tem, ali bi ogrožanje informacij lahko imelo negativne posledice ali povzročilo škodo posameznikom.

56. Tretjič: obveznost subjektov, da odločajo o obveščanju posameznikov, se mora uporabljati hkrati z obveznostjo beleženja podrobne in celovite notranje revizijske sledi, v okviru katere je treba opisati vse kršitve varnosti in navesti poročila o njih, pa tudi vse ukrepe, ki so bili sprejeti za preprečevanje kršitev v prihodnje. Ta notranja revizijska sled mora biti na razpolago organom pri pregledu in morebitni preiskavi. Omogočilo jim bo izvedbo nadzora. To bi bilo mogoče doseči z vključitvijo naslednjega besedila: *„PPECS in ISSP vodijo in hranijo celovite evidence, v katerih so podrobno navedene vse kršitve, z njimi povezane tehnične informacije in ukrepi za izboljšanje. V evidencah so zabeležena tudi vsa obvestila naročnikom ali zadevnim posameznikom ter pristojnim nacionalnim organom, vključno z datumom in vsebino. Evidence se na zahtevo predložijo pristojnemu organu.“*

57. Da se zagotovi doslednost pri izvajanju predpisanega standarda ter drugih vidikov okvira v zvezi s kršitvami varnosti, kot sta oblika in postopki obveščanja, je seveda treba poskrbeti, da lahko Komisija po posvetovanju z ENVP, Delovno skupino iz člena 29 in drugimi zainteresiranimi stranmi sprejme tehnične izvedbene ukrepe.

([14]) To je zagotovljeno tudi v členu 15(a)(3), ki določa, da *„države članice zagotovijo, da imajo pristojni nacionalni organi in po potrebi drugi nacionalni organi vsa potrebna preiskovalna pooblastila in sredstva ter možnost za pridobitev vseh ustreznih informacij, ki so potrebne za spremljanje in izvrševanje nacionalnih določb, sprejetih na podlagi te direktive“*.

Prejemniki obvestila

58. V zvezi s prejemniki obvestila je ENVP bolj naklonjen izrazom, ki jih navajata EP in Komisija, kot terminologiji, ki jo uporablja Svet. EP je besedo „naročniki“ nadomestil z izrazom „uporabniki“. Komisija uporablja izraza „naročniki“ in „zadevni posamezniki“. V predlogih EP in Komisije prejemniki obvestil niso samo sedanji, ampak tudi nekdanji naročniki in tretje strani, kot so uporabniki, ki so v stiku z zadevnimi subjekti, niso pa njihovi naročniki. ENVP pozitivno ocenjuje ta pristop in zato Evropskemu parlamentu in Svetu priporoča, naj ga ohranita.

59. Kljub temu pa ENVP ugotavlja, da obstaja vrsta nedoslednosti glede na terminologijo, ki jo je EP uporabljal v prvi obravnavi; to napako je treba odpraviti. Na primer: beseda „naročniki“ je bila v večini primerov, ne pa v vseh, zamenjana z besedo „uporabniki“, v drugih primerih je bila vstavljena beseda „potrošniki“. To je treba uskladiti.

III. **PODROČJE UPORABE DIREKTIVE O ZASEBNOSTI IN ELEKTRONSKIH KOMUNIKACIJAH: JAVNA IN ZASEBNA OMREŽJA**

60. V členu 3(1) sedanje Direktive o zasebnosti in elektronskih komunikacijah je določeno, kdo so subjekti, na katere se nanaša ta direktiva; gre namreč za subjekte, ki obdelujejo podatke „*v zvezi z*“ zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev (v tem besedilu: PPECS) ([15]). Med dejavnosti PPECS štejemo zagotavljanje dostopa do interneta, prenos informacij prek elektronskih omrežij, povezave mobilne in fiksne telefonije itd.

61. Evropski parlament je sprejel spremembo št. 121 v zvezi s členom 3 prvotnega predloga Komisije, na podlagi katere je bilo področje uporabe Direktive o zasebnosti in elektronskih komunikacijah razširjeno, in sicer tako, da zajema: „*obdelavo osebnih podatkov v zvezi z zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev v javnih in zasebnih komunikacijskih omrežjih in javno dostopnih zasebnih omrežjih v Skupnosti*“ (člen 3(1) Direktive o zasebnosti in elektronskih komunikacijah). Za Svet in Komisijo ta sprememba, žal, ni bila sprejemljiva, zato je nista upoštevala v skupnem stališču in spremenjenem predlogu.

Uporaba direktive o zasebnosti in elektronskih komunikacijah v javno dostopnih zasebnih omrežjih

62. ENVP je naklonjen ohranitvi bistvenega dela spremembe št. 121, saj želi spodbuditi uskladitev mnenj, v nadaljevanju pa navaja tudi druge razloge. Predlaga tudi dodatno spremembo, tj. podrobnejše pojasnilo glede vrst storitev, ki naj bi bile zajete v razširjenem področju uporabe.

63. Zasebna omrežja se pogosto uporabljajo za zagotavljanje elektronskih komunikacijskih storitev, kot je dostop do interneta, neopredeljenemu, potencialno pa zelo velikemu številu ljudi. To denimo drži za dostop do interneta v spletnih kavarnah v hotelih in restavracijah ter na letališčih, vlakih in drugih krajih, ki so dostopni javnosti, kjer ponujajo – pogosto skupaj z drugimi storitvami (pijače, nastanitev itd.) – zaščiteni brezžični dostop (*Wi-Fi*).

64. V vseh navedenih primerih se komunikacijska storitev, torej dostop do interneta, ne zagotavlja javnosti prek javnega omrežja, pač pa prek omrežja, ki bi lahko veljalo za zasebno, saj z njim upravljajo zasebniki. Čeprav gre v zgornjih primerih za zagotavljanje komunikacijskih storitev javnosti, je zaradi vrste omrežja, ki je zasebno in ne javno, *možno*, da tozadevne storitve niso v celoti zajete v direktivi o zasebnosti in elektronskih komunikacijah ali vsaj v nekaterih členih te direktive ([16]). V teh primerih zato niso zaščitene temeljne pravice posameznikov, ki jih zagotavlja ta direktiva. Uporabniki storitev dostopa do interneta prek javnih telekomunikacijskih omrežij in uporabniki istih storitev v zasebnih omrežjih so tako v neenakem pravnem položaju, čeprav so zasebnost in osebni podatki posameznikov v vseh teh primerih enako ogroženi, kot če se storitev izvaja v javnih omrežjih. Zdi se torej, da ni nobene logične osnove, s katero bi bilo mogoče v okviru direktive upravičiti razlikovanje med komunikacijskimi storitvami, ki se zagotavljajo prek zasebnega omrežja, in storitvami, ki jih zagotavlja javno omrežje.

65. ENVP se zato zavzema za spremembo, kot je sprememba št. 121 Evropskega parlamenta, v skladu s katero bi se direktiva o zasebnosti in elektronskih komunikacijah uporabljala tudi za obdelavo osebnih podatkov v zvezi z zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev v *zasebnih* komunikacijskih omrežjih.

