EUROOPA ANDMEKAITSEINSPEKTOR

Euroopa andmekaitseinspektori arvamus järgmiste õigusaktide kohta:

— ettepanek: nõukogu otsus teise põlvkonna Schengeni infosüsteemi (SIS II) loomise, toimimise ja kasutamise kohta (KOM (2005) 230 lõplik);

— ettepanek: Euroopa Parlamendi ja nõukogu määrus teise põlvkonna Schengeni infosüsteemi (SIS II) loomise, toimimise ja kasutamise kohta (KOM (2005) 236 lõplik) ning

— ettepanek: Euroopa Parlamendi ja nõukogu määrus, mis käsitleb liikmesriikides sõidukite registreerimistunnistusi väljaandvate teenistuste juurdepääsu teise põlvkonna Schengeni infosüsteemile (SIS II) (KOM (2005) 237 lõplik).

(2006/C 91/11)

EUROOPA ANDMEKAITSEINSPEKTOR,

võttes arvesse Euroopa Ühenduse asutamislepingut, eriti selle artiklit 286,

võttes arvesse Euroopa Liidu põhiõiguste hartat, eriti selle artiklit 8,

võttes arvesse Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiivi 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta,

võttes arvesse Euroopa Parlamendi ja nõukogu 18. detsembri 2000. aasta määrust (EÜ) nr 45/2001 üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta, eriti selle artiklit 41,

võttes arvesse komisjoni 17. juuni 2005. aasta taotlust arvamuse esitamise kohta kooskõlas määruse (EÜ) nr 45/2001 artikli 28 lõikega 2,

ON VASTU VÕTNUD JÄRGMISE ARVAMUSE:

1. SISSEJUHATUS

1.1. Taust

Schengeni infosüsteem (SIS II) on ELi suuremahuline IT-süsteem, mis loodi tasakaalustava meetmena pärast kontrollide kaotamist Schengeni piirkonna sisepiiridel. SIS võimaldab liikmesriikide pädevatel asutustel vahetada teavet, mida kasutatakse välispiiridel või liikmesriikide territooriumil isikute ja esemete kontrollimiseks ning viisade ja elamislubade väljastamiseks.

Schengeni konventsioon jõustus 1995. aastal valitsustevahelise lepinguna. SIS integreeriti hiljem Schengeni konventsiooni osana Amsterdami lepinguga ELi raamistikku.

Uus "teise põlvkonna" Schengeni infosüsteem (SIS II) asendab praeguse süsteemi, võimaldades seeläbi Schengeni piirkonna laienemist uutele ELi liikmesriikidele. SIS IIga lisatakse süsteemile ka uusi funktsioone. Schengeni sätted, mis on välja töötatud valitsustevahelises koostöös, muudetakse täies ulatuses tavapärasteks Euroopa õigusaktideks.

Euroopa komisjoni esitas 1. juunil 2005 kolm SIS II loomist käsitlevat ettepanekut. Nimetatud ettepanekud on järgmised:

— EÜ asutamislepingu IV jaotisel (viisa-, varjupaiga-, sisserände- ja muu isikute vaba liikumisega seotud poliitika) põhinev kavandatav määrus, mis reguleerib teise samba (sisseränne) alla kuuluvaid SIS II aspekte (edaspidi "kavandatav määrus");

— EÜ asutamislepingu VI jaotisel (politsei- ja õigusalane koostöö kriminaalasjades) põhinev kavandatav otsus, mis reguleerib SISi kasutamist kolmanda samba alla kuuluvatel eesmärkidel (edaspidi "kavandatav otsus");

— V jaotisel (transport) põhinev kavandatav määrus, mis käsitleb eelkõige sõidukite registreerimise eest vastutavate asutuste juurdepääsu SISi andmetele; kõnealust ettepanekut käsitletakse eraldi (vt allpool punkt 4.6).

Selles kontekstis väärib märkimist, et komisjon annab eelolevatel kuudel välja teatise ELi infosüsteemide (SIS, VIS, Eurodac) koostalitlusvõime parandamise ja sünergia suurendamise kohta.

SIS II koosneb Schengeni keskinfosüsteemiks (CS-SIS) nimetatavast kesksest andmebaasist, mille operatiivjuhtimise eest vastutab komisjon ja mis on ühendatud kõigi liikmesriikide poolt määratud juurdepääsupunktidega (NI-SIS). SIRENE asutused tagavad kogu täiendava teabe (teave, mis on seotud SIS II hoiatusteadetega, kuid mida ei säilitata SIS IIs) vahetamise.

Liikmesriigid sisestavad SIS IIte andmeid isikute kohta, keda otsitakse vahistamise, üle- või väljaandmise eesmärgil või kohtumenetluse jaoks, isikute kohta, kes tuleb võtta järelevalve alla või kelle suhtes tuleb teostada erikontrolle, isikute kohta, kellele tuleb keelata sisenemine välispiiril ning kaotatud või varastatud esemete kohta. SISi sisestatud andmekogum, mida nimetatakse "hoiatusteadeteks", võimaldab pädeval asutusel isiku või objekti kindlaks teha.

SIS II toob kaasa uuendusi: laialdasem juurdepääs SISile (Europol, Eurojust, riikide prokurörid, sõidukite registreerimise eest vastutavad asutused), hoiatusteadete omavaheline seostamine, uute andmeliikide, sealhulgas biomeetriliste andmete (sõrmejäljed ja fotod) lisamine ning samuti viisainfosüsteemiga ühine tehniline platvorm. Need täiendused on aastaid andnud ainet aruteludeks SISi eesmärgi sellise nihkumise üle, et kontrollivahendist saab teatamis- ja uurimissüsteem.

1.2. **Üldhinnang ettepanekutele**

1. Euroopa andmekaitseinspektor tervitab asjaolu, et temaga konsulteeritakse määruse (EÜ) nr 45/2001 artikli 28 lõike 2 alusel. Pidades silmas artikli 28 lõike 2 kohustuslikkust, tuleks käesolevat arvamust mainida teksti preambulis.

2. Euroopa andmekaitseinspektor tervitab ettepanekuid mitmel põhjusel. Valitsustevahelise struktuuri muutmine Euroopa õigusaktideks toob endaga kaasa mitmeid positiivseid tagajärgi: selgitatakse SIS II reguleerivate eeskirjade õigusjõudu, Euroopa Kohus saab pädevuse tõlgendada esimese samba alla kuuluvaid õigusakte, Euroopa Parlament kaasatakse vähemalt osaliselt (ehkki protsessi üsna hilises etapis).

3. Peale selle sisaldavad ettepanekud olulisi andmekaitsele pühendatud sätteid, millest mõned on võrreldes praeguse olukorraga teretulnud parandused. Eelkõige võib märkida identiteedi varguse ohvrite kasuks võetud meetmeid, määruse (EÜ) nr 45/2001 laiendamist VI jaotise alla kuuluvatele komisjoni andmetöötlustoimingutele ja sisenemise keelamise eesmärgil isikute suhtes hoiatusteadete väljastamise põhjenduste paremat määratlust.

4. Samuti on ilmne, et ettepanekud on koostatud suure hoolega — need on keerulised, kuid see kajastab pigem selle süsteemi keerukust, mida nad hõlmavad. Enamiku käesolevas arvamuses esitatud märkuste eesmärk on olemasolevate sätete selgitamine või täiendamine, kuid need ei nõua täielikku uuestisõnastamist.

Hoolimata sellest üldjoontes positiivsest hinnangust võib aga siiski väljendada mõningaid reservatsioone eelkõige alljärgneva suhtes:

1. Mitmes mõttes on raske mõista, milline on teksti eesmärk; seletuskirja puudumine on äärmiselt kahetsusväärne. Arvestades kõnealuste dokumentide keerukust, oleks seletuskiri olnud üks põhinõue. Selle puudumine ei jäta aga lugejale mõningatel juhtudel muud võimalust kui oletada.

2. Lisaks sellele on samuti kahetsusväärne, et ei ole läbi viidud mõjuhindamist. Asjaolu, et süsteemi esimene versioon on juba käigus, ei ole siinkohal õigustuseks, kuna kahe süsteemi vahel esineb märkimisväärseid erinevusi. Muu hulgas oleks tulnud paremini läbi mõelda biomeetriliste andmete kasutuselevõtmise mõju.

3. Andmekaitset käsitlev õiguslik raamistik on väga keerukas. See põhineb üldseaduste (*lex generalis*) ja eriseaduste (*lex specialis*) kombineeritud kohaldamisel. Tuleks tagada, et isegi eriseaduse väljatöötamise korral säiliks direktiivis 95/46/EÜ ja määruses (EÜ) nr 45/2001 sätestatud olemasoleva andmekaitseraamistiku täielik kohaldatavus. Erinevate õigusaktide kombineeritud kohaldamine ei tohiks viia ei erinevusteni riiklike süsteemide vahel põhiaspektide osas ega praeguse andmekaitsetaseme langemiseni.

4. Paljude selliste uute asutuste juurdepääsuga, kellesse esialgne isikute ja esemete kontrollimise eesmärk ei puutu, peaks kaasnema rangemad kaitsemeetmed.

5. Ettepanekud põhinevad suures osas muudel veel valmimisjärgus õigusaktidel (millest mõnede kohta ei ole veel isegi ettepanekut tehtud). Euroopa andmekaitseinspektor mõistab raskusi, mis kaasnevad õigusloomega keerukas ja pidevalt muutuvas keskkonnas, kuid pidades silmas selle tagajärgi asjaomastele isikutele ning selle tulemusel tekkivat õiguskindlusetust, ei pea ta seda vastuvõetavaks.

6. Mõnevõrra ähmane on ka liikmesriikide ja komisjoni vaheline pädevuste jaotus. Selgus on otsustava tähtsusega, kuna see on vajalik mitte üksnes süsteemi tõrgeteta toimimiseks, vaid ka seetõttu, et see on põhinõue süsteemi igakülgse järelevalve tagamiseks.

