

# EVROPSKI NADZORNIK ZA VARSTVO PODATKOV

## Mnenje Evropskega nadzornika za varstvo podatkov o Predlogu okvirnega sklepa Sveta o izmenjavi informacij v skladu z načelom dostopnosti (COM (2005) 490 konč.)

(2006/C 116/04)

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV JE —

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

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

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

ob upoštevanju zaprosila za mnenje v skladu s členom 28(2) 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 —

SPREJEL NASLEDNJE MNENJE:

### I. PREDHODNE OPOMBE

1. Komisija je Evropskemu nadzorniku za varstvo podatkov (EDPS) s pismom z dne 12. oktobra 2005 posredovala Predlog okvirnega sklepa Sveta o izmenjavi informacij v skladu z načelom dostopnosti. Evropski nadzornik za varstvo podatkov (EDPS) je pismo razumel kot zaprosilo, da institucijam in organom Skupnosti svetuje v skladu s členom 28(2) Uredbe št. 45/2001/ES. Meni tudi, da je treba pričujoče mnenje navesti v preambuli Okvirnega sklepa.
2. To mnenje je treba razumeti v smislu okvira, opredeljenega v delu II. Kakor je navedeno v delu II, je zelo negotovo, če bo sedanji predlog – ali pristop k dostopnosti, ki ga predlog zavzema – nazadnje privedel do sprejetja pravnega instrumenta. Za druge pristope se zavzema precejšnje število držav članic.

3. Vendar pa je očitno, da je vprašanje dostopnosti informacij organov pregona preko notranjih meja – ali, bolj splošno, izmenjava teh informacij – v državah članicah zelo pomembno, tako v Svetu in zunaj njega ter v Evropskem parlamentu.
4. Prav tako je očitno, da je to vprašanje zelo pomembno z vidika varstva osebnih podatkov, kar bo ponazorilo pričujoče mnenje. EDPS opozarja, da je Komisija sedanji predlog predstavila v tesni povezavi s Predlogom okvirnega sklepa Sveta o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah, o katerem je EDPS podal mnenje 19. decembra 2005.
5. EDPS bo to mnenje izkoristil za predstavitev nekaj splošnih in bolj temeljnih vidikov o vprašanju izmenjave informacij organov pregona in o pristopih za urejanje tega vprašanja. EDPS namerava s predložitvijo tega mnenja zagotoviti, da bo vidik varstva podatkov v prihodnjih razpravah o tem vprašanju ustrezno upoštevan.
6. Posvetovanje z EDPS bo mogoče tudi pozneje, ko bo zakonodajni postopek o tem predlogu in ostalih predlogih na to temo ustrezno napredoval.

### II. OKVIR PREDLOGA

7. Načelo dostopnosti je bilo kakor pomembno novo zakonodajno načelo uvedeno v Haaškem programu. Na podlagi tega načela morajo informacije, ki so potrebne za boj proti kriminalu, neovirano prestopati notranje meje EU. Cilj sedanjega predloga je, da se to načelo izvede v zavezujočem pravnem instrumentu.
8. Izmenjava policijskih informacij med različnimi državami je priljubljena tema zakonodajalcev znotraj okvira EU in izven njega. Nedavno so naslednje pobude pritegnile pozornost EDPS.

9. Prvič – Švedska je 4. junija 2004 predložila Okvirni sklep o poenostavitvi izmenjave informacij in obveščevalnih podatkov med organi pregona držav članic Evropske unije. Svet je na seji 1. decembra 2005 dosegel dogovor o splošnem pristopu k temu predlogu.
10. Drugič – 27. maja 2005 je sedem držav članic v Prümu (Nemčija) podpisalo Konvencijo o okrepitvi čezmejnega sodelovanja, zlasti na področju boja proti terorizmu, čezmejnemu kriminalu in nezakonitemu preseljevanju. Konvencija je med drugim uvedla ukrepe za izboljšanje izmenjave informacij o DNK in prstnih odtisih. Konvenciji se lahko pridruži vsaka država članica Evropske unije. Namen pogodbenic je vključitev določb Konvencije v pravni okvir Evropske unije.
11. Tretjič – dostopnost informacij organov pregona preko notranjih meja Evropske unije bodo nadalje olajšali tudi drugi pravni instrumenti, kakor so predlogi o drugi generaciji Schengenskega informacijskega sistema (SIS II), predlog za dostop z namenom vpogleda v vizumski informacijski sistem (VIS) in Predlog okvirnega sklepa o izmenjavi podatkov, izpisanih iz kazenske evidence med državami članicami. V tem okviru je koristno omeniti tudi Sporočilo Komisije z dne 24. novembra 2005 o izboljšani učinkovitosti, povečani interoperabilnosti in sinergijah med evropskimi zbirkami podatkov na področju pravosodja in notranjih zadev.
12. Iz vseh teh pobud sledi, da se sedanji predlog okvirnega sklepa o dostopnosti ne sme preučiti ločeno, temveč je treba upoštevati tudi druge pristope na področju izmenjave informacij organov pregona. To je toliko bolj pomembno, saj daje sedanja težnja v Svetu prednost drugim pristopom na področju izmenjave informacij in zamisli o dostopnosti kakor splošnemu pristopu, ki ga je v sedanjem predlogu predlagala Komisija. O sedanjem besedilu predloga Svet morda sploh ne bo razpravjal.
13. Poleg tega je predlog tesno povezan s Predlogom okvirnega sklepa o varstvu osebnih podatkov. Sedanji predlog je treba razumeti v povezavi z bolj izčrpnim mnenjem o omenjenem okvirnem sklepu.
14. EDPS je v svojem mnenju o Predlogu okvirnega sklepa o varstvu osebnih podatkov poudaril pomen ustreznega varstva podatkov, kot nujno posledico pravnega instrumenta o dostopnosti. Meni, da se tak pravni instrument ne sme sprejeti brez osnovnih jamstev glede varstva podatkov.

15. Takšno je tudi stališče EDPS glede sprejetja drugih pravnih instrumentov, ki poenostavljajo pretok informacij organov pregona preko notranjih meja EU. EDPS zato pozdravlja dejstvo, da sta Svet in Evropski parlament prej omenjenemu predlogu okvirnega sklepa o varstvu osebnih podatkov namenila prednost.