66. ENVP se sicer zaveda, da bi lahko takšna formulacija imela nepredvidene in morebitne nenamerne posledice. Že samo zaradi navedbe zasebnih omrežij bi bilo mogoče sklepati, da direktiva zajema tudi primere, za katere je sicer jasno, da ne spadajo v njeno področje uporabe. Možna je na primer ugotovitev, da bi z dobesedno oziroma strogo

([15]) „Ta direktiva se uporabi za obdelavo osebnih podatkov v zvezi z zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev v javnih komunikacijskih omrežjih.“

([16]) Nasprotno pa bi bilo mogoče trditi, da zagotavljanje komunikacijskih storitev javnosti, tudi prek zasebnega omrežja, ureja obstoječi pravni okvir, torej ne glede na to, da gre za zasebno omrežje. V Franciji, na primer, so delodajalci, ki svojim zaposlenim zagotavljajo dostop do interneta, izenačeni s komercialnimi ponudniki dostopa do interneta. Ta razlaga sicer ni splošno uveljavljena.

razlago te formulacije v področje uporabe direktive vključili tudi lastnike domov, ki so opremljeni z WiFi ([17]) in s tem vsem, ki so v njihovem dosegu (običajno v domu), omogočajo zaščiteni brezžični dostop; to pa ni namen spremembe št. 121. Da bi se temu izognili, ENVP predlaga novo besedilo spremembe št. 121, tako da bi področje uporabe direktive o zasebnosti in elektronskih komunikacijah zajemalo *„obdelavo osebnih podatkov v zvezi z zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev v javnih ali javno dostopnih zasebnih komunikacijskih omrežjih v Skupnosti*".

67. Na ta način bi bilo jasno navedeno, da naj bi se direktiva o zasebnosti in elektronskih komunikacijah nanašala le na tista zasebna omrežja, ki so javno dostopna. Direktiva, katere določbe se uporabljajo *le* za *javno dostopna zasebna omrežja* (in ne za vsa zasebna omrežja), bo zato zajemala le komunikacijske storitve v okviru zasebnih omrežij, ki so namenoma *dostopna* javnosti. S tako formulacijo bo mogoče v še večji meri izpostaviti dejstvo, da je pri ugotavljanju tega, ali zasebno omrežje spada na področje uporabe direktive, ključni dejavnik predvsem *dostopnost* tega omrežja *za širšo javnost*. Povedano drugače, če je omrežje – ne glede na to, ali gre za javno ali zasebno omrežje – namenoma na voljo javnosti zaradi zagotavljanja javne telekomunikacijske storitve, kot je dostop do interneta, tudi če gre pri tem za dopolnilno storitev (npr. hkrati s hotelsko nastanitvijo), je ta vrsta storitve oziroma omrežja zajeta v Direktivi o zasebnosti in elektronskih komunikacijah.

68. ENVP ugotavlja, da je navedeni pristop, ki ga je podprl, in na podlagi katerega se določbe Direktive o zasebnosti in elektronskih komunikacijah uporabljajo za *javno dostopna zasebna omrežja*, v skladu s pristopi številnih držav članic, kjer so oblasti že odločile, da take vrste storitev, vključno s storitvami v povsem zasebnih omrežjih, spadajo na področje uporabe nacionalnih določb o izvajanju navedene direktive ([18]).

69. Zaradi dodatne pravne varnosti subjektov, ki naj bi jih zajemalo novo področje uporabe, bi bilo morda v Direktivo o zasebnosti in elektronskih komunikacijah koristno vključiti tudi opredelitev „javno dostopnih zasebnih omrežij", ki bi se lahko glasila takole: *„Javno dostopno zasebno omrežje pomeni omrežje, s katerim upravljajo zasebniki in do katerega ima širša javnost praviloma neomejen dostop, in sicer proti plačilu ali zastonj oziroma v povezavi z drugimi storitvami ali ponudbami ter ob upoštevanju veljavnih pogojev.*".

70. V praksi to pomeni, da bi direktiva zajemala zasebna omrežja v hotelih in na drugih mestih, kjer širši javnosti zagotavljajo dostop do interneta prek zasebnega omrežja. Nasprotno pa direktiva ne bi urejala komunikacijskih storitev omejene skupine določljivih posameznikov v povsem zasebnih omrežjih. Virtualna zasebna omrežja in domovi uporabnikov, opremljeni z WiFi, tako na primer ne bi spadali v področje uporabe direktive; enako bi veljalo tudi za storitve, ki se zagotavljajo prek omrežij, ki so izključno korporacijska.

Zasebna omrežja v okviru področja uporabe Direktive o zasebnosti in elektronskih komunikacijah

71. Izključitev zasebnih omrežij kot takih, kot je predlagano zgoraj, bi morala veljati za *začasen* ukrep, o katerem bi bilo treba dodatno razpravljati. Ob upoštevanju posledic, ki bi jih izključitev povsem zasebnih omrežij imela za varstvo zasebnosti, ter po drugi strani dejstva, da izključitev zadeva veliko število ljudi, ki do interneta običajno dostopajo prek korporacijskih omrežij, bi bilo treba to vprašanje v prihodnosti morda zares ponovno preučiti. Da bi spodbudil razpravo o tem, ENVP priporoča, da se v Direktivo o zasebnosti in elektronskih komunikacijah vključi uvodna izjava, na podlagi katere bi Komisija izvedla javno posvetovanje glede uporabe te direktive za vsa zasebna omrežja, pri čemer bi sodelovali tudi ENVP, organi za varstvo podatkov in druge zadevne zainteresirane strani. V uvodni izjavi bi lahko poleg tega določili, da bi morala Komisija po opravljenem javnem posvetovanju preučiti rezultate in temu primerno predlagati vključitev novih vrst subjektov, ki bi jih morala zajemati Direktiva o zasebnosti in elektronskih komunikacijah, oziroma njihovo omejitev.

72. Ustrezno bi bilo treba spremeniti tudi različne člene navedene direktive, tako da se bodo vse izvedbene določbe v zvezi z javnimi omrežji izrecno nanašale tudi na javno dostopna zasebna omrežja.

IV. **OBDELAVA PODATKOV O PROMETU IZ VARNOSTNIH RAZLOGOV**

73. Družbe, ki zagotavljajo varnostne storitve, so med zakonodajnim postopkom v zvezi z revizijo Direktive o zasebnosti in elektronskih komunikacijah izjavile, da bi bilo treba v direktivo vnesti določbo, s katero bi upravičili zbiranje podatkov o prometu in s tem zagotovili učinkovito spletno varnost.

([17]) Običajno gre za brezžično lokalno omrežje (*Local Area Network* – LAN).

([18]) Glej opombo 16.

74. Evropski parlament je zato v besedilo vnesel spremembo št. 181 o oblikovanju novega člena 6(6)(a), s katerim bi bilo izrecno dovoljeno obdelovanje podatkov o prometu iz varnostnih razlogov: „*Brez poseganja v skladnost z določbami, razen člena 7 Direktive 95/46/EC in člena 5 te direktive, se lahko podatki o prometu obdelajo za zakoniti interes kontrolorja podatkov za namene uvajanja tehničnih ukrepov za zagotovitev varnosti omrežja in informacij javnih storitev elektronskih komunikacij, javnega ali zasebnega omrežja elektronskih komunikacij, storitev informacijske družbe ali s tem povezane terminalske in elektronskokomunikacijske opreme, kot je opredeljeno v členu 4(c) Uredbe (ES) št. 460/2004 Evropskega parlamenta in Sveta z dne 10. marca 2004 o ustanovitvi Evropske agencije za varnost omrežij in informacij, razen kadar nad temi interesi ne prevlada interes posameznikovih temeljnih pravic in svoboščin. Obdelava mora biti omejena na to, kar je nujno potrebno za izvajanje določene/takšne varnostne dejavnosti.*“.