1.3. **Arvamuse ülesehitus**

Arvamuse ülesehitus on järgmine: esmalt selgitatakse SIS II suhtes kohaldatavat õiguslikku raamistikku. Seejärel käsitletakse SIS II eesmärgi määratlust ja praegusest süsteemist märkimisväärselt erinevaid elemente. Punkt 5 sisaldab märkusi komisjoni ja liikmesriikide vastavate rollide kohta seoses SIS II toimimisega. Punktis 6 käsitletakse andmesubjekti õigusi ning punktis 7 nii liikmesriikide kui Euroopa andmekaitseinspektori tasandil toimuvat järelevalvet ja järelevalveasutuste vahelist koostööd. Punkt 8 sisaldab mõningaid turvalisusega seotud märkusi ja muudatusettepanekuid. Punktides 9 ja 10 käsitletakse komiteemenetlust ja koostoimimisvõimet. Lõpetuseks tuuakse kokkuvõttes esile peamised järeldused, milleni iga punkti puhul jõuti.

2. ASJAKOHANE ÕIGUSLIK RAAMISTIK

2.1. **SIS II alane andmekaitseraamistik**

Ettepanekutes viidatakse andmekaitset käsitlevate õiguslike alustena direktiivile 95/46/EÜ, konventsioonile nr 108 ja määrusele (EÜ) nr 45/2001. On ka muid asjakohaseid dokumente.

Selle konteksti selgitamiseks ning käesoleva analüüsi peamiste lähtepunktide meeldetuletamiseks on otstarbekas osutada järgmistele asjaoludele:

— Eraelu austamine on olnud Euroopas tagatud alates sellest, kui Euroopa Nõukogu võttis 1950. aastal vastu Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni (edaspidi "EIPKK"). EIPKK artiklis 8 sätestatakse igaühe "õigus sellele, et austataks tema era- ja perekonnaelu",

  Artikli 8 lõike 2 kohaselt võib riigiasutus selle õiguse kasutamist piirata üksnes, kui see on "kooskõlas seadusega" ning "kui see on demokraatlikus ühiskonnas vajalik" oluliste huvide kaitsmiseks. Euroopa Inimõiguste Kohtu praktikas on nende tingimuste tulemusel kehtestatud lisanõuded, mis käsitlevad õiguste piiramise õigusliku aluse kvaliteeti, mis tahes meetme proportsionaalsust ning kuritarvitamise vastaste meetmete vajadust.

— Hiljem on õigus eraelu puutumatusele ja isikuandmete kaitsele sätestatud Euroopa Liidu põhiõiguste harta artiklites 7 ja 8. Harta artikli 52 kohaselt võib neid õigusi piirata samadel tingimusel, mis kehtivad vastavalt EIPKK artiklile 8.

— Euroopa Liidu lepingu artikli 6 lõikes 2 sätestatakse, et liit austab Euroopa inimõiguste ja põhivabaduste kaitse konventsiooniga tagatud põhiõigusi.

Kolm SIS II alaste ettepanekute suhtes selgelt kohaldatavat õigusakti on järgmised:

— Euroopa Nõukogu 28. jaanuari 1981. aasta konventsioon nr 108 üksikisikute kaitse kohta isikuandmete automaattöötlusel (edaspidi konventsioon nr 108), milles esitati aluspõhimõtted üksikisikute kaitseks isikuandmete töötlemisel. Kõik liikmesriigid on konventsiooni nr 108 ratifitseerinud. See on samuti kohaldatav politsei ja õigusalal teostatavate toimingute suhtes. Praegu kohaldatakse SIS konventsiooni suhtes konventsioonis nr 108 ning Euroopa Nõukogu ministrite komitee 17. septembri 1987. aasta soovituses nr R (87) 15 (millega reguleeritakse isikuandmete kasutamist politseivaldkonnas) sätestatud andmekaitsekorda.

— Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (EÜT L 281, lk 31). Edaspidi viidatakse nimetatud direktiivile järgmiselt: "*direktiiv 95/46/EÜ*". Märkimisväärne on ka see, et enamikus liikmesriikides hõlmavad direktiivi rakendamist käsitlevad riiklikud õigusaktid ka politsei ja õigusalal teostatavaid andmetöötlustoiminguid.

— Euroopa Parlamendi ja nõukogu 18. detsembri 2000. aasta määrus (EÜ) nr 45/2001 üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta (EÜT L 8, lk 1). Edaspidi viidatakse nimetatud määrusele järgmiselt: "*määrus 45/2001*".

Direktiivi 95/46/EÜ ja määruse 45/2001 tõlgendamine peab vastavalt 1950. aasta Euroopa inimõiguste ja põhivabaduste kaitse konventsioonile sõltuma osaliselt Euroopa Inimõiguste Kohtu asjaomasest kohtupraktikast. Teisisõnu tuleb direktiivi ja määrust selles ulatuses, milles neis käsitletakse isikuandmete töötlemist, mis võib piirata põhivabadusi, eelkõige eraelu puutumatust, tõlgendada põhiõiguste valguses. Sama tuleneb ka Euroopa Kohtu praktikast ([1]).

([1]) Antud kontekstis on kasulik viidata Euroopa Kohtu otsusele kohtuasjas Österreichischer Rundfunk ja teised (Liidetud kohtuasjad C-465/00, C-138/01 ja C-139/01, 20. mai 2003. aasta kohtuotsus, täiskogu, (2003) EKL I-4989). Kohus käsitles Austria õigusakti, millega nähakse ette avaliku sektori töötajate palkadega seotud üksikasjade edastamine Austria Kontrollikojale ning nende avaldamine seejärel. Oma otsuses sätestab kohus mitmed Euroopa inimõiguste konventsiooni artiklist 8 tulenevad kriteeriumid, mida tuleks kasutada direktiivi 95/46/EÜ kohaldamisel selles ulatuses, milles nimetatud direktiivi alusel on lubatud teatud piirangud eraelu puutumatuse õigusele.

Komisjon esitas 4. oktoobril 2005 ettepaneku võtta vastu nõukogu raamotsus kriminaalasjadega seotud politsei- ja õigusalase koostöö raames töödeldavate isikuandmete kaitse kohta ([1]) (edaspidi "*raamotsuse eelnõu*"). Nimetatud raamotsusega kavatsetakse asendada konventsioon nr 108 kui SIS II käsitleva otsuse eelnõu referentsõigusakt, mis tõenäoliselt mõjutab andmekaitsekorda selles kontekstis (vt allpool punkt 2.2.5).

2.2. **SIS II õiguslik andmekaitsekord**

2.2.1. *Üldmärkus*

SIS II reguleerimiseks vajalik õiguslik alus koosneb erinevatest dokumentidest, kuid — nagu juba põhjendustes märgitud — ei mõjuta see "põhimõtet, et SIS II on üks ühtne infosüsteem, mis peaks sellisena ka toimima. Seetõttu peaksid nende dokumentide teatavad sätted olema samasugused".

Kahe dokumendi struktuur on põhijoontes sama ning peatükid I–III on mõlemas tekstis tõepoolest peaaegu identsed. Asjaolu, et SIS II tuleks käsitada üheainsa infosüsteemina, millel on kaks erinevat õiguslikku alust, kajastub ka üsna keerukas andmekaitsekorras.

Andmekaitsekord on osalt kindlaks määratud ettepanekutes endis eriseadusena (*lex specialis*), mida täiendab iga valdkonna puhul (komisjon, liikmesriigid esimese samba osas, liikmesriigid teise samba osas) eraldi referentsõigusakt (*lex generalis*).

Selline struktuur tõstatab küsimuse, kuidas käsitleda erieeskirju seoses üldseadustega. Sellisel juhul käsitab Euroopa andmekaitseinspektor erieeskirja üldeeskirja rakendusena. Sellest tulenevalt peab eriseadus olema alati kooskõlas üldseadusega; eriseadus arendab üldseadust edasi (täpsustab seda või lisab sellele midagi), kuid seda ei peeta erandiks üldseadusest.

Küsimuse puhul, millist eeskirja tuleks kohaldada erijuhtudel, kehtib põhimõte, et eelisjärjekorras kohaldatakse eriseadust; kui aga eriseaduses asjakohaseid sätteid ei ole või need on ebaselged, tuleks viidata üldseadusele.

Vastavalt kõnealusele struktuurile võib eristada kolme üldseaduste ja eriseaduste kombinatsiooni. Alljärgnevalt on esitatud nende kokkuvõtlik kirjeldus.

2.2.2. *Komisjoni suhtes kohaldatav kord*

Kui komisjon on kaasatud, kohaldatakse määrust 45/2001, sealhulgas Euroopa andmekaitseinspektori rolli osas, olenemata sellest, kas andmetöötlustoiminguid teostatakse esimese (kavandatav määrus) või kolmanda samba (kavandatav otsus) raames.

Kavandatava otsuse põhjenduses 21 sätestatakse järgmist: "Isikuandmete töötlemise suhtes Euroopa Komisjoni poolt kohaldatakse (…) määrust (EÜ) nr 45/2001 (…), kui töötlemine toimub nende tegevuste raames, mis täielikult või osaliselt kuuluvad ühenduse õiguse reguleerimisalasse. Osaliselt kuulub isikuandmete töötlemine SIS IIs ühenduse õiguse alla".

Sellel on praktilised põhjused: selles osas, mis puutub komisjoni, oleks tõepoolest äärmiselt raske määratleda, kas andmeid töödeldakse esimese või kolmanda samba seadusandluse alla kuuluvate tegevuste raames.

Peale selle on ühe õigusakti kohaldamine kõigi komisjoni poolt SIS II raames läbiviidavate tegevuste suhtes mitte ainult praktilisest seisukohast mõistlik, vaid see suurendab ka järjepidevust (tagades vastavalt kavandatava otsuse põhjendusele 21 "isikute põhiõiguste ja –vabaduste kaitset isikuandmete töötlusel käsitlevate eeskirjade" järjepideva ja ühtse kohaldamise). Seetõttu tervitab Euroopa andmekaitseinspektor selle tunnistamist komisjoni poolt, et määrust 45/2001 kohaldatakse kõigi komisjoni poolt SIS II raames teostatavate andmetöötlustoimingute suhtes.

2.2.3. *Liikmesriikide suhtes kohaldatav kord*

Liikmesriikide osas on olukord keerulisem. Kavandatava määruse kohast isikuandmete töötlemist reguleerib kavandatav määrus ise ning direktiiv 95/46/EÜ. Kavandatava määruse põhjendusest 14 nähtub väga selgesti, et direktiivi tuleb käsitada üldseadusena ning SIS II käsitlevat määrust eriseadusena. Sellel on rida tagajärgi, mis leiavad allpool üksikasjalikumat käsitlemist.