### III. NAČELO DOSTOPNOSTI

16. Samo po sebi je načelo dostopnosti enostavno. Informacije, ki so dostopne nekaterim organom v državi članici, morajo biti na voljo tudi enakovrednim organom v drugih državah članicah. Informacije je treba med organi držav članic izmenjati kar se da hitro in enostavno ter predvsem z omogočanjem neposrednega spletnega dostopa.
17. Težave izhajajo iz pogojev, v katerih je treba načelo dostopnosti izvajati:
- Raznolika organizacija policije in sodstva v državah članicah z različnim ravnovesjem moči.
  - Vključene so različne vrste (občutljivih) informacij (kot so DNK in prstni odtisi).
  - Različni načini dostopa pristojnih organov do ustreznih informacij celo znotraj držav članic.
  - Zaradi jezikovnih razlik, razlik v tehnoloških (interoperabilnost) in pravnih sistemih je težko zagotoviti, da bodo informacije, ki izvirajo iz druge države članice, pravilno tolmačene.
  - To načelo je treba vključiti v obstoječ in obsežen sklop pravnih določb, ki obravnavajo izmenjavo informacij organov pregona med državami.
18. Ne glede na to zapleteno okolje je splošno znano, da načelo samo ne more delovati. Nujni so dodatni ukrepi, s katerimi bi se zagotovilo, da se informacije lahko učinkovito najdejo in ocenijo. Ti ukrepi morajo v vsakem primeru omogočiti, da organi pregona enostavneje ugotovijo, ali imajo organi pregona v drugih državah članicah na razpolago ustrezne informacije in kje je te ustrezne informacije mogoče najti. Takšne dodatne ukrepe bi lahko sestavljali vmesniki, ki omogočajo neposredni dostop do vseh ali do posebnih podatkov drugih držav članic. Zaradi tega uvaja predlog okvirnega sklepa o dostopnosti „indeksne podatke“, tj. posebne podatke, do katerih je mogoč neposreden dostop iz druge države.

19. Načelo dostopnosti mora na splošno olajšati pretok informacij med državami članicami. Notranje meje bodo odpravljene, države članice pa morajo omogočiti, da bodo informacije, ki so dostopne njihovim policijskim organom, vse bolj dostopne drugim organom. Države članice izgubijo pristojnost nad nadzorom pretoka informacij, kar se odraža tudi v dejstvu, da njihove nacionalne zakonodaje niso več zadostni instrumenti za primerno varstvo informacij.
20. Prav zaradi tega je treba z vidika varstva osebnih podatkov predlogu posvetiti posebno pozornost. Prvič – informacije, ki običajno veljajo za zaupne in dobro varovane, je treba posredovati organom v drugih državah članicah. Drugič – za delovanje sistema je treba oblikovati indeksne podatke in organom v drugih državah članicah omogočiti dostop do njih. Z izvajanjem tega načela bo posledično pridobljenih več podatkov, kakor jih je trenutno na voljo.
23. Predlog ne navaja, ali so „razpoložljive informacije“ zgolj informacije, ki jih pristojni organi že nadzorujejo, ali pa te vključujejo tudi informacije, ki jih ti organi lahko pridobijo. Vendar pa EDPS meni, da je predlog mogoče tolmačiti kakor, da sta zajeti obe vrsti informacij.
24. Medtem ko se zdi, da člen 2(2) predlaga ožje področje uporabe z navedbo, da Okvirni sklep „ne predvideva nobene obveznosti zbiranja in shranjevanja informacij [...] samo zato, da bi postale dostopne“, pa omogoča člen 3(a) širšo razlago, saj navaja, da „informacije“ pomenijo „obstoječe informacije iz Priloge II“.
25. Priloga II omenja vsaj dve kategoriji podatkov, ki jih navadno ne nadzoruje policija, temveč drugi organi. Prva kategorija so informacije o registraciji vozila. V številnih državah članicah zbirk podatkov, ki te informacije vsebujejo, organi pregona ne nadzorujejo, čeprav do teh zbirk redno dostopajo. Ali sodi ta vrsta informacij v področje uporabe „razpoložljivih informacij“, ki so v skladu s členom 1 na voljo enakovrednim pristojnim organom drugih držav članic? Druga kategorija podatkov iz Priloge II, ki jo je treba omeniti, so telefonske številke in drugi komunikacijski podatki: ali morajo ti podatki šteti za „razpoložljive“, čeprav jih ne nadzorujejo pristojni organi, temveč zasebna podjetja?

#### IV. GLAVNI ELEMENTI

##### Področje uporabe načela dostopnosti

21. Najprej je treba predvsem opredeliti, za katere vrste informacij velja načelo dostopnosti. Področje uporabe tega načela je splošno opredeljeno v členu 2 predloga, v povezavi s členom 1(1) in členom 3(a). Načelo velja za naslednje informacije:
- obstoječe informacije;
  - šest vrst informacij, opredeljenih v Prilogi II;
  - informacije, dostopne pristojnim organom.
- To so trije osnovni elementi področja uporabe načela iz predloga Komisije. Področje uporabe je nadalje izpopolnjeno v členu 2. Člen 2(1) omejuje uporabo načela dostopnosti na stopnjo pred začetkom sodnega pregona, medtem ko člen 2(2), (3) in (4) določa nekaj bolj posebnih omejitev.
22. Za razumevanje posledic predloga je potrebna bolj poglobljena analiza treh zgoraj navedenih osnovnih elementov. Prva dva elementa področja uporabe sta sama precej jasna. Opredelitev „obstojećih informacij“ je oblikovana v členu 2(2) in navaja, da okvirni sklep ne predvideva nobene obveznosti zbiranja in shranjevanja informacij samo zato, da bi postale dostopne, medtem ko seznama iz Priloge II ni mogoče tolmačiti na različne načine. Nadaljnjo pojasnitev pa potrebuje tretji osnovni element, sam in v povezavi s prvima dvema elementoma.
26. Poleg tega druge določbe predloga, zlasti člen 3(d) in člen 4(1)(c) predloga, podpirajo stališče, da lahko „imenovani organi“ in celo „imenovane strani“ nadzorujejo informacije, ki so „pristojnim organom“ „razpoložljive“. Iz besedila predloga tudi sledi, da „pristojni organ države članice pomeni organ iz prve alinee člena 29 Pogodbe EU, medtem ko je vsak nacionalni organ lahko „imenovani organ““.
27. EDPS meni, da zastavlja uporaba načela dostopnosti za informacije, ki jih nadzorujejo imenovani organi in imenovane strani, naslednja vprašanja:
- Ali zagotavlja člen 30(1)(b) zadostno pravno podlago, saj morajo imenovani organi in imenovane strani dati na voljo informacije, in sicer iz zbirk podatkov, ki ne sodijo v okvir tretjega stebra?
  - Ali se bo Okvirni sklep o varstvu osebnih podatkov uporabljal, kakor je predvideno npr. v členu 8 Predloga?
  - V kolikor ne, ali je obdelava v skladu z obveznostmi iz Direktive 95/46/ES?