75. V spremenjenem predlogu Komisije je ta sprememba načeloma upoštevana, črtana pa je odločilna klavzula, katere namen je bil zagotoviti spoštovanje drugih določb direktive in ki se glasi: „*Brez poseganja v […] … določbe te direktive […]*“. Svet je sprejel preoblikovano različico, v kateri so pomembne določbe o zaščiti in uravnoteženosti interesov iz spremembe št. 181 še nekoliko bolj oslabljene, saj se sedaj glasi takole: „*Podatki o prometu se lahko obdelujejo, kolikor je to potrebno za zagotovitev varnosti omrežij in informacij, kot je opredeljena v členu 4(c) Uredbe (ES) 460/2004 Evropskega parlamenta in Sveta z dne 10. marca 2004 o ustanovitvi Evropske agencije za varnost omrežij in informacij*“.

76. Kot je podrobneje obrazloženo v nadaljevanju, je člen 6(6)(a) nepotreben, obstaja pa tudi nevarnost zlorabe, zlasti če bi bil sprejet brez pomembnih zaščitnih ukrepov, klavzul o upoštevanju drugih določb direktive ter uravnoteženosti interesov. ENVP zato priporoča črtanje tega člena ali vsaj zagotovitev, da bodo vsi tovrstni členi vsebovali zaščitne ukrepe, in sicer po vzoru spremembe št. 181, ki jo je sprejel Evropski parlament.

Pravni razlogi za obdelavo podatkov o prometu, ki veljajo za elektronske komunikacijske storitve in druge upravljavce podatkov na podlagi sedanje zakonodaje na področju varstva podatkov

77. Ponudniki javno razpoložljivih elektronskih komunikacijskih storitev lahko zakonito obdelujejo podatke o prometu ob upoštevanju omejitev iz člena 6 Direktive o zasebnosti in elektronskih komunikacijah; v skladu s tem členom je tovrstna obdelava dovoljena le za nekatere namene, kot so denimo obračunavanje, medsebojno povezovanje in trženje. Ta obdelava lahko poteka le ob upoštevanju natančno določenih pogojev – v primeru trženja je to privoljenje posameznikov. V skladu s členom 7 Direktive o varstvu podatkov – ta določa, da lahko upravljavci podatkov obdelujejo osebne podatke ob upoštevanju vsaj ene od naštetih pravnih podlag oziroma pravnih razlogov – lahko poleg tega podatke o prometu obdelujejo tudi drugi upravljavci podatkov, kot so ponudniki storitev informacijske družbe.

78. Eden od primerov takšne pravne podlage je člen 7(a) Direktive o varstvu podatkov, v katerem je določeno, da je potrebna privolitev posameznika, na katerega se nanašajo osebni podatki. Če želi na primer spletni trgovec na drobno obdelovati podatke o prometu zaradi razpošiljanja oglasnih ali tržnih gradiv, mora za to pridobiti privoljenje posameznika. Drug primer pravne podlage iz člena 7 v nekaterih primerih npr. dopušča, da lahko podatke o prometu iz varnostnih razlogov obdelujejo tudi podjetja za varovanje, ki nudijo varnostne storitve; to je utemeljeno s členom 7(f), v katerem je določeno, da lahko upravljavci podatkov obdelujejo osebne podatke le, „*če je obdelava potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja stranka ali stranke, ki so jim osebni podatki posredovani, razen kadar nad takimi interesi prevladajo temeljne pravice in svoboščine posameznika, na katerega se osebni podatki nanašajo […]*“ V Direktivi o varstvu podatkov ni posebej določeno, v katerih primerih bi obdelava osebnih podatkov ustrezala tej zahtevi. Tovrstne odločitve zato sprejemajo upravljavci podatkov, in sicer za vsak primer posebej, pogosto s soglasjem nacionalnih organov za varstvo podatkov in drugih organov.

79. Preučiti bi bilo treba medsebojno učinkovanje člena 7 Direktive o varstvu podatkov ter predlaganega člena 6(6)(a) Direktive o zasebnosti in elektronskih komunikacijah; v slednjem je podrobno opisano, kaj je potrebno za izpolnjevanje zahtev iz navedenega člena 7(f). Člen 6(6)(a) namreč z odobritvijo obdelave podatkov o prometu, s čimer naj bi zagotovili varnost omrežja in informacij, omogoča takšno obdelavo zaradi zakonitih interesov, za katere si prizadeva upravljavec podatkov.

80. Kot je obrazloženo v nadaljevanju, ENVP meni, da predlagani člen 6(6)(a) ni niti potreben niti koristen. S pravnega vidika načeloma pravzaprav ni potrebe po tem, da bi bilo treba ugotavljati, ali določena dejavnost obdelovanja podatkov, v tem primeru je to obdelava podatkov o prometu iz varnostnih razlogov, izpolnjuje zahteve iz člena 7(f) Direktive o varstvu podatkov, pri čemer je morda potrebna privolitev posameznika na podlagi člena 7(a). Kot je bilo že navedeno, o tem ponavadi odločijo upravljavci podatkov, torej podjetja, in sicer, glede izvajanja, po posvetovanju z organi za varstvo podatkov, po potrebi pa o tem odločajo tudi sodišča. ENVP na splošno meni, da je za zakonito obdelavo podatkov o prometu iz varnostnih razlogov v specifičnih primerih, ki ne vpliva na temeljne pravice in svoboščine posameznikov, verjetno,

da bo ustrezala zahtevam iz člena 7(f) Direktive o varstvu podatkov. V obeh direktivah, tisti o varstvu podatkov ter Direktivi o zasebnosti in elektronskih komunikacijah, poleg tega ni nobenih drugih primerov izločevanja ali posebne obravnave določenih vrst dejavnosti obdelave podatkov v skladu z merili iz člena 7(f), prav tako pa tudi ni nobenih dokazov, da bi bile take izjeme potrebne. Ravno nasprotno, glede na povedano se zdi, da bi v številnih primerih taka dejavnost popolnoma ustrezala določbam sedanjega besedila. Pravna določba, s katero naj bi to oceno potrdili, je zato načeloma nepotrebna.

Člen 6(6)(a) – različice Evropskega parlamenta, Sveta in Komisije

81. Kot je bilo že obrazloženo, je sprememba št. 181, ki jo je sprejel Evropski parlament, sicer nepotrebna, vseeno pa je treba poudariti, da so bila pri njenem oblikovanju v določeni meri upoštevana načela zasebnosti in varstva podatkov, določena v zakonodaji o varstvu podatkov. V spremembi št. 181, ki jo je pripravil Evropski parlament, bi lahko varstvu podatkov in zasebnosti dali še večji poudarek, če bi vanjo na primer vključili besede „v posebnih primerih“ in s tem zagotovili selektivno uporabo tega člena, ali pa z določitvijo specifičnega obdobja hrambe.