Kavandatava otsuse puhul on andmekaitsealaseks referentsõigusaktiks (*lex generalis*) konventsioon nr 108, mis võib mõnes osas kaasa tuua olulise erinevuse esimese ja kolmanda samba alla kuuluvate andmekaitsekordade vahel.

2.2.4. *Mõju andmekaitse tasemele*

Andmekaitse sellist korraldust käsitleva üldise märkusena rõhutab Euroopa andmekaitseinspektor järgmist:

— Kavandatava määruse kohaldamine direktiivi 95/46/EÜ eriseadusena (ning analoogselt sellele kavandatava otsuse kohaldamine konventsiooni nr 108 eriseadusena) ei tohiks mingil juhul viia direktiivi või konventsiooniga tagatud andmekaitsetaseme langemiseni. Euroopa andmekaitseinspektor esitab oma sellekohased soovitused (vt nt õigus kasutada õiguskaitsevahendeid).

([1]) (KOM (2005) 475 lõplik).

— Samamoodi ei tohi õigusaktide kombineeritud kohaldamise tagajärjeks olla praeguse Schengeni konventsiooniga tagatud andmekaitsetaseme langus (vt nt allpool esitatud märkused direktiivi 95/46/EÜ artikli 13 kohta).

— Kahe erineva õigusakti kohaldamine, olenemata selle vajalikkusest Euroopa õigusliku raamistiku tõttu, ei tohiks viia põhjendamatute lahknevusteni asjaomaste isikute andmete kaitse vahel töödeldavate andmete liigist tulenevalt. Seda tuleb vältida niipalju kui võimalik. Allpool toodud soovituste eesmärk on samuti suurendada niipalju kui võimalik järjepidevust (vt nt riiklike järelevalveasutuste volitused).

— Õiguslik raamistik on nii keerukas, et see tekitab väga tõenäoliselt mõningast segadust praktilisel rakendamisel. Mõnedel juhtudel on raske mõista, milline on üldseaduste ja eriseaduste omavaheline mõju ning seda oleks otstarbekas ettepanekutes selgitada. Peale selle on kirjeldatud keerulises õiguskeskkonnas väga kasulik soovitus, mille Schengeni ühine järelevalveasutus esitas oma arvamuses SIS II kavandatava õigusliku aluse kohta (27. september 2005) ning mille kohaselt võiks välja töötada "vademeekumi", milles loetletakse kõik SIS IIga seonduvad olemasolevad õigused ning esitatakse kohaldatavate õigusaktide selge hierarhia.

Sellest tulenevalt püütakse käesoleva arvamusega tagada kõrgetasemeline andmekaitse, järjepidevus ja selgus, et anda andmesubjektile vajalik õiguskindlus.

2.2.5. *Andmekaitset kolmanda samba raames käsitleva raamotsuse eelnõu mõju*

Konventsioon nr 108 kui SIS II käsitleva otsuse andmekaitsealane referentsdokument asendatakse raamotsusega andmekaitse kohta kolmanda samba raames ([1]). Ettepanekus seda ei mainita, kuid see tuleneb kavandatavast raamotsusest. Selle artikli 34 lõikes 2 sätestatakse, et "kõiki viiteid Euroopa Nõukogu 28. jaanuari 1981. aasta konventsioonile nr 108 üksikisikute kaitse kohta isikuandmete automaattöötlusel käsitletakse viidetena käesolevale raamotsusele." Euroopa andmekaitseinspektor esitab eelolevatel nädalatel eraldi arvamuse raamotsuse eelnõu kohta ning ei analüüsi käesolevas arvamuses üksikasjalikult selle sisu. Kui aga raamotsuse kohaldamine avaldab tõenäoliselt märkimisväärset mõju SIS II andmekaitsekorrale, ei jäeta seda märkimata.

2.2.6. *Direktiivi 95/46/EÜ artikli 13 ja konventsiooni nr 108 artikli 9 kohaldamine*

Direktiivi 95/46/EÜ artiklis 13 ja konventsiooni nr 108 artiklis 9 sätestatakse, et liikmesriigid võivad võtta seadusandlikke meetmeid, et piirata neis ette nähtud kohustuste ja õiguste ulatust, kui selline piirang on vajalik muude oluliste huvide kaitsmiseks (nt riiklik julgeolek, riigikaitse, avalik julgeolek) ([2]).

Nii kavandatava määruse kui kavandatava otsuse põhjendustes mainitakse, et liikmesriigid võiksid seda võimalust kasutada ettepanekute siseriiklikul rakendamisel. Sellisel juhul peaks olema täidetud kaks eeldust: direktiivi 95/46/EÜ artikli 13 kohaldamine peab olema kooskõlas Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikliga 8 ja ei tohiks viia kehtiva andmekaitsekorra halvenemiseni.

See on veelgi olulisem SIS II puhul, kuna süsteem peab olema usaldusväärne. Kuna liikmesriigid jagavad omavahel andmeid, peab olema võimalik saada piisavalt usaldusväärset teavet selle kohta, kuidas neid riiklikul tasandil töödeldakse.

Sellega seoses on eelkõige üks murettekitav asjaolu, mille puhul ettepanekud võiksid viia praeguse andmekaitsetaseme langemiseni. Schengeni konventsiooni artiklis 102 sätestatakse sellise süsteemi loomine, mille puhul andmete kasutamine on isegi riiklike õigusaktidega rangelt reguleeritud ja piiritletud ("Andmekasutust, mis ei vasta lõigetele 1–4, käsitatakse konventsiooniosalise siseriikliku õiguse kohaselt väärkasutusena"). Nii direktiivis 95/46/EÜ kui konventsioonis nr 108 sätestatakse aga, et riiklike õigusaktidega võib kehtestada erandeid muu hulgas ka eesmärgi suhtes kohaldatavate piirangute põhimõttest. Kui seda tehakse, kujutaks see endast vastuolu Schengeni konventsiooniga kehtestatud praeguse süsteemiga, mille kohaselt riiklik seadusandlus ei tohi kõrvale kalduda eesmärgi ja kasutuse suhtes kohaldatavate piirangute põhimõttest.

Raamotsuse vastuvõtmine ei muudaks kõnealuse tähelepaneku puhul midagi: probleem seisneb nimelt pigem SIS II andmete töötlemisel range eesmärgikohase piirangu põhimõtte säilitamises kui selle tagamises, et andmeid töödeldaks kooskõlas raamotsusega.

([1]) Lisaks asendatakse sellega Schengeni konventsioonis ette nähtud üldine andmekaitsekord (Schengeni konventsiooni artiklid 126–130). Nimetatud korda ei kohaldata SISi suhtes.

([2]) Liikmesriik, kes soovib kasutada nimetatud võimalust õiguste piiramiseks, võib seda - nagu eespool mainitud - teha üksnes kooskõlas Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikliga 8.

Euroopa andmekaitseinspektor teeb ettepaneku lisada SIS II käsitlevatesse ettepanekutesse (täpsemalt kavandatava määruse artiklisse 21 ja kavandatava otsuse artiklisse 40) samasuguse mõjuga säte kui Schengeni konventsiooni artikli 102 praegune lõige 4, milles piiratakse liikmesriikide võimalust sätestada selliste andmete kasutamine, mida ei ole mainitud SIS II käsitlevates tekstides. Teine võimalus oleks kavandatavas otsuses ja kavandatavas määruses selgesõnaliselt piirata nende erandite ulatust, mida võib direktiivi artikli 13 ja konventsiooni artikli 9 kohaselt kasutada, sätestades näiteks, et liikmesriigid võivad piirata üksnes juurdepääsu- ja teabe saamise õigust, kuid mitte andmete kvaliteeti käsitlevaid põhimõtteid.

3. **EESMÄRK**

Vastavalt kummagi dokumendi artiklile 1 (“SIS II loomine ja üldeesmärk”), luuakse SIS II, et “liikmesriikide pädevad asutused saaksid teha koostööd, vahetades teavet isikute ja esemete kontrollimiseks” ning süsteem “aitab kaasa kõrgetasemelise turvalisuse säilitamisele liikmesriikide vaheliste sisepiirikontrollideta alal”.

SIS II eesmärk on sõnastatud üsna üldsõnaliselt; eespool nimetatud sätted ei sisalda iseenesest täpset määratlust, mida nimetatud eesmärk hõlmab (tähendab).

SIS II eesmärk näib märksa laiem kui praeguse SISi eesmärk, mis on sätestatud Schengeni konventsiooni artiklis 92, milles märgitakse eelkõige, et “(Schengeni infosüsteemi kaudu saavad konventsiooniosaliste määratud asutused …) kätte teated isikute ja esemete kohta piirikontrolli ning muude riigis siseriikliku õiguse kohaselt tehtavate politsei- ja tollikontrollide korral, ning artiklis 96 osutatud teatekategooria korral selleks, et anda viisasid ja elamislube ning rakendada välismaalaste õigusi (…)”.

Nimetatud laiem eesmärk tuleneb ka SIS II-le selliste uute funktsioonide ja juurdepääsuõiguste lisamisest, mis ei kuulu esialgse isikute ja esemete kontrollimise eesmärgi, vaid pigem uurimisvahendile kohase eesmärgi alla. Eelkõige on ette nähtud selliste asutuste juurdepääs SIS II andmetele, kes kasutavad neid enda eesmärkidel ning mitte SIS II eesmärkide saavutamiseks (vt allpool); hoiatusteadete omavahelist seostamist üldistatakse, kuna see on politsei poolt kasutatava uurimisvahendi tüüpiline tunnusjoon.

Peale selle on küsimusi seoses eelseisvatel aastatel väljatöötatava biomeetriliste tunnuste otsingumootoriga, mis võimaldab teostada süsteemis kontrollisüsteemi vajadusi ületavaid päringuid.

Kokkuvõtlikult võib öelda, et ettepanekutel on palju laiem reguleerimisala kui olemasoleval õigusraamistikul. Seega on vaja täiendavaid kaitsemeetmeid. Sellega seoses keskendub Euroopa andmekaitseinspektor oma analüüsis mitte niivõrd artiklis 1 esitatud üldisele määratlusele, vaid SIS II funktsioonidele ja muudele süsteemi koostisosadele.