28. Izvajanje tako širokega načela, kakor je „načelo dostopnosti“, zahteva jasno in natančno opredelitev podatkov, ki bodo šteli za razpoložljive. Evropski nadzornik za varstvo podatkov zato priporoča:

- pojasnitev področja uporabe;
- kot prvo možnost omejiti področje uporabe načela dostopnosti na informacije, ki jih nadzorujejo pristojni organi.
- kot drugo pa je v primeru širšega področja uporabe zagotoviti zadostna varovala za varstvo osebnih podatkov. Upoštevati je treba vprašanja, zastavljena v točki 27.

#### **Druga vprašanja, povezana s področjem uporabe**

29. V skladu s členom 2(1) Predloga se Okvirni sklep uporablja za obdelavo informacij pred začetkom sodnega pregona. Njegovo področje uporabe je bolj omejeno od področja uporabe Predloga okvirnega sklepa o varstvu osebnih podatkov, ki v celoti velja za pravosodno sodelovanje v kazenskih zadevah.

30. Vendar pa EDPS meni, da ta omejitev sama po sebi ne omejuje področja uporabe Predloga na policijsko sodelovanje. Vključeno bi lahko bilo tudi pravosodno sodelovanje v kazenskih zadevah, saj imajo pravosodni organi v več državah članicah pristojnosti tudi nad kazenskimi preiskavami pred začetkom sodnega pregona. Ker pa predlog temelji izključno na členu 30(1)(b) PEU, se zdi, da velja le za policijsko sodelovanje. Dobrodošla bi bila pojasnitev tega vidika.

31. Sedanji predlog velja za posredovanje informacij Europolu, medtem ko Predlog okvirnega sklepa o varstvu osebnih podatkov obdelavo podatkov s strani Europolu izključuje. EDPS svetuje, da se izmenjava informacij z Europolom omeji na namene samega Europolu, kakor je navedeno v členu 2 Konvencije o Europolu in v njeni Prilogi. Poleg tega je treba upoštevati natančna pravila za izmenjavo podatkov z Europolom, ki so že določena v več aktih Sveta.

#### **Brez novih zbirk podatkov, ki vsebujejo osebne podatke**

32. Izhodišče Predloga je, da ta ne bo vodil k oblikovanju novih zbirk podatkov, ki vsebujejo osebne podatke. Člen

2(2) je glede tega jasen: ne predvideva nobene obveznosti zbiranja in shranjevanja informacij samo zato, da bi postale dostopne. Z vidika varstva podatkov je to pomemben in pozitiven element predloga. EDPS opozarja na svoje mnenje o Predlogu direktive o hrabi podatkov, obdelanih v zvezi z zagotavljanjem javnih elektronskih komunikacij<sup>(1)</sup>, v katerem poudarja, da pravne obveznosti, zaradi katerih so nastale obsežne zbirke podatkov, predstavljajo posebno tveganje za zadevnega posameznika, zlasti v zvezi z nezakonito uporabo.

33. Vendar pa:

— Pomembno je zagotoviti, da predlog ne bo spodbujal neomejene medsebojne povezljivosti zbirk podatkov in posledično mreže zbirk podatkov, ki jo bo težko nadzorovati.

— Obstaja izjema v zgoraj navedenem izhodišču: člen 10 predloga, ki zagotavlja, da so indeksni podatki na voljo na spletu. Indeksni podatki lahko vsebujejo osebne podatke ali pa vsaj razkrijejo njihov obstoj.

#### **Neposredni in posredni dostop do informacij**

34. Predlog predvideva neposredni in posredni dostop do informacij. Člen 9 Predloga predvideva neposredni spletni dostop do informacij, ki jih vsebujejo zbirke podatkov, do katerih imajo ustrezni nacionalni organi neposredni spletni dostop. Člen 10 predvideva posredni dostop. Indeksni podatki informacij, ki niso spletno dostopne, so za spletni vpogled na voljo enakovrednim pristojnim organom drugih držav članic in Europolu. Če je vpogled v indeksne podatke uspešen, lahko ta organ izda zahtevo za informacije in jo pošlje imenovanemu organu, da pridobi informacije, opredeljene na podlagi indeksnih podatkov.

35. Neposredni dostop ne vodi do oblikovanja novih zbirk podatkov, temveč zahteva interoperabilnost zbirk podatkov enakovrednih pristojnih sistemov znotraj držav članic. Poleg tega bo nujno uvedel novo uporabo že obstoječih zbirk podatkov, saj bo vsem pristojnim organom držav članic zagotovil možnost, ki je bila do sedaj na voljo le nacionalnim pristojnim organom. Neposredni dostop bo samodejno pomenil, da bo imelo večje število oseb dostop do zbirke podatkov in zaradi tega je nevarnost zlorabe vse večja.

<sup>(1)</sup> Mnenje z dne 26. septembra 2005 o predlogu direktive Evropskega parlamenta in Sveta o hrabi podatkov, obdelanih v zvezi z zagotavljanjem javnih elektronskih komunikacijskih storitev, in spremembi Direktive 2002/58/ES (COM (2005) 438 konč.).