82. Sprememba št. 181 ima nekaj pozitivnih strani. Potrjuje, da bi morala obdelava potekati v skladu z vsemi drugimi načeli varstva podatkov, ki veljajo za obdelavo osebnih podatkov: „*Brez poseganja v skladnost z določbami […] Direktive 95/46/ES in […] te direktive*“. Sprememba št. 181 sicer dopušča obdelavo podatkov iz varnostnih razlogov, vendar hkrati v enaki meri upošteva interese subjekta, ki obdeluje podatke o prometu, ter interese posameznikov, katerih podatki se obdelujejo; takšna obdelava podatkov je torej mogoča le v primeru, kadar interes subjekta, ki obdeluje podatke, ne prevlada nad interesom temeljnih pravic in svoboščin posameznikov („*razen kadar nad temi interesi ne prevlada interes posameznikovih temeljnih pravic in svoboščin*“). Ta zahteva je bistvena, saj je z njo mogoče upravičiti obdelovanje podatkov o prometu v specifičnih primerih, ne pa tudi obdelavo svežnjev podatkov o prometu.

83. Spremenjena različica spremembe, ki jo je pripravil Svet, ima nekaj pohvale vrednih elementov; v njej so obdržali izraz „*nujno potrebno*“, s čimer je poudarjeno omejeno področje uporabe tega člena. Toda v različici Sveta ni več navedenih zaščitnih ukrepov glede varstva podatkov in zasebnosti. Načeloma sicer veljajo splošne določbe o varstvu podatkov, ne glede na specifično sklicevanje pri vsakem primeru posebej, toda člen 6(6)(a) v različici Sveta bi bilo mogoče kljub temu razumeti tako, kot da dopušča neomejeno obdelavo podatkov o prometu, ne da bi bilo treba pri tem upoštevati kakršne koli zaščitne ukrepe glede varstva podatkov in zasebnosti, ki se sicer uporabljajo pri obdelavi podatkov o prometu. Slednje bi torej lahko zbirali, hranili in jih nadalje uporabljali brez upoštevanja načel varstva podatkov in izpolnjevanja specifičnih obveznosti, ki sicer veljajo za zadevne strani, kot je na primer načelo kakovosti ali obveznost poštene in zakonite obdelave ter obveznost varovanja zaupnosti podatkov in njihove varne hrambe. Glede na to, da v različici Sveta ni nobenega sklicevanja na veljavna načela varstva podatkov, ki določajo roke za hrambo informacij, oziroma na to, da v členu niso določeni nobeni tozadevni specifični roki, bi bilo mogoče to različico razumeti tudi tako, da dopušča zbiranje in obdelavo podatkov o prometu iz varnostnih razlogov za nedoločen čas.

84. V nekaterih delih besedila je Svet poleg tega predvidel manj zavezujoče določbe o varovanju zasebnosti, saj je uporabljena bolj splošna formulacija. V njem na primer ni več sklicevanja na „*zakoniti interes upravljavca podatkov*“, kar zbuja dvom glede vrst subjektov, ki bi lahko izkoristili to izjemo. Nadvse pomembno je, da se vsem uporabnikom ali pravnim osebam prepreči, da bi se s to spremembo okoristili.

85. Nedavne izkušnje v Evropskem parlamentu in Svetu so pokazale, da je s predpisi težko določiti obseg in pogoje za zakonito obdelavo podatkov iz varnostnih razlogov. Le malo verjetno je, da bi se bilo mogoče s kakršnim koli obstoječim ali bodočim členom izogniti tveganju zaradi preširoke uporabe navedene izjeme iz kakršnih koli drugih razlogov, ki niso izključno varnostni; ravno tako se ne bi bilo mogoče izogniti temu, da bi izjemo izkoristili subjekti, ki do tega sicer niso upravičeni. To pa še ne pomeni, da podatkov sploh ne bi smeli obdelovati na ta način. Toda možnosti za tako obdelavo in obseg njene izvedbe bi bilo morda lažje oceniti na ravni izvajanja. Subjekti, ki bi želeli obdelovati podatke na ta način, bi se morali o področju uporabe in pogojih posvetovati z organi za varstvo podatkov in po možnosti z Delovno skupino iz člena 29. Druga možnost pa je, da se v Direktivo o zasebnosti in elektronskih komunikacijah vnese člen, ki bi dopuščal obdelavo podatkov o prometu iz varnostnih razlogov, za kar pa bi bilo potrebno tudi izrecno dovoljenje organov za varstvo podatkov.

86. ENVP je ob upoštevanju tveganja, ki ga člen 6(6)(a) predstavlja za temeljno pravico do varstva podatkov in zasebnosti posameznikov, ter dejstva, da je ta člen (kakor je obrazloženo v tem mnenju) s pravnega vidika nepotreben, zato sklenil, da bi bila najboljša rešitev črtanje celotnega predlaganega člena.

87. Če bi bilo kljub nasprotnemu priporočilu ENVP vseeno sprejeto kakršno koli besedilo po vzoru katere koli od trenutnih različic člena 6(6)(a), bi moralo v vsakem primeru vsebovati prej navedene zaščitne ukrepe glede varstva podatkov. Ravno tako bi ga bilo treba tudi primerno vključiti v sedanji člen 6, po možnosti kot nov odstavek 2(a).

V. **MOŽNOST PRAVNIH OSEB, DA UKREPAJO OB KRŠITVAH DIREKTIVE O ZASEBNOSTI IN ELEKTRONSKIH KOMUNIKACIJAH**

88. Evropski parlament je sprejel spremembo št. 133, ki ponudnikom dostopa do interneta in drugim pravnim osebam, kot so združenja potrošnikov, omogoča, da lahko sprožijo sodni postopek zaradi kršitve katere koli določbe Direktive o zasebnosti in elektronskih komunikacijah ([19]). Vendar te spremembe Komisija in Svet nista sprejela. ENVP meni, da gre za izredno dobrodošlo spremembo in priporoča, da se jo ohrani.

89. Da bi lahko dojeli, kako pomembna je ta sprememba, je treba vedeti, da škoda, ki je na področju zasebnosti in varstva podatkov povzročena posamezniku, ponavadi ni zadosten razlog za uvedbo sodnega postopka. Posamezniki običajno ne gredo na sodišče, če so prejeli neželeno elektronsko pošto ali če je bilo njihovo ime pomotoma vneseno v imenik. Ta sprememba bi združenjem potrošnikov in sindikatom, ki zastopajo skupne interese potrošnikov, omogočila, da v njihovem imenu sprožijo sodni postopek. Tudi raznovrstnejši mehanizmi uveljavljanja bi po vsej verjetnosti pripomogli k boljši usklajenosti, s tem pa k učinkoviti uporabi določb Direktive o zasebnosti in elektronskih komunikacijah.

90. Pravni okviri nekaterih držav članic vključujejo pravne precedense, na podlagi katerih je že predvidena možnost kolektivnega pravnega sredstva; z njim naj bi potrošnikom oziroma interesnim skupinam omogočili, da lahko od strani, ki jim je povzročila škodo, zahtevajo nadomestilo.

91. V drugih državah članicah imajo poleg tega potrošniki in interesne skupine (ter *prizadeti konkurent*) v skladu s predpisi o konkurenci ([20]) pravico, da lahko vložijo tožbo proti kršitelju. Podjetja, ki kršijo predpise o konkurenci, se bodo namreč s tem najbrž okoristila, saj se potrošniki, ki so utrpeli le manjšo škodo, ponavadi le stežka odločajo za tožbo. To utemeljitev bi lahko smiselno uporabili tudi na področju varstva podatkov in zasebnosti.