4. **MÄRKIMISVÄÄRSED MUUDATUSED SIS IIS**

Selles peatükis keskendutakse esmalt SIS IIga kaasnevatele uutele elementidele, nimelt biomeetria kasutuselevõtmisele, uutele, eelkõige Europolile ja Eurojustile antavatele juurdepääsuõigustele, sõidukite registreerimise eest vastutavatele asutustele, hoiatusteadete omavahelisele seostamisele ja erinevate asutuste juurdepääsule sisserände alastele andmetele.

4.1. **Biomeetria**

SIS II käsitlevate ettepanekutega viiakse sisse võimalus töödelda uut liiki andmeid, mis väärivad erilist tähelepanu, nimelt biomeetrilisi andmeid. Nagu Euroopa andmekaitseinspektor oma viisainfosüsteemi käsitlevas arvamuses ([1]) juba rõhutas, nõuab biomeetrilistele andmetele omane tundlikkus erilisi kaitsemeetmeid, mida SIS II käsitlevad ettepanekud ei sisalda.

Üldise märkusena võib öelda, et biomeetriliste andmete kasutamine kogu ELi hõlmavates infosüsteemides (VIS, EURODAC, juhilubade infosüsteem jne) näitab pidevat tõusutendentsi, kuid sellega kaasnevatele ohtudele ja vajalikele kaitsemeetmetele ei pöörata piisavat tähelepanu.

Seda põhjalikumate asjakohaste kaalutluste vajadust rõhutati ka biomeetria alases resolutsioonis, mis võeti hiljuti vastu Montreux’s toimunud rahvusvahelisel andmekaitsevolinike konverentsil ([2]). Seni on seisnud küsimuse puhul, milline on standardite väljatöötamisega kaasnev lisandväärtus, tähelepanu keskmes üksnes süsteemide vaheline koostalitusvõime ja mitte biomeetriliste andmete töötlemise kvaliteedi parandamine.

([1]) Euroopa andmekaitseinspektori 23. märtsi 2005. aasta arvamuse (Euroopa Parlamendi ja nõukogu määruse kohta, mis käsitleb viisainfosüsteemi ja liikmesriikidevahelist teabevahetust lühiajaliste viisade kohta) punkt 3.4.2.

([2]) 16. septembril 2005 Montreux’s toimunud 27. rahvusvaheline andmekaitse ja eraelu puutumatuse eest vastutavate volinike konverents; resolutsioon biomeetriliste andmete kasutamise kohta passides, isikutunnistustel ja reisidokumentides.

Otstarbekas oleks välja töötada kõnealuste andmete spetsiifilisust arvesse võtvate ühiste kohustuste või nõuete kogum ja ühine metoodika selliste kohustuste või nõuete rakendamiseks. Kõnelaused ühised nõuded võiksid sisaldada eelkõige järgmisi elemente (mille vajalikkust näitavad SIS II käsitlevad ettepanekud):

— **Suunatud mõjuhindamine:** Tuleb rõhutada, et ettepanekute suhtes ei ole läbi viidud biomeetriliste andmete kasutamisele keskenduvat mõjuhindamist ([1]).

— **Registreerimismenetluse rõhutamine:** Biomeetriliste andmete allikat ja nende kogumise viisi ei ole täpsemalt kirjeldatud. Registreerimine on keskse tähtsusega samm isiku biomeetrilise tuvastamise protsessis; seda ei ole võimalik paika panna lisades või alltöörühmade koosolekutel toimuvatel aruteludel, kuna sellest sõltub otseselt protsessi lõpptulemus, s.t valedel alustel tagasilükkamiste või valedel alustel heakskiitmiste määr.

— **Täpsuse määra esiletõstmine:** Biomeetriliste andmete kasutamine isiku tuvastamisel (võrdlus: üks mitmele), mida ettepanekus esitletakse "biomeetrilise otsingumootori" tulevase rakendusvõimalusena, on problemaatilisem, kuna selle protsessi tulemuste täpsuse määr on madalam kui autentimise või kontrollimise puhul (võrdlus: üks ühele). Isiku biomeetrilisest tuvastamisest ei tohiks seetõttu kujuneda isikutuvastamise ainus meetod ega ainus juurdepääsuvõimalus täiendavale teabele.

— **Varumenetlus:** Hõlpsasti kättesaadavaid varumenetlusi rakendatakse, et austada nende isikute väärikust, kes on valesti tuvastatud ning vältida seda, et nad kannataksid süsteemi puuduste all.

Biomeetriliste andmete kasutamine ilma nõuetekohase eelhindamiseta näitab samuti, et biomeetria usaldusväärsust ülehinnatakse. Biomeetrilised andmed "elavad" ja muutuvad aja jooksul; andmebaasis säilitatavad näidised kujutavad endast vaid dünaamilise tunnuse hetkeülesvõtet. Selle püsivus ei ole tagatud ning seda tuleb kontrollida. Biomeetriliste andmete täpsust tuleb alati vaadelda koostoimes teiste tunnustega, kuna see ei ole kunagi eksimatu.

([1]) Hindamine võiks põhineda nn seitsmel biomeetrilise tarkuse alustalal, mis on esitatud väljaandes "*Biometrics at the frontiers: Assessing the impact on Society*", IPTS, DG-JRC, EUR 21585 EN, osa 1.2, lk 32.

SIS II andmete võimalik kasutamine uurimise eesmärgil toob kaasa tõsiseid ohte andmesubjektile, kui tuginetakse eelkõige biomeetrilistele tõenditele või omistatakse neile liiga suurt tähtsust, nagu varasematel juhtudel on selgunud ([2]).

Seetõttu tuleks ettepanekutes tunnistada biomeetria tõelisi võimalusi isiku tuvastamisel ning tõsta sellekohast teadlikkust.

4.2. **Juurdepääs SIS II andmetele**

4.2.1. *Uus nägemus juurdepääsuõigusest*

Asutused, millel on juurdepääs SISi andmetele, määratletakse iga hoiatusteate puhul eraldi. Põhimõtteliselt peab SISi andmetele juurdepääsu andmiseks olema täidetud kaks eeldust: juurdepääs tuleb anda asutustele, kes vastavad täielikult SISi üldeesmärgile ja iga hoiatusteate erieesmärgile.

See tuleneb nii kavandatavas määruses kui kavandatavas otsuses esitatavast hoiatusteate määratlusest (mõlema dokumendi artikli 3 lõike 1 punktis a sätestatakse: *hoiatusteade — SIS II sisestatud andmekogum, mis võimaldab pädevatel asutustel teha kindlaks isik või objekt vajaliku erimeetme võtmiseks*). Kavandatava otsuse artikli 39 lõikes 3 kinnitatakse eeltoodut, sätestades, et "*lõikes 1 osutatud andmeid kasutatakse ainult isiku tuvastamiseks konkreetse meetme rakendamiseks kooskõlas käesoleva otsusega*". Selles suhtes on SIS IIs endiselt elemente, mis iseloomustavad kokkulangevusest või selle puudumisest teada andvat süsteemi, mille puhul hoiatusteade sisestatakse kindla eesmärgiga (üleandmine, sisenemiskeeld jne).

SISi andmetele juurdepääsu omavate asutustele kehtib nende andmete suhtes *de facto* kasutuspiirang, kuna nad saavad andmetele põhimõtteliselt juurdepääsu üksnes vajaliku erimeetme võtmiseks.

Mõned uutes ettepanekutes antud juurdepääsuõigused ei ole siiski selle loogikaga vastavuses, kuna nende eesmärk seisneb asutuse teabega varustamises ja mitte selles, et võimaldada asutusel isikut tuvastada ja võtta hoiatusteatega ette nähtud meede.

([2]) 2004. aasta juunis hoiti Portlandist (USA) pärit advokaati kaks nädalat vangistuses, kuna FBI tegi kindlaks, et tema sõrmejälg sobis sõrmejäljega, mis leiti Madridi terrorirünnakute uurimisel (detonaatorit sisaldanud kilekotilt). Lõpuks suudeti aga tõestada, et võrdlusprotsess oli ebakorrektne ning viis väärtõlgenduseni.

See puudutab täpsemalt järgmist:

— varjupaigaasutuste juurdepääs sisserände alastele andmetele;

— pagulasseisundi andmise eest vastutavate asutuste juurdepääs sisserände alastele andmetele;

— Europoli juurdepääs hoiatusteadetele, mis käsitlevad väljaandmist, varjatud jälgimist ja varastatud dokumente nende konfiskeerimiseks;

— Eurojusti juurdepääs väljaandmist ja lokaliseerimist käsitlevatele andmetele.

Kõigi nende asutuste puhul kehtib SIS II andmetega seoses järgmine:

nad ei saa võtta hoiatusteate määratluses nimetatud erimeedet. Neile antakse juurdepääs teabe hankimiseks nende endi tarbeks.

Isegi nende asutuste puhul tuleb aga eristada asutusi, kellel on andmetele juurdepääs oma tarbeks, kuid üsna konkreetse eesmärgiga, ning neid (nimelt Europol ja Eurojust), kelle puhul ei ole juurdepääsu eesmärki üldse täpsustatud. Nt varjupaigaasutustele antakse juurdepääs kindlal eesmärgil, isegi kui see ei ole hoiatusteates nimetatud eesmärk. Neil on võimalus juurde pääseda sisserände alastele andmetele, "et nad saaksid kindlaks määrata, kas varjupaigataotleja on viibinud ebaseaduslikult teise liikmesriigi territooriumil". Europolil ja Eurojustil on aga juurdepääs teatavate hoiatusteate kategooriate alla kuuluvatele andmetele, "mis on vajalikud nende ülesannete täitmiseks".

Kokkuvõtlikult antakse juurdepääs SIS II andmetele kolmel eesmärgil:

— hoiatusteates märgitud meetme rakendamiseks;

— SIS IIs märgitust erineval, kuid ettepanekutes täpselt piiritletud eesmärgil;

— SIS IIs märgitust erineval eesmärgil, mida ei ole aga täpselt kirjeldatud.