36. V primeru neposrednega dostopa s strani pristojnih organov druge države članice imenovani organi države članice izvora nimajo nadzora nad dostopom in nadaljnjo uporabo podatkov. To posledico neposrednega dostopa, kakor ga predvideva predlog, je treba primerno obravnavati, ker:

- se zdi, da razveljavlja pristojnosti imenovanih organov, da zavrnejo določbo o informacijah (iz člena 14);
- zastavlja vprašanja glede odgovornosti v zvezi s točnostjo in posodabljanjem podatkov po odobrenem dostopu do teh podatkov. Kako lahko imenovani organ države članice izvora zagotovi, da se podatki posodabljujejo?
- poleg tega, da imenovani organ ne more več izpolnjevati vseh svojih obveznosti iz zakona o varstvu podatkov, tudi nacionalni organ za varstvo podatkov države članice izvora podatkov ne more več nadzorovati izvajanja obveznosti, saj nima nobene pristojnosti do organov pregona drugih držav članic.
- Ti problemi še bolj prevladujejo v primeru dostopa do zbirk podatkov imenovanih organov in imenovanih strani, ki niso organi pregona (glej točke 25–28 tega mnenja).

Ta posledica neposrednega dostopa je pomemben razlog za pogojenost sprejetja sedanjega predloga s sprejetjem Okvirnega sklepa o varstvu osebnih podatkov. Ostaja en problem: težko si je predstavljati, kako bi imenovani organi lahko zavrnilo zagotovitev informacij na podlagi člena 14.

37. Glede posrednega dostopa preko indeksnih podatkov, ki nudijo informacije po sistemu zadetek/brez zadetka: ta pojav ni nov. Predstavlja osnovo delovanja evropskih obsežnih informacijskih sistemov, kakor je Schengenski informacijski sistem. Prednost vzpostavitve sistema indeksnih podatkov je, da državam članicam izvora podatkov omogoča nadzorovanje izmenjave informacij iz njihovih policijskih datotek. Če je rezultat vpogleda v indeksne podatke uspešen, lahko organ prosilec izda zahtevo za informacije v povezavi z zadevnim posameznikom. To zahtevo lahko zaprosen organ primerno oceni.

38. Vseeno pa je potrebna primerna analiza, saj vzpostavitev sistema indeksnih podatkov — na področjih, kjer ti sistemi, razen obsežnih evropskih informacijskih sistemov, do sedaj še niso obstajali — lahko ustvari nova tveganja za

zadevnega posameznika. Čeprav indeksni podatki ne vsebujejo veliko informacij o zadevnem posamezniku, EDPS poudarja, da lahko vpogled v indeksne podatke vodi do zelo občutljivega rezultata. Razkrije lahko, da je oseba navedena v policijski datoteki v povezavi s kaznivimi dejanji.

39. Zato je najpomembnejše, da evropski zakonodajalec zagotovi ustrezna pravila, vsaj glede oblikovanja indeksnih podatkov, vodenja zbirk indeksnih podatkov in ustrezne organizacije dostopa do indeksnih podatkov. EDPS meni, da predlog v teh točkah ni zadovoljiv. EDPS je na tej stopnji podal tri ugotovitve:
- Opredelitev indeksnih podatkov je nejasna. Ni jasno, ali so indeksni podatki obravnavani kakor metapodatki, primarni ključni ali celo oboje? Pojasniti je treba pojem indeksnih podatkov, saj imajo neposredni vpliv na stopnjo varstva podatkov in potrebna varovala.
  - Predlog mora pojasniti vlogo nacionalnih kontaktnih točk glede indeksnih podatkov. Vključitev nacionalnih kontaktnih točk bi bila lahko nujna, zlasti takrat, kadar razlaga indeksnih podatkov zahteva strokovno znanje, npr. v primeru morebitne primerjave prstnih odtisov.
  - V predlogu je sprejetje potrebnih pravil za oblikovanje indeksnih podatkov v skladu s postopkom komitologije, ki je predviden v členu 19, prepuščeno izvedbeni zakonodaji. Čeprav bi lahko bila potrebna izvedbena pravila, je treba v okvirni sklep vključiti osnovna pravila za oblikovanje indeksnih podatkov.

### Predhodna odobritev pravosodnih organov

40. Pri izmenjavi informacij se zaprosena država članica ne sme oizogniti obveznosti, da od pravosodnih organov zahteva predhodno odobritev za posredovanje informacij organu prosilcu, kadar so te informacije pod pravosodnim nadzorom v zaproseni državi. To je pomembno, saj glede na raziskavo o pristojnostih policije pri izmenjavi osebnih podatkov <sup>(1)</sup> policija v vseh državah članicah nima neodvisnega dostopa do teh podatkov. EDPS meni, da načelo dostopnosti ne sme spodkopati obveznosti iz nacionalne zakonodaje, da se pridobi predhodna odobritev za informacije ali pa se vsaj oblikujejo posebna pravila glede kategorij podatkov, za katere je treba pridobiti predhodno odobritev, ki bodo veljala v vseh državah članicah.

<sup>(1)</sup> Odgovori na vprašalnik o Okvirnem sklepu o poenostavitvi izmenjave informacij in obveščevalnih podatkov med organi pregona držav članic EU, zlasti glede hudih kaznivih dejanj, vključno s terorističnimi dejanji (dok. Sveta št. 5815/1/05).

41. To obveznost je treba tolmačiti v povezavi s členom 11(2) Predloga okvirnega sklepa o varstvu osebnih podatkov, ki prav tako predvideva, da država članica, ki podatke posreduje, odloča o nadaljnji uporabi podatkov v državi članici, v katero so bili podatki posredovani. EDPS je seznanjen, kako pomembno je to načelo, ki je potrebno za zagotovitev, da se omejevalne nacionalne zakonodaje o nadaljnji uporabi osebnih podatkov zaradi dostopnosti ne bo obšlo.

varstvo osebnih podatkov, med drugim tudi, ker je sposobnost držav članic za celovit nadzor okrnjena. Predlog ne sme biti sprejet ločeno od Okvirnega sklepa o varstvu osebnih podatkov.

### Končna opomba

42. Ti elementi zahtevajo visoke standarde na področju varstva podatkov. Posebna pozornost naj se posveti zagotovitvi načel omejitve namena, nadaljnji obdelavi ter točnosti in zanesljivosti informacij, do katerih se dostopa (glej mnenje EDPS o Okvirnem sklepu o varstvu osebnih podatkov, IV.2 in IV.6).