92. Kot je bilo že navedeno, pa je še bolj pomembno, da lahko pravne osebe, kot so združenja potrošnikov in PPECS, vložijo tožbo, saj je s tem položaj potrošnikov močnejši, spodbuja pa se tudi splošna skladnost z zakonodajo o varstvu podatkov. Če podjetjem, ki kršijo predpise, grozi večja verjetnost tožbe, si bodo najbrž bolj prizadevala za skladnost z zakonodajo o varstvu podatkov, kar bo dolgoročno izboljšalo spoštovanje zasebnosti in varstvo potrošnikov. ENVP zato glede na vse navedeno poziva Evropski parlament in Svet, naj sprejmeta določbo, ki bo pravnim osebam omogočala, da lahko sprožijo sodni postopek zaradi kršitve katere koli določbe Direktive o zasebnosti in elektronskih komunikacijah.

VI. **SKLEP**

93. Skupno stališče Sveta, besedilo Evropskega parlamenta iz prve obravnave in spremenjeni predlog Komisije vsebujejo bolj ali manj pozitivne elemente, ki bi pripomogli k boljši zaščiti zasebnosti posameznikov in njihovih osebnih podatkov.

94. Toda ENVP meni, da še vedno obstajajo možnosti za izboljšave, zlasti kar zadeva skupno stališče Sveta, iz katerega so bile, žal, črtane nekatere spremembe, ki jih je predlagal Evropski parlament, da bi s tem pripomogel k ustrezni zaščiti zasebnosti posameznikov in njihovih osebnih podatkov. Zato poziva Evropski parlament in Svet, naj ponovno uvedeta zaščitne ukrepe glede zasebnosti, ki jih je Parlament sprejel v prvi obravnavi.

95. ENVP poleg tega meni, da bi bilo treba racionalizirati nekatere določbe direktive. Še zlasti to velja za določbe o kršitvah varnosti; ENVP je namreč mnenja, da bodo vse prednosti uradnega obvestila o kršitvi najbolj prišle do izraza, če bo že v zasnovi ustrezno določen pravni okvir. ENVP pa tudi meni, da bi bilo treba izboljšati in pojasniti formulacijo nekaterih določb navedene direktive.

96. Glede na navedeno ENVP poziva Evropski parlament in Svet, naj si še bolj prizadevata, da bodo posamezne določbe Direktive o zasebnosti in elektronskih komunikacijah bolje in jasneje formulirane, hkrati pa poskrbita tudi za to, da bodo znova uvedene spremembe, ki jih je Evropski parlament sprejel v prvi obravnavi in katerih namen je zagotoviti ustrezno raven zasebnosti in varstva podatkov. V točkah 97, 98, 99 in 100 v nadaljevanju so povzeta vsa odprta vprašanja; navedena pa so tudi nekatera priporočila in predlagane določene rešitve. ENVP poziva vse udeležene strani, naj jih upoštevajo pri dokončnem sprejetju direktive o zasebnosti in elektronskih komunikacijah.

Kršitev varnosti

97. Evropski parlament, Komisija in Svet so sprejeli različne pristope glede uradnega obveščanja o kršitvi varnosti. Navedeni trije modeli se med drugim razlikujejo glede subjektov, za katere velja ta obveznost, standarda oziroma povoda za uradno obvestilo, posameznikov, na katere se nanašajo osebni podatki in so upravičeni do obvestila itd. Evropski parlament in Svet morata storiti vse, kar je v njuni moči, in oblikovati zanesljiv pravni okvir v zvezi s kršitvami varnosti. Zato bi morala:

([19]) Člen 13(6) – prva obravnava v Evropskem parlamentu.

([20]) Glej na primer člen 8 nemškega zakona o nepošteni konkurenci (*Gesetz gegen den unlauteren Wettbewerb* – UWG).

— v besedilih Evropskega parlamenta, Sveta in Komisije *pustiti nespremenjeno* opredelitev kršitve varnosti, saj je ta dovolj široka, da zajame večino situacij, v katerih bi bila potrebno uradno obvestilo o kršitvi varnosti;

— kar zadeva subjekte, za katere naj bi veljala predlagana zahteva glede uradnega obvestila, *vključiti* ponudnike storitev informacijske družbe. Spletni trgovci na drobno, spletne banke in spletne lekarne so ravno tako izpostavljeni kršitvam varnosti kot telekomunikacijska podjetja, če ne še v večji meri. Državljani pričakujejo, da bodo obveščeni ne le o kršitvah varnosti, ki jih utrpijo ponudniki dostopa do interneta, temveč zlasti, kadar se to zgodi spletnim bankam in lekarnam;

— kar zadeva povod za uradno obvestilo, je standard iz spremenjenega predloga, tj. *da je dokaj verjetno, da bodo [podatki] ogroženi*, ustrezno, saj zagotavlja funkcionalnost sistema. Treba pa je zagotoviti, da je „škoda" dovolj široko opredeljena, da zajema vse vidike negativnih posledic na zasebnost ali druge zakonite interese posameznikov. Sicer bi bilo sicer bolje oblikovati novo opredelitev, v skladu s katero bi bilo obveščanje obvezno, *„če je mogoče upravičeno pričakovati, da bo kršitev škodovala posameznikom"*. V predlogu Sveta je zahteva, da ima kršitev *resne* posledice za zasebnost posameznika; glede na zahtevo, da mora kršitev imeti „resne" posledice, s takšnim pristopom ne bi bila zagotovljena ustrezna zaščita posameznikov, hkrati pa bi vplival na objektivnost presoje.

— vključitev ustreznega organa, ki naj bi odločil o tem, ali mora zadevni subjekt obvestiti posameznike, ima zagotovo tudi pozitivne strani, vendar se lahko zgodi, da ta rešitev ne bo praktična in jo bo težko uveljavljati ter da bo povzročila preusmeritev sredstev, ki so sicer namenjena za druge pomembne prioritete. ENVP se boji, da v primeru, če oblasti ne bodo zmožne izredno hitre reakcije, tak sistem lahko celo oslabi varstvo posameznikov in po nepotrebnem obremeni organe oblasti. ENVP zato na splošno svetuje, da se *vzpostavi* sistem, na podlagi katerega zadevni subjekti sami ocenijo, ali je uradno obvestilo potrebno ali ne;

— da bi organom omogočili preverjanje ocen, ki jih zadevni subjekti pripravijo v zvezi s tem, ali je uradno obvestilo potrebno ali ne, *uvesti* naslednje zaščitne ukrepe:

  — *zagotoviti*, da so takšni subjekti zavezani organe oblasti uradno obvestiti o vseh kršitvah, ki izpolnjujejo predpisani standard;

  — *poskrbeti*, da imajo organi oblasti vlogo nadzornika, kar jim omogoča selektivnost, s tem pa učinkovitost. Da bi to tudi dosegli, se v besedilo vnese naslednji stavek: *„Če naročnik ali posameznik, na katerega se podatki nanašajo, še ni bil obveščen o kršitvi, lahko pristojni nacionalni organ po preučitvi zadeve zahteva od PPECS ali ISSP, da pošlje obvestilo."*

  — *sprejeti* novo določbo, ki bi subjekte zavezovala k beleženju podrobne in celovite revizijske sledi v podjetju. To bi bilo mogoče doseči s sprejetjem naslednje formulacije: *„PPECS in ponudniki storitev informacijske družbe vodijo in hranijo celovite evidence, v katerih so podrobno navedene vse kršitve, z njimi povezane tehnične informacije in ukrepi za izboljšanje. V evidencah so zabeležena tudi vsa obvestila naročnikom ali zadevnim posameznikom ter pristojnim nacionalnim organom, vključno z datumom in vsebino. Evidence se na zahtevo predložijo pristojnemu nacionalnemu organu."*

— da se zagotovi doslednost pri izvajanju okvira v zvezi s kršitvami varnosti, *poskrbeti*, da lahko Komisija po posvetovanju z ENVP, delovno skupino iz člena 29 in drugimi zainteresiranimi stranmi sprejme tehnične izvedbene ukrepe;

— kar zadeva posameznike, ki bi jih bilo treba obvestiti o kršitvi, *uporabiti* terminologijo Komisije ali Evropskega parlamenta, torej „zadevni posamezniki" oziroma „prizadeti uporabniki", saj vključuje vse posameznike, katerih osebni podatki so bili ogroženi.