Euroopa andmekaitseinspektor on seisukohal, et mida üldisem on juurdepääsu andmise eesmärk, seda rangemad peavad olema rakendatavad kaitsemeetmed. Alljärgnevalt kirjeldatakse üksikasjalikult üldiseid kaitsemeetmeid; seejärel käsitletakse Europoli ja Eurojusti eriolukorda.

4.2.2. *Juurdepääsu andmise tingimused*

1. Juurdepääs antakse igal juhul üksnes siis, kui see on kooskõlas SIS II üldeesmärgi ja õigusliku alusega.

Praktikas tähendab see seda, et juurdepääs sisserände alastele andmetele peab kavandatava määruse kohaselt toetama selliste poliitikate elluviimist, mis on seotud nende isikute liikumisega, kelle suhtes kohaldatakse Schengeni *acquis*'d.

Analoogselt sellele peab otsuses nimetatud hoiatusteadetele antav juurdepääs olema suunatud politsei- ja õigusasutuste vahelise kriminaalasjades tehtava operatiivkoostöö toetamisele.

Seoses sellega juhib Euroopa andmekaitseinspektor tähelepanu peatükile, milles käsitletakse sõidukite registreerimistunnistusi väljaandvate teenistuste juurdepääsu SIS II-le (vt allpool punkt 4.6).

2. Vajadust SIS II andmetele juurde pääseda tuleb tõendada, nagu ka seda, et andmete hankimine muid, vähem pealetükkivaid vahendeid kasutades on võimatu või äärmiselt raske. Seda oleks tulnud käsitleda seletuskirjas, mille puudumine on — nagu juba öeldud — väga kahetsusväärne.

3. Andmete kasutamine tuleb määratleda selgesõnaliselt ja piiritlevalt.

Varjupaigaasutustel on nt juurdepääs sisserände alastele andmetele, "et nad saaksid kindlaks määrata, kas varjupaigataotleja on viibinud ebaseaduslikult teise liikmesriigi territooriumil". Europolil ja Eurojustil on aga juurdepääs teatavat liiki hoiatusteadetes sisalduvatele andmetele, "mis on vajalikud nende ülesannete täitmiseks". Viimane ei ole piisavalt üksikasjalik selgitus (vt allpool).

4. Juurdepääsu tingimused peavad olema täpselt määratletud ja piiritletud. Eelkõige peaksid SIS II-le saama juurdepääsu vaid selliste organisatsioonide üksused, mis peavad tegelema SIS II andmetega. Sellele kavandatava otsuse artiklis 40 ja kavandatava määruse artikli 21 lõikes 2 sätestatud kohustusele tuleks lisada riiklike asutuste kohustus pidada ajakohastatud registrit isikutest, kellel on SIS II-le juurdepääsu luba. Sama peaks kehtima ka Europoli ja Eurojusti suhtes.

5. Asjaolu, et neil asutustel on juurdepääs SIS II andmetele, ei saa olla põhjendus andmete süsteemi sisestamiseks või nende säilitamiseks süsteemis, kui andmed ei ole vajalikud selle konkreetse hoiatusteate seisukohast, mille osaks nad on. Uusi andmekategooriaid ei ole lubatud lisada sel põhjusel, et neist oleks kasu teistele infosüsteemidele. Kavandatava otsuse artiklis 39 sätestatakse näiteks hoiatusteate väljastanud asutust käsitlevate andmete sisestamine hoiatusteatesse. Neid andmeid ei ole vaja meetme võtmiseks (vahistamine, jälgimine jne) ning ainus põhjus nende sisseviimiseks oleks tõenäoliselt kasu, mida sellest saaks Europol või Eurojust. Nimetatud andmete töötlemist tuleks seega selgelt põhjendada.

6. Andmete säilitamise aega ei tohi pikendada, kui see ei ole vajalik sel eesmärgil, milleks andmed sisestati. See tähendab, et isegi kui Europolil või Eurojustil on andmetele juurdepääs, ei ole see piisav põhjus nende süsteemis säilitamiseks (nt tuleks niipea, kui tagaotsitav isik on välja antud, tema andmed kustutada, ehkki need võiksid olla Europolile kasulikud). Siin on taas vaja hoolikat järelevalvet tagamaks, et riiklikud asutused eeltoodut järgiksid.

4.2.3. *Europoli ja Eurojusti juurdepääs*

a. *Juurdepääsu põhjused*

Europoli ja Eurojusti juurdepääsu üle mõnedele SISi andmetele arutleti juba enne, kui neile nõukogu 24. veebruari 2005. aasta otsusega ([1]) juurdepääsuõigus anti. Kõigist enda tarbeks juurdepääsu omavatest asutustest omavad nimetatud asutused kõige laialdasemat juurdepääsu. Olgugi, et kõnealuste andmete kasutust on kirjeldatud otsuse XII peatükis, ei ole piisavalt põhjendatud, miks juurdepääs üleüldse anti. See omab seda suuremat tähendust, et Europoli ja Eurojusti ülesanded aja jooksul tõenäoliselt laienevad.

Euroopa andmekaitseinspektor kutsub komisjoni tungivalt üles piiritlema neid ülesandeid, mille täitmiseks Europoli ja Eurojusti juurdepääs oleks õigustatud.

b. *Andmetele juurdepääsu piiramine*

Vältimaks seda, et Europol ja Eurojust teostavad süsteemis sihipäratuid päringuid, ja kindlustamaks, et neil on juurdepääs vaid andmetele, "mis on vajalikud nende ülesannete täitmiseks", soovitas Schengeni ühine järelevalveasutus oma 27. septembri 2005. aasta arvamuses SIS II käsitlevate ettepanekute kohta piirata Europoli ja Eurojusti juurdepääsu selliste isikute andmetega, kelle nimi juba esineb nende endi toimikutes. Sellega tagataks, et Europol ja Eurojust tutvuksid vaid neile vajalike hoiatusteadetega. Euroopa andmekaitseinspektor toetab nimetatud soovitust.

c. *Turvalisusega seotud aspektid*

Euroopa andmekaitseinspektor tervitab kõikide Europoli ja Eurojusti poolt teostatud toimingute registreerimise kohustust ning süsteemi osade kopeerimise või mahalaadimise keeldu.

Kavandatava otsuse artiklis 56 nähakse Europolile ja Eurojustile ette üks või kaks juurdepääsupunkti. Nii mõistetav, kui see ka ei ole, et liikmesriigid vajavad oma pädevate asutuste detsentraliseeritud struktuuri tõttu rohkem kui ühte juurdepääsupunkti, ei õigusta seda taotlust aga Europoli ja Eurojusti staatus ja tegevused. Peale selle tuleb rõhutada, et turvalisuse seisukohast suurendab juurdepääsupunktide hulga suurenemine väärkasutuste ohtu ja seetõttu tuleks seda asjakohasemate argumentidega põhjendada. Veenvate argumentide puudumisel teeb Euroopa andmekaitseinspektor ettepaneku anda Europolile ja Eurojustile ainult üks juurdepääsupunkt.

4.3. **Hoiatusteadete omavaheline seostamine**

Määruse artiklis 26 ja otsuse artiklis 46 sätestatakse, et liikmesriigid võivad kooskõlas oma riiklike õigusaktidega luua hoiatusteateid ühendavaid linke, et luua seos kahe või enama hoiatusteate vahel.

Kuigi hoiatusteadete vahelised lingid võivad kontrollimiseks olla tõesti kasulikud (nt võib linkida autovarga suhtes tehtud vahistamismääruse varastatud autot käsitleva hoiatusteatega), on teadete omavaheline linkimine väga iseloomulik politsei poolt kasutatavale uurimisvahendile.

Hoiatusteadete omavaheline seostamine võib avaldada märkimisväärset mõju asjaomaste isikute õigustele, kuna isikut ei "hinnata" enam ainult temaga seonduvate andmete põhjal, vaid tema võimaliku seose põhjal teiste isikutega. Isikuid, kelle andmed on lingitud kurjategijate või tagaotsitavate isikute andmetega, koheldakse tõenäoliselt suurema umbusuga kui teisi. Peale selle tähendab hoiatusteadete omavaheline seostamine ka SISi uurimisvolituste laiendamist, kuna seeläbi saab võimalikuks väidetavate kuritegelike jõukude või rühmituste registreerimine (kui nt ebaseaduslike sisserändajate andmed lingitakse inimkaubitsejate andmetega). Lisaks tuleb mainida, et kuna linkide loomine toimub kooskõlas riiklike õigusaktidega, on selle võimalikuks tagajärjeks ka see, et liikmesriigid võivad luua oma õigusaktidega kooskõlas olevaid linke, mis on aga mõnes teises liikmesriigis ebaseaduslikud, sisestades seega süsteemi "ebaseaduslikke" andmeid.

([1]) Nõukogu 24. veebruari 2005. aasta otsus 2005/211/JSK Schengeni infosüsteemi jaoks mõnede uute, sealhulgas terrorismivastast võitlust käsitlevate toimingute sisseseadmise kohta (ELT L 68, 15.3.2005, lk 44).

Nõukogu 14. juuni 2004. aasta järeldustes SIS II-le seatavate funktsionaalsete nõuete kohta märgiti, et iga lingi loomine peab olema põhjendatud selge talitlusliku vajadusega, see peab põhinema selgelt määratletud seosel ning olema kooskõlas proportsionaalsuse põhimõttega. Lisaks sellele ei tohi see avaldada mõju juurdepääsuõigustele. Kuna aga hoiatusteadete omavaheline seostamine kujutab endast andmetöötlustoimingut, peab see igal juhul olema kooskõlas direktiivi 95/46/EÜ ja/või konventsiooni nr 108 rakendamiseks välja antud riiklike õigusaktide sätetega.

Ettepanekutes kinnitatakse korduvalt, et linkide olemasolu ei tohi muuta juurdepääsuõigusi (vastasel juhul võimaldaks see juurdepääsu andmetele, mille töötlemine ei oleks riiklike õigusaktide kohaselt seaduslik, rikkudes direktiivi artiklit 6).

