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