Javno dostopna zasebna omrežja

98. Javnost ima pogosteje kot prek javnih omrežij dostop do komunikacijskih storitev prek omrežij, s katerimi upravljajo zasebniki (npr. zaščiteni brezžični dostop (*Wi-Fi*) v hotelih in na letališčih), ti pa v direktivi niso zajeti. Evropski parlament je sprejel spremembo št. 121 (člen 3), ki področje uporabe direktive razširja na javna in zasebna komunikacijska omrežja pa tudi javno dostopna zasebna omrežja. Evropski parlament in Svet bi zato morala:

— *ohraniti* bistveni del spremembe št. 121, vendar jo *preoblikovati*, tako da bo področje uporabe direktive o zasebnosti in elektronskih komunikacijah zajemalo le *„obdelavo osebnih podatkov v zvezi z zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev v javnih ali javno dostopnih zasebnih komunikacijskih omrežjih v Skupnosti"*. Omrežja, s katerimi upravljajo izključno zasebniki (za razliko od javno dostopnih zasebnih omrežij) v direktivi ne bi bila izrecno zajeta;

— ustrezno *spremeniti* različne izvedbene določbe v zvezi z javnimi omrežji, da se bodo izrecno nanašale tudi na javno dostopna zasebna omrežja;

— *vključiti* spremembo, s katero se opredeli, da *„javno dostopno zasebno omrežje pomeni omrežje, s katerim upravljajo zasebniki in do katerega ima širša javnost praviloma neomejen dostop, in sicer proti plačilu ali zastonj oziroma v povezavi z drugimi storitvami ali ponudbami ter ob upoštevanju veljavnih pogojev“*. Za subjekte, ki naj bi jih zajemalo novo področje uporabe, bo to pomenilo dodatno pravno varnost;

— *sprejeti* novo uvodno izjavo, ki bo Komisiji omogočila izvedbo javnega posvetovanja glede uporabe Direktive o zasebnosti in elektronskih komunikacijah za vsa zasebna omrežja, pri čemer bi sodelovali tudi ENVP, delovna skupina iz člena 29 ter druge zadevne zainteresirane strani. V njej bi lahko pojasnili, da bi morala Komisija po opravljenem javnem posvetovanju predlagati ustrezno vključitev novih vrst subjektov, ki bi jih morala zajemati direktiva o zasebnosti in elektronskih komunikacijah, oziroma njihovo omejitev.

Obdelava podatkov o prometu iz varnostnih razlogov

99. Evropski parlament je na prvi obravnavi sprejel spremembo št. 181 (člen 6(6)(a)), ki dovoljuje obdelovanje podatkov o prometu iz varnostnih razlogov. Svet je v skupnem stališču sprejel nov pristop, v katerem so nekateri zaščitni ukrepi glede zasebnosti nekoliko manj strogi. ENVP zato Evropskemu parlamentu in Svetu priporoča, naj:

— ta člen v celoti *zavrneta*, ker je nepotreben, obstaja pa tudi nevarnost zlorabe, kar bi lahko preveč ogrozilo varstvo podatkov in zasebnost posameznikov;

— če bi bila kljub temu sprejeta katera od različic po vzoru sedanjega besedila člena 6(6)(a), vanj *vključita* zaščitne ukrepe glede varstva podatkov, obravnavane v tem mnenju (po vzoru ukrepov iz spremembe, ki jo je predlagal Evropski parlament).

Ukrepi v zvezi s kršitvami Direktive o zasebnosti in elektronskih komunikacijah

100. Evropski parlament je sprejel spremembo št. 133 (člen 13(6)), ki pravnim osebam omogoča, da lahko sprožijo sodni postopek zaradi kršitve katere koli določbe navedene direktive. Toda Svet te spremembe, žal, ni podprl. Svet in Evropski parlament bi morala:

— *odobriti* določbo, ki pravnim osebam, kot so združenja potrošnikov in poslovna združenja, omogoča, da lahko sprožijo sodni postopek zaradi kršitve katere koli določbe navedene direktive (in ne le zaradi kršitve določb o neželeni elektronski pošti, kakor je trenutno določeno v skupnem stališču in spremenjenem predlogu). Raznovrstnejši mehanizmi uveljavljanja bodo pripomogli k boljši usklajenosti, s tem pa k učinkoviti uporabi določb celotne Direktive o zasebnosti in elektronskih komunikacijah.

Reševanje izziva

101. Evropski parlament in Svet morata pri vseh navedenih vprašanjih najti odgovor na vprašanje, kako oblikovati ustrezna pravila in določbe, ki bodo izvedljivi, funkcionalni in v katerih bosta upoštevani pravica do zasebnosti ter pravica do varstva podatkov posameznikov. ENVP pričakuje, da si bodo vse udeležene strani po svojih najboljših močeh prizadevale, da bi rešile ta izziv, in upa, da bo k temu prispevalo tudi to mnenje.

V Bruslju, 9. januarja 2009

Peter HUSTINX

Evropski nadzornik za varstvo podatkov

Mnenje Evropskega nadzornika za varstvo podatkov o predlogu Direktive Sveta o obveznosti držav članic glede vzdrževanja minimalnih zalog surove nafte in/ali naftnih derivatov

(2009/C 128/05)

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV JE –

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

ob upoštevanju Listine Evropske unije o temeljnih pravicah in zlasti člena 8 te 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 ter zlasti člena 41 te uredbe ([2]),

ob upoštevanju prošnje za mnenje v skladu s členom 28(2) Uredbe (ES) št. 45/2001, ki jo je prejel 14. novembra 2008 –

SPREJEL NASLEDNJE MNENJE:

I. UVOD

1. Komisija je 13. novembra 2008 sprejela predlog direktive Sveta o obveznosti držav članic glede vzdrževanja minimalnih zalog surove nafte in/ali naftnih derivatov (v nadaljnjem besedilu: predlog) ([3]).

2. Namen direktive je zagotoviti visoko stopnjo varnosti oskrbe z nafto v Skupnosti z zanesljivimi in preglednimi mehanizmi, ki temeljijo na solidarnosti med državami članicami, za vzdrževanje minimalnih zalog nafte ali naftnih derivatov in za vzpostavitev proceduralnih sredstev, potrebnih za odpravljanje morebitnega resnega pomanjkanja.

3. Komisija je predlog 14. novembra 2008 poslala ENVP, da bi se z njim posvetovala v skladu s členom 28(2) uredbe (ES) št. 45/2001. ENVP je zadovoljen, da je bil v skladu s členom 28 uredbe (ES) št. 45/2001 zaprošen za mnenje o tem vprašanju, in ugotavlja, da je to posvetovanje omenjeno v preambuli predloga.