Euroopa andmekaitseinspektor rõhutab kavandatava määruse artikli 26 ja kavandatava otsuse artikli 46 range tõlgendamise olulisust. Üks võimalus selle tagamiseks on selgitada, et lisaks sellele, et asutustel, kellel ei ole teatavatele andmekategooriatele juurdepääsu õigust, ei ole õigust nendele kategooriatele osutavatele linkidele juurde pääseda, ei tohiks nad nimetatud linkidest isegi mitte teadlikud olla. Linkide visualiseerimine peab olema võimatu, kui lingitud andmetele puudub juurdepääsu õigus.

Peale selle soovib Euroopa andmekaitseinspektor, et temaga konsulteeritaks selle tagamiseks vajalike tehniliste meetmete osas.

4.4. **Hoiatusteated sisenemise keelamiseks**

4.4.1. *Lisamise põhjused*

Kolmandate riikide kodanike suhtes sisenemise keelamiseks väljastatud hoiatusteadete (määruse artikkel 15) kasutamine omab märkimisväärset mõju üksikisiku vabadustele: isik, kelle suhtes on selle sätte alusel sisestatud hoiatusteade, ei tohi mitu aastat Schengeni territooriumile siseneda. Selline hoiatusteade on seni olnud kõige levinum. Arvestades kõnealuse hoiatusteate tagajärgi ning asjaomaste isikute hulka, tuleb selle koostamisel ja rakendamisel üles näidata erilist hoolikust. Kuigi seda tuleb teha ka teiste hoiatusteadete puhul, pühendab Euroopa andmekaitseinspektor sellele hoiatusteatele eraldi peatüki, kuna see põhjustab andmete sisestamise seisukohast erilisi probleeme.

Uus hoiatusteade sisenemise keelamiseks parandab küll praegust olukorda, kuid samas ei ole see päris rahuldav, kuna see põhineb suures osas õigusaktidel, mida ei ole veel vastu võetud või mille kohta ei ole isegi ettepanekut tehtud.

Parandused seisnevad selles, et andmete sisestamise põhjuseid on täpsemalt kirjeldatud. Schengeni konventsiooni praegune sõnastus on viinud olukorrani, kus nende isikute hulk, kelle suhtes on sisestatud konventsiooni artikli 96 alusel hoiatusteade, erineb liikmesriigiti märkimisväärselt. Schengeni ühine järelevalveasutus viis läbi sellekohase põhjaliku uurimuse [1] ning esitas soovitused, mille kohaselt "poliitikakujundajad peaksid kaaluma hoiatusteadete koostamise põhjuste ühtlustamist erinevates Schengeni riikides".

Kavandatav artikkel 15 on koostatud üksikasjalikumalt, mis on väga tervitatav.

Peale selle esitatakse artikli 15 lõikes 2 loetelu juhtudest, mil isikute suhtes ei saa hoiatusteadet sisestada, kuna nad elavad ühte või teist õiguslikku staatust omades seaduslikult mõne liikmesriigi territooriumil. Ehkki selle võiks välja lugeda ka praegusest Schengeni konventsioonist, on praktika näidanud, et ka selle korra kohaldamine erineb liikmesriigiti. Seetõttu on selgitamine tervitatav.

Samas kutsub see säte esile ka teravat kriitikat, kuna see põhineb olulises osas tekstil, mida ei ole veel vastu võetud, nimelt tagasisaatmist käsitleval direktiivil.

Pärast SIS II käsitlevate ettepanekute vastuvõtmist esitas komisjon (1. septembril 2005) ettepaneku, mis käsitleb direktiivi liikmesriikides kohaldatavate ühiste standardite ja menetluste kohta riigi territooriumil ebaseaduslikult viibivate kolmanda riigi kodanike tagasisaatmiseks, kuid niikaua, kui seda teksti ei ole lõplikult vastu võetud, ei saa seda käsitada piisava põhjusena andmete süsteemi sisestamiseks. See rikuks eelkõige Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklit 8, kuna sekkumine isikute eraellu peab muu hulgas põhinema selgetel ja kättesaadavatel õigusaktidel.

Seetõttu kutsub Euroopa andmekaitseinspektor komisjoni tungivalt üles seda sätet tagasi võtma või seda olemasolevate õigusaktide alusel uuesti sõnastama, võimaldamaks isikutel teada, milliseid meetmeid asutused võivad tema suhtes võtta.

4.4.2. *Juurdepääs artikli 15 kohastele hoiatusteadetele*

Artiklis 18 sätestatakse, millistel asutustel on neile hoiatusteadetele juurdepääs ja mis eesmärgil. Artikli 18 lõigetes 1 ja 2 määratletakse, millistel asutustel on juurdepääs hoiatusteadetele, mis on sisestatud tagasisaatmist käsitleva direktiivi alusel. Siinkohal kehtivad samad märkused, mis eespool.

[1] Schengeni Ühise Järelevalveasutuse aruanne artikli 96 kohaste hoiatusteadete kasutamist Schengeni infosüsteemis käsitleva uurimuse kohta (Brüssel, 20. juuni 2005).

Kavandatava määruse artikli 18 lõikega 3 antakse juurdepääs põgenikustaatuse andmise eest vastutavatele asutustele vastavalt direktiivile, mille kohta ei ole isegi veel ettepanekut tehtud. Kättesaadava teksti puudumise tõttu peab Euroopa andmekaitseinspektor osutama veel kord eeltoodud märkustele.

4.4.3. *Artikli 15 kohaste hoiatusteadete säilitamise tähtaeg*

Artikli 20 kohaselt ei tohi hoiatusteadet säilitada (välja- või tagasisaatmist käsitlevas) otsuses sätestatud sisenemiskeelu kehtivusajast kauem. See on kooskõlas andmekaitseeeskirjadega. Lisaks sellele kustutatakse hoiatusteade automaatselt viie aasta pärast, kui liikmesriik, kes andmed SIS IIte sisestas, ei otsusta teisiti.

Nõuetekohane järelevalve riiklikul tasandil peaks tagama, et ei toimuks andmete säilitusaja põhjendamatut automaatset pikendamist ja et liikmesriigid kustutaksid andmed enne viieaastase tähtaja möödumist, kui sisenemiskeelu kehtivusaeg on lühem.

4.5. **Säilitamise tähtajad**

Kuigi säilitamise suhtes kehtiv põhimõte jääb samaks (reeglina tuleks hoiatusteade SIS IIst kustutada, niipea kui hoiatusteates nõutud meede on võetud), on ettepanekute tulemuseks see, et hoiatusteadete säilitamise tähtaega on üldiselt pikendatud.

Schengeni konventsiooni kohaselt tuleb andmete edasise säilitamise vajalikkus läbi vaadata hiljemalt kolm aastat pärast nende sisestamist (või hiljemalt ühe aasta pärast, kui need sisestati varjatud jälgimiseks). Uutes ettepanekutes nähakse ette, et andmed kustutatakse automaatselt (mille teate väljastanud liikmesriik võib vaidlustada) sisserände alaste andmete puhul 5 aasta möödudes, vahistamist, kadunud isikuid ja kohtumenetluse jaoks otsitavaid isikuid käsitlevate andmete puhul 10 aasta möödudes ja 3 aasta möödudes selliste isikute andmete puhul, kelle suhtes on ette nähtud varjatud jälgimise kohaldamine.

Ehkki liikmesriigid on põhimõtteliselt kohustatud andmed kustutama, kui hoiatusteate eesmärk on täidetud, viib see andmete maksimaalse säilitusaja märkimisväärse pikenemiseni (enamikul juhtudest kolmekordistumiseni), ilma et komisjon seda kuidagi põhjendaks. Sisserände alaste andmete puhul võib üksnes oletada, et säilitusaja viieaastane kestus on seotud sisenemiskeelu kestusega, nagu soovitatud tagasisaatmist käsitleva direktiivi eelnõus. Kõigil muudel juhtudel ei ole Euroopa andmekaitseinspektori teada põhjendust.

Võimalik mõju andmesubjektidele, kelle suhtes SISi on sisestatud hoiatusteateid, võib omada asjaomaste isikute elus märkimisväärseid tagajärgi. Eriti murettekitav on see hoiatusteadete puhul, mis on sisestatud isikute varjatud jälgimiseks või erikontrolliks, kuna sellised hoiatusteated võivad olla sisestatud pelga kahtluse alusel.

Euroopa andmekaitseinspektor sooviks, et andmete säilitamise tähtaegade sellist pikendamist asjakohaselt põhjendataks. Veenva põhjenduse puudumisel soovitab ta lühendada tähtaegu nende praeguse kestuseni, mida ta soovib eelkõige näha varjatud jälgimiseks või erikontrolliks sisestatud hoiatusteadete puhul.

4.6. **Sõidukite registreerimistunnistuste väljaandmise eest vastutavate asutuste juurdepääs**

Põhiprobleem seisneb selles, et valitud on enam kui küsitava väärtusega õiguslik alus. Komisjonil ei õnnestu veenvalt põhjendada, miks kasutada "transporti" käsitlevat esimese samba õiguslikku alust meetme joaks, mis annaks haldusasutustele juurdepääsu SISile kuritegevuse (varastatud sõidukitega kauplemine) ennetamiseks ja selle vastu võitlemiseks. SIS II-le juurdepääsu andmiseks veenva põhjenduse ja nõuetekohase õigusliku aluse vajadust on üksikasjalikult kirjeldatud käesoleva arvamuse punktis 4.2.2.

Euroopa andmekaitseinspektor osutab antud teema kohastele märkustele, mille Schengeni ühine järelevalveasutus esitas oma arvamuses SIS II kavandatava õigusliku aluse kohta. Eelkõige tuleks järgida Schengeni ühise järelevalveasutuse soovitust muuta kavandatavat otsust kõnealuse juurdepääsuõiguse hõlmamiseks.

5. KOMISJONI JA LIIKMESRIIKIDE ÜLESANDED

SIS IIga seonduvate kohustuste selge kirjeldus ja jaotus on esmatähtis mitte üksnes süsteemi tõrgeteta toimimiseks, vaid ka järelevalve seisukohast. Järelevalvealaste pädevuste jaotus tuleneb kohustuste kirjeldusest, mistõttu on vajalik selle täielik selgus.