## V. DRUGI PRISTOPI

### Švedski predlog

43. Švedski predlog ni omejen na posebne vrste informacij, temveč zajema vse informacije *in obveščevalne podatke*, celo informacije in obveščevalne podatke, ki jih ne hranijo pristojni organi pregona, temveč drugi organi. Predlog nadgradi sodelovanje, saj določa časovne omejitve za odziv na zahteve za informacije ter ukinja diskriminacijo med izmenjavo znotraj ene države članice in čezmejno izmenjavo informacij. Ne zagotavlja dodatnih ukrepov, ki bi omogočili uspešen dostop do informacij. Zaradi tega je razumljivo, da Komisija ni menila, da je švedski predlog kot tak ustrezen instrument za izvajanje načela dostopnosti<sup>(1)</sup>.

44. Z vidika varstva podatkov so splošne posledice pristopa iz švedskega predloga naslednje:

— Zaželeno je, da se predlog omeji izključno na obdelavo obstoječih podatkov in ne povzroča oblikovanja novih zbirk podatkov, niti zbirke „indeksnih podatkov“.

— Vendar pa dejstvo, da „indeksni podatki“ niso predvideni, ni nujno pozitiven element. Če so indeksni podatki ustrezno varovani, lahko olajšajo ciljno usmerjeno in zato manj vsiljivo iskanje podatkov občutljive narave. Prav tako lahko omogočajo boljše filtriranje zahtev in boljši nadzor.

— Predlog vsekakor vodi k povečanju čezmejne izmenjave osebnih podatkov, kar je povezano s tveganji za

### Konvencija iz Prüma

45. Konvencija iz Prüma zavzema drugačen pristop k izvajanju načela dostopnosti. Medtem ko sedanji predlog okvirnega sklepa zavzema splošni pristop – ne predvideva posebnih pravil za izmenjavo posebnih vrst informacij, temveč se uporablja za vse vrste informacij, v kolikor so te navedene v Prilogi II (glej točke 21–28 tega mnenja) – je pristop Konvencije iz Prüma postopen.

46. Ta pristop je znan tudi pod imenom „pristop od podatkovnega polja do podatkovnega polja“. Velja za posebne vrste informacij (podatki o DNK, prstnih odtisih in registraciji vozila) in določa obveznost upoštevanja posebne narave podatkov. Konvencija za namene preiskovanja kaznivih dejanj določa obveznost oblikovanja in hrambe datotek analiz DNK. Podobna obveznost velja za podatke o prstnih odtisih. V primeru podatkov o registraciji vozila pa je treba neposredni dostop omogočiti nacionalnim kontaktnim točkam drugih držav članic.

47. Pristop Konvencije iz Prüma privede do treh vrst ugotovitev.

48. Najprej je samo po sebi razumljivo, da EDPS ne odobrava postopka, ki je izven institucionalnega okvira Evropske unije in posledično brez znatne vključitve Komisije privedel do Konvencije. Poleg tega to pomeni, da Evropski parlament ne izvaja demokratičnega nadzora, Sodišče pa ne pravosodnega in zaradi tega obstaja manj jamstev, da so vsi (javni) interesi enakovredno uravnoteženi. To vključuje vidik varstva podatkov. Povedano drugače, institucije Evropske unije nimajo možnosti, da bi pred vzpostavitvijo sistema ocenile vpliv izbranih strategij na varstvo osebnih podatkov.

49. Drugič – očitno je, da so nekateri elementi Konvencije iz Prüma za zadevnega posameznika bolj vsiljivi kakor Predlog okvirnega sklepa o dostopnosti. Konvencija nujno vodi do oblikovanja novih zbirk podatkov, kar predstavlja tveganje za varstvo osebnih podatkov. Dokazati je treba potrebo po oblikovanju in sorazmernost oblikovanja teh novih zbirk podatkov. Zagotoviti je treba ustrezna varovala za varstvo osebnih podatkov.

(<sup>1</sup>) Glej delovni dokument služb Komisije z naslovom „Priloga k predlogu okvirnega sklepa Sveta o izmenjavi informacij v skladu z načelom dostopnosti“, SEK 2005 (1270) z dne 12.10.2005.

### „Pristop od podatkovnega polja do podatkovnega polja“

50. Tretjič – kakor je bilo že omenjeno, zavzema Konvencija „pristop od podatkovnega polja do podatkovnega polja“. EDPS je zgoraj omenil težave in negotovosti, ki so povezane s pogoji, v katerih je treba izvajati načelo dostopnosti. EDPS meni, da je v teh okoliščinah bolje, da se ne oblikuje sistem za vse vrste podatkov, temveč se prične s previdnejšim pristopom, ki vključuje eno vrsto podatkov, in zatem spremlja, do kakšnega obsega lahko načelo dostopnosti učinkovito podpira organe pregona, ter ugotovi, katera so posebna tveganja za varstvo osebnih podatkov. Na podlagi teh izkušenj se sistem lahko razširi na druge vrste podatkov in/ali spremeni, da bi bil bolj učinkovit.

51. Ta „pristop od podatkovnega polja do podatkovnega polja“ bi tudi bolje izpolnil zahteve načela sorazmernosti. EDPS meni, da bi potrebe pa boljši čezmejni izmenjavi podatkov v namene pregona lahko opravičile sprejetje pravnega instrumenta na ravni EU, da pa bi bil ta instrument sorazmeren, mora biti primeren za doseganje svojih ciljev, ki so lahko bolje določeni po obdobju dejanskih izkušenj. Poleg tega instrument ne sme nesorazmerno škodovati zadevnemu posamezniku. Izmenjava ne sme obsegati več vrst podatkov, kakor je nujno potrebno, predvidena pa naj bo anonimna izmenjava podatkov, ki mora potekati pod strogimi pogoji glede varstva podatkov.

52. Poleg tega bi lahko bolj previden pristop, za katerega se zavzema EDPS – po možnosti dopolnjen s „pristopom od podatkovnega polja do podatkovnega polja“ – vključeval pričetek izvajanja načela dostopnosti le s posrednim dostopom preko indeksnih podatkov. To EDPS omenja z namenom, da bo upoštevano v nadaljnjem zakonodajnem postopku.