4. Komisija se je pred sprejetjem predloga neuradno posvetovala z ENVP o enem členu osnutka predloga (tj. sedanjem členu 19). ENVP je bil zadovoljen, da se je Komisija z njim neuradno posvetovala, saj je zaradi tega lahko dal nekaj priporočil, še preden je Komisija sprejela predlog.

II. ANALIZA PREDLOGA

Splošna analiza

5. Iz vprašanja, ki ga načenja predlog Komisije, je dobro razvidno, da je treba predpise o varstvu podatkov vedno upoštevati. V primeru držav članic in njihove obveznosti, da vzdržujejo varnostne zaloge nafte, ki so pretežno v lasti pravnih oseb, morda ni očitno, da bi se osebni podatki lahko obdelovali, vendar se ti lahko obdelujejo, čeprav to ni bilo predvideno. Vsekakor je treba preveriti, kolikšna je verjetnost, da se bodo osebni podatki obdelovali, in temu ustrezno ukrepati.

6. Trenutno sta v direktivi predvideni dve dejavnosti, pri katerih bi lahko prišlo do obdelave podatkov. Prva je zbiranje informacij o naftnih zalogah s strani držav članic in kasnejše pošiljanje teh informacij Komisiji. Druga je povezana s pristojnostjo Komisije za izvajanje nadzornih ukrepov v državah članicah. Med informacijami, ki bi se zbirale o lastnikih naftnih zalog, bi bili lahko osebni podatki, kot so imena in kontaktni podatki direktorjev podjetij. Zbiranje in kasnejše pošiljanje podatkov Komisiji bi v tem primeru pomenilo obdelavo osebnih podatkov, zaradi česar bi se morala uporabiti bodisi nacionalna zakonodaja, s katero so bile prenesene določbe direktive 95/46/ES, bodisi uredba (ES) št. 45/2001, odvisno od tega, kdo bi dejansko obdeloval podatke. Osebni podatki bi se lahko zbirali in potemtakem obdelali tudi zato, ker bi imela Komisija pristojnost za izvajanje nadzora nad varnostnimi zalogami, kar vključuje tudi pristojnost za splošno zbiranje podatkov.

([1]) UL L 281, 23.11.1995, str. 31.
([2]) UL L 8, 12.1.2001, str. 1.
([3]) COM(2008) 775 konč.

7. V okviru neuradnega posvetovanja, v katerem so bile obravnavane le določbe o pooblastilu Komisije za nadzor, je ENVP svetoval Komisiji, naj ugotovi, ali bi bila obdelava osebnih podatkov v okviru nadzora Komisije le naključna, ali bi do nje redno prihajalo in bi služila namenom nadzora. Glede na končne ugotovitve Komisije sta bila predlagana dva pristopa.

8. Če obdelava osebnih podatkov ni načrtovana in bi bila torej povsem naključna, je ENVP priporočil, naj se, prvič, izrecno izključi možnost, da bi obdelava osebnih podatkov služila namenom nadzora s strani Komisije, in naj se, drugič, izjavi, da se osebni podatki, na katere bo Komisija naletela med nadzorom, ne bodo zbirali ali upoštevali in da bodo v primeru naključnega zbiranja takoj izbrisani. ENVP je kot dodatno varovalko predlagal tudi vključitev določbe, da direktiva ne posega v predpise o varstvu podatkov, določenimi z direktivo 95/46/ES in uredbo (ES) št. 45/2001.

9. Če pa je predvideno, da se bodo podatki v okviru nadzora, ki ga opravlja Komisija, redno obdelovali, je ENVP priporočil Komisiji, naj vključi besedilo, iz katerega bi bilo razvidno, da so zahteve po varstvu podatkov ustrezno upoštevane. Vključeni bi morali biti naslednji elementi: (I) dejanski namen obdelave podatkov, (II) nujnost obdelave podatkov za uresničitev tega namena in (III) sorazmernost pri obdelavi podatkov.

10. Čeprav se je neuradno priporočilo ENVP nanašalo le na pristojnost Komisije za nadzor, so njegove pripombe relevantne tudi za drugo glavno dejavnost, predvideno v predlagani direktivi, tj. zbiranje informacij s strani držav članic in njihovo pošiljanje Komisiji.

11. Iz končnega predloga Komisije je jasno razvidno, da po mnenju Komisije za namene direktive ni predvidena nikakršna obdelava podatkov. ENVP je zadovoljen, da je bil predlagani prvi pristop v celoti upoštevan v predlogu.

12. ENVP se zato strinja z načinom, s katerim je Komisija zagotovila spoštovanje predpisov o varstvu podatkov v predlagani direktivi. V nadaljevanju bodo predstavljena samo nekatera priporočila glede posameznih vidikov predloga.

Opombe k posameznim vidikom predloga

13. Člen 15 predlagane direktive ureja obveznost držav članic, da Komisiji pošiljajo tedenska statistična poročila o količini komercialnih zalog na svojem državnem ozemlju. Te informacije naj navadno ne bi vsebovale veliko osebnih podatkov. Lahko pa bi vsebovale podatke o fizičnih osebah, ki imajo v lasti naftne zaloge ali ki so zaposlene pri pravni osebi, ki ima v lasti naftne zaloge. Da države članice ne bi pošiljale takšnih informacij Komisiji, odstavek 1 člena 15 določa, da v primeru takšnih informacij, „ne omenjajo imen lastnikov zadevnih zalog“. Čeprav se je treba zavedati, da nenavedba imena ne pomeni vedno, da se na podlagi podatkov ne more izslediti fizične osebe, se zdi, da bo v tem primeru (statistična poročila o količini naftnih zalog) že s tem dodanim stavkom mogoče zagotoviti, da Komisiji ne bi bili poslani nobeni osebni podatki.

14. Pristojnost Komisije za nadzor je določena s členom 19 predlagane direktive. Iz tega člena je jasno razvidno, da se je Komisija odločila za prvi pristop, opisan v 8. točki. Določa, da namen nadzornih ukrepov, ki jih izvaja Komisija, ni obdelava osebnih podatkov. Če pa Komisija naleti na takšne podatke, jih ne sme upoštevati in jih mora, če so bili zbrani slučajno, izbrisati. Da bi besedilo uskladili z besedilom zakonodaje o varstvu podatkov in se izognili nesporazumom, ENVP predlaga, da se beseda „zbiranja“ v prvem stavku odstavka 2 nadomesti z besedo „obdelave“.

15. ENVP je zadovoljen, da je bila kot splošna varovalka v predlog vključena tudi relevantna zakonodaja o varstvu podatkov. V členu 20 so države članice in Komisija ter drugi organi Skupnosti jasno opozorjeni na obveznosti, ki jih imajo v skladu z direktivo 95/46/ES in uredbo (ES) št. 45/2001. V določbi so tudi izpostavljene pravice, ki jih imajo subjekti v skladu s temi predpisi, kot so pravica, da ugovarjajo obdelavi svojih podatkov, pravico do dostopa do svojih podatkov in pravica do popravka svojih podatkov, če so netočni. ENVP ima pripombo le glede umestitve te določbe v predlogu. Ker je splošna, se ne nanaša le na pristojnost Komisije za nadzor. Zato ENVP predlaga, da se ta člen prenese v prvi del direktive, na primer za člen 2.