5.1. **Komisjoni ülesanded**

Euroopa andmekaitseinspektor tervitab mõlema ettepaneku III peatükki, milles kirjeldatakse komisjoni rolli seoses SIS IIga (milleks on "operatiivjuhtimine"). Selline selgitus puudus VISi käsitlevas ettepanekus. Siiski aga ei määratleta selles peatükis komisjoni rolli ammendavalt. Nagu kirjeldatud käesoleva arvamuse 9. peatükis, osaleb komisjon komiteemenetluse kaudu ka süsteemi rakendamises ja haldamises.

Andmekaitse osas on komisjoni täita roll, mida on juba tunnustatud süsteemide VIS ja Eurodac raames, nimelt vastutab ta operatiivjuhtimise eest. Koos komisjoni põhiülesandega, milleks on süsteemi arendamine ja hooldus, tuleks seda käsitada *sui generis* vastutava töötleja ülesandena. Nagu juba öeldud Euroopa andmekaitseinspektori arvamuses VISi kohta, hõlmab see ülesanne enamat kui volitatud töötleja oma, kuid on samas piiratum kui tavamõistes vastutava töötleja roll, kuna komisjonil ei ole juurdepääsu andmetele, mida SIS II raames töödeldakse.

Kuna SIS II ehitatakse üles keerukatele süsteemidele, millest mõned põhinevad alles esilekerkivatel uutel tehnoloogiatel, nõuab Euroopa andmekaitseinspektor, et suurendataks komisjoni vastutust süsteemi pideval ajakohastamisel ning selleks turvalisuse ja andmekaitsega seotud parimate kättesaadavate tehnoloogiate rakendamisel.

Seetõttu tuleks ettepanekute artiklisse 12 lisada, et komisjon peaks tegema korrapäraselt ettepanekuid selliste uute tehnoloogiate rakendamise kohta, mis esindavad vastava valdkonna tehnika taset, tõstavad andmekaitse ja turvalisuse taset ning hõlbustavad kõnealustele andmetele juurdepääsu omavate riiklike asutuste ülesandeid.

5.2. **Liikmesriikide ülesanded**

Liikmesriikide olukord ei ole päris selge, kuna üsna keeruline on välja selgitada, milline asutus või millised asutused on vastutava töötleja rollis.

Ettepanekutes kirjeldatakse nii SIS II riiklike büroode ülesannet (tagada pädevate asutuste juurdepääs SIS II-le) kui ka SIRENE asutuste rolli (tagada kogu täiendava teabe vahetamine). Liikmesriigid peavad samuti tagama oma NS-i (siseriikliku süsteemi) toimimise ja turvalisuse. Ei ole selge, kas viimatinimetatud ülesannet peab täitma üks eespool nimetatud asutustest. Seda tuleks igal juhul täpsustada.

Andmekaitse osas tuleks komisjoni ja liikmesriike vaadelda ühiste vastutavate töötlejatena, kellest igaühel on oma kindlad kohustused. Nende ülesannete vastastikuse täiendavuse tunnustamine on ainus viis tagada, et ükski SIS II valdkonna tegevus ei jääks järelevalveta.

6. **ANDMESUBJEKTIDE ÕIGUSED**

6.1. **Teavitamine**

6.1.1. *Kavandatav määrus*

Kavandatava määruse artiklis 28 nähakse ette andmesubjekti peamiselt direktiivi 95/46 artiklile 10 tuginev õigus teabele. See on teretulnud muudatus võrreldes praeguse olukorraga, mil konventsioonis ei ole õigust teabele selgesõnaliselt ette nähtud. Mõningad parandused on aga võimalikud järgmiste punktide osas:

Loetellu tuleks lisada teavet, kuna see aitaks kaasa andmesubjekti õiglase kohtlemise tagamisele ([1]). See teave peaks puudutama andmete säilitamise tähtaega, õigust taotleda hoiatusteate väljastamise otsuse läbivaatamist või kaevata see otsus edasi (mõnedel juhtudel; vt kavandatava määruse artikli 15 lõige 3), võimalust saada abi andmekaitseasutuselt ja õiguskaitsevahendite olemasolu.

Kavandatavas määruses ei ole märgitud, millal teavet tuleks anda. See võib teha andmesubjektile õiguste kasutamise võimatuks. Et neid õigusi oleks tegelikkuses võimalik kasutada, tuleks määruses ette näha täpne aeg, mil teavet tuleks anda, vastavalt sellele, milline asutus hoiatusteate väljastas.

Praktiline lahendus oleks lisada hoiatusteadet käsitlev teave otsusesse, millel hoiatusteade algselt põhineb. Selline otsus on kas kohtu- või haldusotsus, mis põhineb avalikku korda (…) ähvardaval ohul, või tagasisaatmisotsus või väljasaatmiskorraldus, millega kaasneb taassisenemiskeeld. Need andmed tuleks lisada määruse artiklile 28.

6.1.2. *Kavandatav otsus*

Otsuse artiklis 50 sätestatakse, et teavet antakse andmesubjekti taotlusel, ja märgitakse ära võimalikud põhjused selle teabe andmisest keeldumiseks. Selle õiguse piirangud on loomulikult mõistetavad, arvestades andmete iseloomu ja nende töötlemise konteksti.

Õigus teabele ei tohiks aga seada sõltuvusse andmesubjekti taotlusest (see oleks nimelt pigem juurdepääsutaotluse määratlus). Võib lähtuda sellest, et teabe "taotlemise" vajadus on põhjendatud juhtudel, mil andmesubjekti ei saa teavitada, kuna tema asukoht ei ole teada.

Küsimust oleks võimalik paremini käsitleda, lisades erandi teabe saamise õigusest juhtudeks, mil teavitamine osutub võimatuks või kui see nõuaks ülemääraseid jõupingutusi. Otsuse artiklit 50 tuleks vastavalt muuta.

([1]) Vt siinkohal ka Euroopa andmekaitseinspektori arvamust viisainfosüsteemi loomise kohta (punkt 3.10.1).

Selline lahendus oleks samuti kooskõlas andmekaitset kolmanda samba raames käsitleva raamotsuse eelnõu kohaldamisega.

6.2. **Juurdepääs**

Nii kavandatavas määruses kui kavandatavas otsuses kehtestatakse juurdepääsutaotlustele vastamise tähtajad, mis on positiivne areng. Kuna aga juurdepääsuõiguse kasutamise menetlus määratletakse riiklikul tasandil, võib tekkida küsimus, milline on ettepanekutes kehtestatud tähtaegade ja olemasolevate menetluste vastastikune mõju, eriti kui liikmesriikidel on lühemad tähtajad juurdepääsutaotlusele vastamiseks. Tuleks täpsustada, et kohaldada tuleks andmesubjektile kõige soodsamaid tähtaegu.

6.2.1. *Kavandatav määrus*

Tuleb märkida, et kavandatav määrus ei sisalda Schengeni konventsiooni alusel praegu kehtivaid juurdepääsuõiguse piiranguid ("[teabe edastamisest (…)] keeldutakse, kui see on vajalik teatega seotud seaduslike ülesannete täitmiseks või kolmandate isikute õiguste ja vabaduste kaitsmiseks").

See tuleneb aga ilmselt direktiivi 95/46/EÜ kohaldatavusest, milles (artiklis 13) nähakse ette võimalus kehtestada riiklike õigusaktidega erandeid. Igal juhul tuleks juhtida tähelepanu sellele, et artikli 13 kasutamine riiklike õigusaktidega juurdepääsuõiguse piiramiseks peaks olema alati kooskõlas Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikliga 8 ning see on lubatud üksnes erandjuhtudel.

6.2.2. *Kavandatav otsus*

Kavandatavas otsuses võetakse juurdepääsuõiguse piirang Schengeni konventsioonist üle. Kavandatav raamotsus sisaldab põhijoontes samu juurdepääsuõiguse piiranguid; seega ei tooks selle dokumendi vastuvõtmine kaasa märkimisväärseid muudatusi.

Kuna mitmetes liikmesriikides on juurdepääs õiguskaitseandmetele "kaudne" (s.t, et see toimub riikliku andmekaitseasutuse kaudu), oleks kasulik sätestada andmekaitseasutuste kohustus teha juurdepääsuõiguse kasutamisel aktiivselt koostööd.

6.3. **Õigus hoiatusteate väljastamise otsuse läbivaatamisele või selle edasikaebamisele**

Määruse artikli 15 lõikega 3 kehtestatakse õigus hoiatusteate väljastamise otsuse läbivaatamisele õigusasutuse poolt või otsuse edasikaebamisele õigusasutusele, kui otsuse on teinud haldusasutus. See on praeguse Schengeni konventsiooniga võrreldes teretulnud täiendus.

Sellega toonitatakse, et andmesubjekti on vaja täielikult ja õigeaegselt teavitada, nagu märgitud eespool punktis 6.1. Ilma selle teabeta jääks kõnealune uus õigus vaid teoreetiliseks.

6.4. **Õiguskaitsevahendid**

Kavandatava määruse artiklis 30 ja kavandatava otsuse artiklis 52 sätestatakse õigus pöörduda hagi või kaebusega mis tahes liimesriigi kohtu poole, kui andmesubjektil ei võimaldatud kasutada õigust tutvuda temaga seotud andmetega või lasta need parandada või kustutada või õigust saada teavet või hüvitist.

Sõnastusest ("igaüks (…) iga liikmesriigi territooriumil") järeldub, et kaebuse esitaja peab hagi kohtule esitamiseks füüsiliselt viibima liikmesriigi territooriumil. Selline territoriaalne piirang ei ole põhjendatud ja võib muuta õiguskaitsevahendite kasutamise õiguse võimatuks, kuna kaebuse esitaja hageb väga paljudel juhtudel tõenäoliselt just seetõttu, et tal ei lubata siseneda Schengeni territooriumile. Lisaks sellele tuleb kavandatava määruse puhul arvestada, et kuna direktiiv on üldseadus (*lex generalis*) tuleb arvesse võtta selle artiklit 22, milles sätestatakse "kõigi isikute" õigus kasutada õiguskaitsevahendeid olenemata oma elukohast. Ka kavandatav raamotsus ei sisalda territoriaalset piirangut. Euroopa andmekaitseinspektor teeb ettepaneku jätta territoriaalne piirang artiklitest 30 ja 52 välja.