### VI. KATERI PODATKI?

53. Priloga II našteva vrste informacij, ki jih je mogoče pridobiti s predlaganim okvirnim sklepom. Vseh šest vrst informacij, ki so našteje v njej, predstavlja v različnih okoliščinah osebne podatke, saj jih je mogoče pripisati določeni ali določljivi osebi.

54. Indeksni podatki v smislu člena 3(g) Predloga pomenijo „podatke, katerih namen je razločno opredeliti informacije in po katerih se lahko poizveduje na podlagi iskalnika, da

se ugotovi, ali so informacije na razpolago ali ne“. V „pristopu za izvajanje načela dostopnosti“<sup>(1)</sup> so indeksni podatki naslednji podatki:

- ugotavljanje istovetnosti zadevnih oseb;
- identifikacijska številka za zadevne predmete (vozila/dokumenti);
- prstni odtisi/digitalne fotografije.

Druga vrsta podatkov, ki lahko veljajo za indeksne, so DNK profili. Ta seznam indeksnih podatkov kaže, da ti lahko vsebujejo osebne podatke in je zato potrebno ustrezno varstvo.

55. EDPS posebej obravnava vprašanje DNK profilov. Analiza DNK se je izkazala za zelo pomembno pri preiskovanju kaznivih dejanj, učinkovita izmenjava DNK podatkov pa je v boju proti kriminalu lahko bistvena. Vendar pa je pomembno, da se pojem DNK podatkov jasno opredeli, posebne značilnosti teh podatkov pa primerno upošteva. Z vidika varstva podatkov pa je med DNK vzorci in DNK profili zares velika razlika.

56. DNK vzorce (pogosto jih zbirajo in hranijo organi pregona) je treba obravnavati kakor posebno občutljive, saj je verjetnost, da vsebujejo celo DNK „sliko“, večja. Zagotovijo lahko informacije o genetskih značilnostih in zdravstvenem stanju osebe, kar se lahko potrebuje za povsem drugačne namene, kakor npr. zdravstveno svetovanje posameznikom in mladim parom.

57. V nasprotju pa lahko DNK profili vsebujejo nekatere delne DNK informacije, pridobljene iz DNK vzorca: lahko se uporabljajo za preverjanje istovetnosti osebe, vendar načeloma ne razkrivajo genetskih značilnosti osebe. Vendar pa napredek znanosti lahko poveča količino informacij, ki jih DNK profili lahko razkrijejo: kar je v nekem trenutku obravnavano kakor „nedolžni“ DNK profil, lahko kasneje razkrije več informacij, kakor je pričakovano ali potrebno, zlasti informacije o genetskih značilnostih osebe. Informacije, ki jih DNK profil lahko razkrije, je zato treba obravnavati kakor spremenljive.

58. S tega vidika EDPS opaža, da Konvencija iz Prüma in predlog Komisije spodbujata izmenjavo DNK podatkov med organi pregona, vendar na zelo različna načina.

<sup>(1)</sup> Dokument predsedstva Svetu z dne 5. aprila 2005 (dok. št. 7641/05).

59. EDPS pozdravlja dejstvo, da predlog Komisije ne določa nobene obveznosti za zbiranje DNK podatkov ter da jasno omejuje izmenjavo DNK podatkov na DNK profile. Priloga II opredeljuje DNK profile s pomočjo izhodiščnega skupnega seznama označevalcev DNK, ki se uporabljajo v forenzični analizi DNK v državah članicah. Ta seznam – ki temelji na sedmih označevalcih DNK iz Evropskih standardov, kakor so opredeljeni v Prilogi I Resolucije Sveta z dne 25. junija 2001 o izmenjavi rezultatov analiz DNK<sup>(1)</sup> – jamči, da pridobljeni DNK profili ne bodo vsebovali nobene informacije o posebnih dednih značilnostih.
60. EDPS poudarja, da ta resolucija Sveta določa nekatera zelo pomembna varovala, ki so posebej povezana s spremenljivo naravo DNK profilov. Oddelek III Resolucije, potem ko omeji izmenjave rezultatov analiz DNK na „kromosomska območja [...], za katera ni znano, da bi zagotavljala informacije o posebnih dednih značilnostih“, nadalje državam članicam priporoča, naj prenehajo z uporabo tistih označevalcev DNK, ki lahko zaradi razvoja znanosti zagotovijo informacije o posebnih dednih značilnostih.
61. Konvencija iz Prüma predvideva drugačen pristop, saj pogodbenice za namene preiskovanja kaznivih dejanj zavezuje k oblikovanju in hrambi datotek analiz DNK. Posledica tega je zato oblikovanje novih zbirk DNK podatkov in povečano zbiranje DNK podatkov. Poleg tega ni jasno, kateri podatki so vključeni v „datoteke analiz DNK“, Konvencija pa ne upošteva dinamičnega razvoja DNK profilov.
62. EDPS opozarja, da mora vsak pravni instrument, ki določa izmenjave DNK podatkov:

- jasno omejiti in opredeliti vrsto DNK podatkov, ki se lahko izmenjajo (tudi glede na temeljne razlike med DNK vzorci in DNK profili);
- oblikovati skupne tehnične standarde, katerih namen je preprečiti, da bi razlike v praksah držav članic na področju sodnih zbirk DNK podatkov vodile do težav in netočnih rezultatov pri izmenjavi podatkov;
- zagotoviti ustrezna pravno zavezujoča varovala, da bi se zaradi razvoja znanosti preprečilo pridobivanje osebnih podatkov iz DNK profilov, tj. osebnih podatkov, ki niso le občutljivi, temveč tudi nepotrebni za namen, zaradi katerega so bili zbrani.

63. S tega vidika EDPS sedaj potrjuje in vključuje opombe, ki jih je že podal v svojem mnenju o Okvirnem sklepu o varstvu osebnih podatkov (točka 80). EDPS je v tem mnenju opozoril, da je treba v primeru DNK podatkov zagotoviti posebna varovala, s katerimi bo zagotovljeno, da: se lahko razpoložljive informacije uporabljajo le za preverjanje istovetnosti posameznikov za namene preprečevanja, odkrivanja ali preiskovanja kaznivih dejanj; se skrbno upošteva stopnja točnosti DNK profilov in da jo lahko zadevni posameznik spodbija s pomočjo lahko dostopnih sredstev; se v celoti zagotovi spoštovanje dostojanstva ljudi<sup>(2)</sup>.