16. Direktiva 95/46/ES in uredba (ES) št. 45/2001 sta omenjeni tudi v uvodni izjavi 25, katere namen pa ni najbolj jasen, saj je v njej zakonodaja o varstvu podatkov omenjena brez kakršnih koli drugih navedb. V uvodni izjavi bi moralo biti jasno zapisano, da določbe direktive ne posegajo v navedeno zakonodajo. Poleg tega bi se iz zadnjega stavka uvodne izjave lahko sklepalo, da zakonodaja o varstvu podatkov izrecno določa, da morajo nadzorniki takoj uničiti naključno zbrane podatke. Čeprav je to na podlagi določb povsem mogoče, ta zakonodaja takšne obveznosti ne določa. Splošno načelo varstva podatkov je, da se osebni podatki ne hranijo dlje, kot je to potrebno za namene, za katere so bili zbrani ali nadalje obdelani. Če bi se uvodna izjava spremenila, kot se predlaga, bi bil

zadnji stavek odveč. Zato ENVP predlaga, da se zadnji stavek uvodne izjave 25 črta.

III. **SKLEP**

17. ENVP se strinja z načinom, s katerim je Komisija zagotovila spoštovanje predpisov o varstvu podatkov v predlagani direktivi.

18. Glede posameznih vidikov predloga pa ENVP predlaga:

— da se beseda „zbiranja“ v prvem stavku člena 19(2) nadomesti z besedo „obdelave“;

— da se člen 20, ki je splošna določba o varstvu podatkov, prenese v prvi del direktive, in sicer takoj za člen 2;

— da se v uvodni izjavi 25 doda, da določbe te direktive ne posegajo v določbe direktive 95/46/ES in uredbe (ES) št. 45/2001;

— da se črta zadnji stavek uvodne izjave 25.

V Bruslju, 3. februarja 2009

Peter HUSTINX

Evropski nadzornik za varstvo podatkov

IV

(Informacije)

INFORMACIJE INSTITUCIJ IN ORGANOV EVROPSKE UNIJE

KOMISIJA

Menjalni tečaji eura [1]

5. junija 2009

(2009/C 128/06)

1 euro =

	Valuta	Menjalni tečaj		Valuta	Menjalni tečaj
USD	ameriški dolar	1,4177	AUD	avstralski dolar	1,7606
JPY	japonski jen	137,48	CAD	kanadski dolar	1,5657
DKK	danska krona	7,4472	HKD	hongkonški dolar	10,9887
GBP	funt šterling	0,87920	NZD	novozelandski dolar	2,2263
SEK	švedska krona	10,9250	SGD	singapurski dolar	2,0530
CHF	švicarski frank	1,5191	KRW	južnokorejski won	1 768,65
ISK	islandska krona		ZAR	južnoafriški rand	11,4189
NOK	norveška krona	8,9700	CNY	kitajski juan	9,6871
BGN	lev	1,9558	HRK	hrvaška kuna	7,3550
CZK	češka krona	27,003	IDR	indonezijska rupija	14 078,75
EEK	estonska krona	15,6466	MYR	malezijski ringit	4,9556
HUF	madžarski forint	289,10	PHP	filipinski peso	67,016
LTL	litovski litas	3,4528	RUB	ruski rubelj	43,5789
LVL	latvijski lats	0,7094	THB	tajski bat	48,464
PLN	poljski zlot	4,5420	BRL	brazilski real	2,7345
RON	romunski leu	4,2185	MXN	mehiški peso	18,7066
TRY	turška lira	2,1834	INR	indijska rupija	66,7910

[1] *Vir*: referenčni menjalni tečaj, ki ga objavlja ECB.

POPRAVKI

Popravek obrestne mere, ki jo Evropska centralna banka uporablja v svojih glavnih refinančnih operacijah

(Uradni list Evropske unije C 124 z dne 4. junija 2009)

(2009/C 128/07)

Stran 1 in naslovnica:

besedilo: „1,00 % 4. junija 2009“

se glasi: „1,00 % 1. junija 2009“.

Cena naročnine 2009 (brez DDV, skupaj s stroški pošiljanja z navadno pošto)

Uradni list EU, seriji L + C, samo papirna različica	22 uradnih jezikov EU	1 000 EUR na leto (*)
Uradni list EU, seriji L + C, samo papirna različica	22 uradnih jezikov EU	100 EUR na mesec (*)
Uradni list EU, seriji L + C, papirna različica + letni CD-ROM	22 uradnih jezikov EU	1 200 EUR na leto
Uradni list EU, serija L, samo papirna različica	22 uradnih jezikov EU	700 EUR na leto
Uradni list EU, serija L, samo papirna različica	22 uradnih jezikov EU	70 EUR na mesec
Uradni list EU, serija C, samo papirna različica	22 uradnih jezikov EU	400 EUR na leto
Uradni list EU, serija C, samo papirna različica	22 uradnih jezikov EU	40 EUR na mesec
Uradni list EU, seriji L + C, mesečni zbirni CD-ROM	22 uradnih jezikov EU	500 EUR na leto
Dopolnilo k Uradnemu listu (serija S – razpisi za javna naročila), CD-ROM, 2 izdaji na teden	Večjezično: 23 uradnih jezikov EU	360 EUR na leto (= 30 EUR na mesec)
Uradni list EU, serija C – natečaji	Jezik(-i) v skladu z natečajem(-i)	50 EUR na leto

(*) Prodaja po številki:
— do 32 strani: 6 EUR
— od 33 do 64 strani: 12 EUR
— več kot 64 strani: cena se določi glede na posamezen primer

Naročilo na *Uradni list Evropske unije*, ki izhaja v uradnih jezikih Evropske unije, je na voljo v 22 jezikovnih različicah. Uradni list je sestavljen iz serije L (Zakonodaja) in serije C (Informacije in objave).

Na vsako jezikovno različico se je treba naročiti posebej.

V skladu z Uredbo Sveta (ES) št. 920/2005, objavljeno v Uradnem listu L 156 z dne 18. junija 2005, institucije Evropske unije začasno niso obvezane sestavljati in objavljati vseh pravnih aktov v irščini, zato se Uradni list v irskem jeziku objavlja posebej.

Naročilo na Dopolnilo k Uradnemu listu (serija S – razpisi za javna naročila) zajema vseh 23 uradnih jezikovnih različic na enem večjezičnem CD-ROM-u.

Na zahtevo nudi naročilo na *Uradni list Evropske unije* pravico do prejemanja različnih prilog k Uradnemu listu. Naročniki so o objavi prilog obveščeni v „Obvestilu bralcu“, vstavljenem v *Uradni list Evropske unije*.

Prodaja in naročila

Plačljive publikacije, ki jih izdaja Urad za publikacije, so na voljo pri naših komercialnih distributerjih. Seznam komercialnih distributerjev je na spletnem naslovu:

http://publications.europa.eu/others/agents/index_sl.htm

EUR-Lex (http://eur-lex.europa.eu) nudi neposreden in brezplačen dostop do prava Evropske unije. Ta spletna stran omogoča pregled *Uradnega lista Evropske unije*, zajema pa tudi pogodbe, zakonodajo, sodno prakso in pripravljalne akte za zakonodajo.

Za boljše poznavanje Evropske unije preglejte spletno stran http://europa.eu

Urad za publikacije
Publications.europa.eu

URAD ZA URADNE PUBLIKACIJE EVROPSKIH SKUPNOSTI
L-2985 LUXEMBOURG

SL