64. Ti vidiki nadalje vodijo do zaključka, da je treba zakonodajo o oblikovanju DNK datotek in izmenjavi podatkov iz teh datotek sprejeti šele po izvedeni oceni vpliva, v kateri bodo koristi in tveganja pravilno ocenjeni. EDPS priporoča, naj ta zakonodaja vsebuje obveznosti za redno vrednotenje po njenem začetku veljavnosti.

65. Nazadnje Priloga II vključuje druge vrste informacij, ki se jih lahko izmenja. Vključuje informacije, katerih vir so zasebne ustanove, saj so telefonski operaterji običajno res vir telefonskih števil in ostalih komunikacijskih podatkov ter podatkov o prometu. Obrazložiten memorandum potrjuje, da si morajo države članice izmenjati ustrezne informacije organov pregona, ki jih nadzorujejo organi ali zasebne strani, imenovane v ta namen, z enakovrednimi pristojnimi organi drugih držav članic in Europolom. Medtem ko predlog velja za osebne podatke, katerih vir so zasebne strani, mora veljavni pravni okvir – po mnenju EDPS – vsebovati dodatna varovala za varstvo zadevnega posameznika, da se zagotovi točnost podatkov.

## VII. NAČELA VARSTVA PODATKOV

66. V predlaganem okvirnem sklepu Sveta pravila o varstvu osebnih podatkov niso natančno določena, medtem ko v drugih instrumentih, kakor sta Konvencija iz Prüma ali švedski predlog, posebne določbe o varstvu osebnih podatkov obstajajo. Dejstvo, da v predlogu o dostopnosti ni posebnih pravil o varstvu osebnih podatkov, je sprejemljivo le, če se splošna pravila iz Predloga okvirnega sklepa o varstvu podatkov v tretjem stebru v celoti uporabljajo in zagotavljajo zadostno varstvo. Poleg tega pravila o varstvu osebnih podatkov, ki jih določata posebna instrumenta – kakor sta švedski predlog in Konvencija iz Prüma – ne smejo znižati stopnje varstva, ki jo zagotavlja splošni okvir. EDPS priporoča, da se doda posebna klavzula o možnih nesoglasjih med različnimi pravili o varstvu podatkov.

<sup>(2)</sup> V skladu z navedenim glej tudi „Poročilo o napredku v zvezi z uporabo načel Konvencije 108 o zbiranju in obdelavi biometričnih podatkov“ Sveta Evrope iz februarja 2005.

<sup>(1)</sup> UL C 187, str. 1.



67. EDPS opozarja na svoje mnenje glede Okvirnega sklepa o varstvu osebnih podatkov in želi s tem sedaj ponovno poudariti pomen usklajenih in obsežnih pravil o varstvu podatkov za sodelovanje na področju kazenskega pregona, ki veljajo za vse obdelave. Zato EDPS ponovno poudarja druge vidike iz tega mnenja. V tem odstavku so poudarjena naslednja vprašanja o varstvu podatkov:

— Zakonita obdelava osebnih podatkov. EDPS zagovarja pristop, da so informacije lahko na voljo le, če so bile zbrane zakonito (kakor je omenjeno v členu 2.2 v povezavi z informacijami, zbranimi s prisilnimi ukrepi). Zakonita obdelava osebnih podatkov bi prav tako zagotovila, da se informacije, ki so na voljo in so bile izmenjane, lahko primerno uporabijo tudi v pravosodnih postopkih. Čeprav informacije, ki se obdelajo po začetku sodnega pregona, ne sodijo v področje uporabe predlaganega instrumenta, še vedno obstaja možnost, da se bodo informacije, ki so jih organi pregona izmenjali pred tem, uporabile v pravosodnih postopkih.

— Posebnega pomena je kakovost osebnih podatkov, saj je načelo dostopnosti naklonjeno temu, da bodo informacije uporabljali organi pregona, ki delujejo izven okvira, v katerem so bili ti podatki zbrani. Ti organi imajo celo neposredni dostop do zbirk podatkov drugih držav članic. Kakovost osebnih podatkov je mogoče zagotoviti le, če se njihova točnost redno in pravilno preverja, če se informacije razlikujejo glede na različne kategorije zadevnih oseb (žrtve, osumljenci, priče, itd.) in če je, kadar je to potrebno, stopnja točnosti navedena (glej mnenje EDPS o varstvu osebnih podatkov, IV.6).

Ti vidiki ponovno ponazarjajo, zakaj morajo pravila o varstvu podatkov in zlasti pravila o točnosti veljati za vse vrste obdelav, tudi za obdelave na državni ravni. Drugače so lahko osebni podatki, do katerih se dostopa neposredno, netočni, zastareli in s tem kratio pravice zadevnemu posamezniku terovirajo učinkovitost preiskav.

— Omejitev namena. V skladu z načelom dostopnosti so osebni podatki dostopni enakovrednim pristojnim organom drugih držav članic. Vendar pa se lahko pristojnosti organov pregona med državami občutno razlikujejo. Zato je nujno, da se zagotovi spoštovanje osnovnega načela omejitve namena, ne glede na različne pristojnosti raznih pristojnih organov, ki sodelujejo pri izmenjavi podatkov. Informacije, ki jih nek organ zbere in obdela s posebnim namenom, se ne

smejo uporabiti v druge namene samo zato, ker ima organ, ki jih prejme, različne, mogoče širše pristojnosti.

Zato EDPS pozdravlja člen 7 predlaganega okvirnega sklepa, ki ga je treba razumeti kakor podoben opis splošnih pravil, določenih v predlaganem okvirnem sklepu o varstvu osebnih podatkov. EDPS nadalje ugotavlja, da je treba oceno enakovrednosti med različnimi organi (ki je v sedanjem predlogu prepuščena postopku komitologije) natančno izvesti, ob ustreznem upoštevanju načela omejitve namena.

— Roke za shranjevanje izmenjanih informacij je prav tako treba obravnavati v okviru načela omejitve namena: informacije, do katerih se dostopa ali se jih izmenjuje za en namen, je treba izbrisati takoj, ko za ta namen niso več potrebne. S tem bi se izognilo nepotrebnemu podvajanju zbirk podatkov, pristojnim organom pa bil ponoven dostop do (posodobljenih) razpoložljivih informacij še vedno dovoljen, v primeru, da so te informacije potrebne za druge zakonite namene.

— Prijava informacij, ki so posredovane v skladu z načelom dostopnosti. Prijavo morata opraviti obe strani: v zaproseni državi članici in državi članici prosilki. Dnevnik o dostopu in ne le izmenjavi je treba hraniti (glej mnenje EDPS o varstvu osebnih podatkov, točka 133) tudi z namenom, da se zagotovi, da si nacionalni pristojni organi zaupajo in ne izgubijo v celoti nadzora nad razpoložljivimi informacijami. Potreba po sledljivosti informacij vsebuje tudi možnost posodobitve in/ali spremembe informacij.

— Pravice zadevnih posameznikov. S sistemi za izmenjavo informacij med organi pregona EU nastaja vse več okoliščin, v katerih pristojni organi v različnih državah članicah osebne podatke istočasno (začasno) obdelujejo. To na eni strani pomeni, da je treba vzpostaviti skupne standarde EU o pravicah zadevnih posameznikov, na drugi strani pa morajo biti zadevni posamezniki sposobni uveljavljati svoje pravice v povezavi z organi, ki dajejo podatke na voljo, in organi, ki te podatke obdelujejo, in sicer do obsega, ki ga omogočajo pravila o varstvu podatkov v tretjem stebru.

— Nadzor. EDPS poudarja, da je lahko glede na primer več nacionalnih nadzornih organov pristojnih za spremljanje obdelave osebnih podatkov, ki se izvaja na podlagi sedanjih predlogov. S tega vidika zahteva neposredni spletni dostop do informacij organov pregona povečani nadzor in boljše usklajevanje pristojnih nacionalnih organov za varstvo podatkov.

## VIII. ZAKLJUČKI

**Splošni zaključki glede načela dostopnosti**

68. EDPS izkorišča to priložnost, da v tem mnenju predstavi nekaj splošnih in bolj temeljnih vidikov o vprašanju izmenjave informacij organov pregona in o pristopih k urejanju tega vprašanja. Posvetovanje z EDPS je mogoče tudi pozneje, ko bo zakonodajni postopek o tem predlogu ali ostalih predlogih na to temo ustrezno napredoval.
69. EDPS meni, da mora biti načelo dostopnosti vzpostavljeno v obliki zavezujočega pravnega instrumenta s previdnejšim pristopom, ki vključuje eno vrsto podatkov; spremljati je treba, do kakšnega obsega lahko načelo dostopnosti učinkovito podpira organe pregona ter ugotoviti, katera so posebna tveganja za varstvo osebnih podatkov. Ta previdnejši pristop bi lahko vključeval začetek izvajanja načela dostopnosti le z neposrednim dostopom preko indeksnih podatkov. Na podlagi teh izkušenj se sistem lahko razširi na druge vrste podatkov in/ali spremeni, da bi bil bolj učinkovit.
70. Brez predhodnega sprejetja nujnih jamstev o varstvu podatkov, kakor so vključena v Predlog okvirnega sklepa o varstvu osebnih podatkov, se ne sme sprejeti noben pravni instrument, ki uveljavlja načelo dostopnosti.

**Priporočila za spremembo sedanjega predloga**

71. EDPS svetuje, da se pojasni področje uporabe načela dostopnosti, in sicer:
- Dodati je treba jasno in natančno opredelitev podatkov, ki bodo veljali za razpoložljive.
  - Prva možnost je omejitev področja uporabe načela dostopnosti na informacije, ki jih nadzorujejo pristojni organi.
  - Druga pa je v primeru širšega področja uporabe zagotoviti zadostna varovala za varstvo osebnih podatkov. Upoštevati je treba vprašanja, zastavljena v točki 27.
72. EDPS o neposrednem dostopu pristojnih organov druge države članice do zbirk podatkov ugotavlja:
- Vprašanje je treba primerno obravnavati, saj imenovani organi države članice izvora podatkov v primeru neposrednega dostopa nimajo nadzora nad dostopom in nadaljnjo uporabo podatkov.

- Predlog ne sme spodbujati neomejene medsebojne povezljivosti zbirk podatkov in posledično mreže zbirk podatkov, ki bi jo bilo težko nadzorovati.
73. Okvirni sklep mora biti natančnejši glede vzpostavitve sistema indeksnih podatkov. Zlasti:
- Predlog mora zagotoviti ustrezna pravila, vsaj glede oblikovanja indeksnih podatkov, vodenja zbirk indeksnih podatkov in ustrezne organizacije dostopa do indeksnih podatkov.
  - Pojasniti je treba opredelitev indeksnih podatkov.
  - Predlog mora pojasniti vlogo nacionalnih kontaktnih točk glede indeksnih podatkov.
  - Osnovna pravila za oblikovanje indeksnih podatkov je treba vključiti v Okvirni sklep, z njimi se ne sme ukvarjati izvedbena zakonodaja v skladu s postopkom komitologije.
74. EDPS opozarja, da mora Predlog – v kolikor določa izmenjavo DNK podatkov:
- jasno omejiti in opredeliti vrsto DNK podatkov, ki se lahko izmenjajo (tudi glede na temeljne razlike med DNK vzorci in DNK profili);
  - oblikovati skupne tehnične standarde, katerih namen je preprečiti, da bi razlike v praksah držav članic na področju sodnih zbirk DNK podatkov vodile do težav in netočnih rezultatov pri izmenjavi podatkov;
  - zagotoviti ustrezna pravno zavezujoča varovala, da bi se zaradi razvoja znanosti preprečilo pridobivanje osebnih podatkov iz DNK profilov, tj. osebnih podatkov, ki niso le občutljivi, temveč tudi nepotrebni za namen, zaradi katerega so bili zbrani;
  - biti sprejet šele po izvedeni oceni vpliva.
75. EDPS svetuje, da se izmenjava informacij z Europolom omeji na namene samega Eurola, kakor je navedeno v členu 2 Konvencije o Europolu in v njeni prilogi.

V Bruslju, 28. februarja 2006

Peter HUSTINX

*Evropski nadzornik za varstvo podatkov*