7. **JÄRELEVALVE**

7.1. **Sissejuhatav märkus: jagatud vastutus**

Ettepanekutes jagatakse järelevalve ülesanne riiklike järelevalveasutuste ([1]) ja Euroopa andmekaitseinspektori vahel, kusjuures igaüks tegutseb oma vastutusala piires. See on kooskõlas ettepanekute lähenemisviisiga kohaldatavale õigusele ning SIS II toimimise ja kasutamisega seotud kohustustele ning kooskõlas tõhusa järelevalve vajadusega.

Seetõttu tervitab Euroopa andmekaitseinspektor kavandatava määruse artiklis 31 ja kavandatava otsuse artiklis 53 esitatud lähenemisviisi. Vastavate ülesannete parema mõistetavuse ja selgitamise huvides teeb aga Euroopa andmekaitseinspektor ettepaneku jagada mõlemad artiklid mitmeks sätteks, millest igaüks oleks pühendatud ühele järelevalve tasandile, nagu on nõuetekohaselt tehtud VISi käsitlevas ettepanekus.

([1]) Europoli ja Eurojusti järelevalveasutused osalevad samuti, kuid väiksemas ulatuses.

7.2. **Riiklike andmekaitseasutuste teostatav järelevalve**

Vastavalt kavandatava määruse artiklile 31 ja kavandatava otsuse artiklile 53 peab iga liikmesriik tagama, et SIS IIs sisalduvate isikuandmete töötlemise seaduslikkust kontrolliks sõltumatu asutus.

Kavandatava otsuse artikliga 53 lisatakse üksikisiku õigus paluda järelevalveasutusel kontrollida teda käsitlevate andmete töötlemise seaduslikkust. Kavandatavasse määrusesse sellist sätet ei ole lisatud, kuna siinkohal kehtib üldseadusena (*lex generalis*) direktiiv. Seetõttu tuleb arvesse võtta, et riiklikud andmekaitseasutused võivad seoses SIS IIga kasutada neile direktiivi 95/46/EÜ artikliga 28 antud kõiki pädevusi, sealhulgas kontrollida andmete töötlemise seaduslikkust. Määruse artikli 31 lõikes 1 täpsustatakse nende ülesandeid, kuid see ei tohiks nimetatud volitusi piirata. Kavandatava määruse tekstis tuleks selgitada kõnealuste pädevuste jaotust.

Mis puudutab kavandatavat otsust, omistatakse selles riiklikele järelevalveasutustele ulatuslikumad ülesanded, kuna otsus põhineb erineval üldseadusel (*lex generalis*). Olukord, kus järelevalveasutustel on töödeldavate andmete kategooriatest tulenevalt erinevad ülesanded ja pädevused, ei ole aga kuigi mõistlik ning sellega on praktikas raske toime tulla. Seetõttu tuleks seda vältida, omistades kõnealustele asutustele kavandatava otsuse enda tekstis samad pädevused või osutades teisele üldseadusele (nimelt raamotsusele, mis käsitleb andmekaitset kolmanda samba raames), millega antakse andmekaitseasutustele suuremad volitused.

7.3. **Euroopa andmekaitseinspektori teostatav järelevalve**

Euroopa andmekaitseinspektor jälgib, et komisjoni andmetöötlustoiminguid viidaks läbi kooskõlas ettepanekutega. Analoogselt peaks Euroopa andmekaitseinspektoril olema võimalik kasutada talle määrusega 45/2001 antud kõiki pädevusi, võttes siiski arvesse komisjoni piiratud volitusi andmete eneste osas.

Siinkohal on kasulik lisada, et vastavalt määruse 45/2001 artikli 46 punktile f teeb Euroopa andmekaitseinspektor "siseriiklike järelevalveorganitega nende kohustuste täitmiseks vajalikku koostööd". Liikmesriikidega tehtav koostöö SIS II üle järelevalve teostamisel ei tulene mitte ainult ettepanekutest, vaid ka määrusest 45/2001.

7.4. **Ühine järelevalve**

Ettepanekutes tunnistatakse samuti vajadust kooskõlastada süsteemiga seotud erinevate asutuste järelevalvetegevust. Kavandatava määruse artiklis 31 ja kavandatava otsuse artiklis 53 sätestatakse, et "siseriiklikud järelevalveasutused ja Euroopa andmekaitseinspektor teevad aktiivset koostööd. Euroopa andmekaitseinspektor kutsub vähemalt kord aastas selleks kokku koosoleku."

Euroopa andmekaitseinspektor tervitab ettepanekut, mis sisaldab põhijoontes elemente, mis on vajalikud riiklikul ja Euroopa tasandil tegutsevate järelevalveasutuste vahelise ning tõepoolest keskset tähtsust omava koostöö käivitamiseks. Rõhutada tuleks, et ettepanekutes nähakse ette koosoleku toimumine vähemalt kord aastas, kuid seda tuleb käsitada alammäärana.

Neid sätteid (kavandatava määruse artikkel 31 ja kavandatava otsuse artikkel 53) oleks siiski kasulik muuta selgemaks tehtava koostöö sisu osas. Olemasolev ühine järelevalveasutus on vastutav konventsiooni tõlgendamisel või kohaldamisel esinevate probleemide analüüsi, seoses sõltumatu järelevalve teostamise või juurdepääsuõiguse kasutamisega tekkida võivate probleemide uurimise ja olemasolevatele probleemidele ühiseid lahendusi sisaldavate ühtlustatud ettepanekute koostamise eest.

Uued ettepanekud ei tohi viia ühise järelevalve praeguse ulatuse vähenemiseni. Kui lähtuda sellest, et andmekaitseasutused võivad seoses SIS IIga kasutada kõiki neile direktiiviga antud järelevalvepädevusi, võib nende asutuste koostöö hõlmata ulatuslikke SIS II järelevalve aspekte, sealhulgas olemasoleva ühise järelevalveasutuse ülesandeid, mida on kirjeldatud Schengeni konventsiooni artiklis 115.

Täieliku selguse huvides oleks aga kasulik seda ettepanekutes veel kord selgesõnaliselt kinnitada.

8. **TURVALISUS**

SIS II optimaalse turvalisuse taseme haldamine ja säilitamine on põhinõue andmebaasi salvestatud isikuandmete piisava kaitse tagamiseks. Sellise rahuldava turvalisuse taseme saavutamiseks tuleb rakendada asjakohased kaitsemeetmed, et tulla toime süsteemi infrastruktuuri ja sellesse kaasatud isikutega seotud võimalike riskidega. Antud teemat käsitletakse ettepanekute erinevates osades ning seda tuleks mõnevõrra täiendada.

Ettepanekute artiklid 10 ja 13 sisaldavad erinevaid meetmeid andmete turvalisuse tagamiseks ning nendes selgitatakse, millist väärkasutust tuleks vältida. Euroopa andmekaitseinspektor tervitab asjaolu, et nimetatud artiklid hõlmavad sätteid turvameetmete süstemaatilise (sise)kontrolli kohta.

Kavandatava otsuse artikkel 59 ja kavandatava määruse artikkel 34, millega nähakse ette järelevalve ja hindamine, ei peaks käsitlema ainult tulemusi, kulutasuvust ja teenuste kvaliteeti, vaid samuti vastavust õigusaktides sätestatud nõuetele, eelkõige andmekaitse valdkonnas. Euroopa andmekaitseinspektor soovitab seega nimetatud artiklite reguleerimisala laiendada andmete töötlemise seaduslikkuse jälgimisele ja selle kohta aruannete esitamisele.

Lisaks sellele tuleks kavandatava otsuse artikli 10 lõike 1 punkti f või artiklit 18 ja kavandatava määruse artiklit 17 (mis käsitlevad andmetele juurdepääsu omavat nõuetekohaselt volitatud personali) täiendada, lisades, et liikmesriigid (ning Europol ja Eurojust) peaksid tagama täpsete kasutajaprofiilide olemasolu (mis peaksid olema kontrollimiseks riiklike järelevalveasutuste käsutuses). Lisaks kasutajaprofiilidele peavad liikmesriigid koostama kasutajate täieliku nimekirja ja seda pidevalt ajakohastama. Sama kehtib *mutatis mutandis* komisjoni kohta.

Nimetatud turvameetmeid täiendatakse järelevalve ja organisatsiooniliste kaitsemeetmetega. Ettepanekute artiklites 14 kirjeldatakse kõigi andmetöötlustoimingute registreerimise tingimusi ja eesmärke. Neid kirjeid säilitatakse mitte üksnes andmekaitse jälgimise ja andmete turvalisuse tagamiseks, vaid ka artiklis 10 nõutud SIS II korrapärase sisekontrolli tugevdamiseks. Sisekontrolli tulemusel koostatud aruanded aitavad kaasa ülesannete tõhusale täitmisele järelevalveasutuste poolt, kes saavad nende alusel tuvastada nõrku kohti ning keskenduda neile oma kontrollimenetlust läbi viies.

Nagu märgitud eespool käesolevas arvamuses, tuleb süsteemi juurdepääsupunktide hulga suurendamist üksikasjalikult põhjendada, kuna see suurendab automaatselt väärkasutuse ohtu. Seetõttu tuleks mõlema ettepaneku artikli 4 lõike 1 punktis b ette näha, et teise juurdepääsupunkti vajadust peab konkreetselt põhjendama.

Ettepanekutes ei selgitata täpselt kesksüsteemi riiklike koopiate vajadust, mis annab alust tõsistele kahtlustele süsteemi üldise ohustatuse ja turvalisuse taseme suhtes; siin tuleks märkida järgmist:

— koopiate tegemine suurendab väärkasutuse ohtu (iseäranis võttes arvesse uute, nt biomeetriliste andmete olemasolu);

— ei ole täpselt määratletud, milliseid andmeid koopiad sisaldavad;

— artiklis 9 määratletud nõuded täpsusele, kvaliteedile ja andmete kättesaadavusele kujutavad endast suuri tehnilisi väljakutseid ning suurendavad seega kulusid vastavalt kättesaadavale tehnika tasemele;

— nende koopiate üle järelevalve teostamine riiklike asutuste poolt nõuab täiendavaid inimressursse ja rahalisi vahendeid, mis ei pruugi olla alati kättesaadavad.

Arvestades kaasnevaid ohte, ei ole Euroopa andmekaitseinspektor veendunud riiklike koopiate kasutamise vajalikkuses (arvestades olemasolevaid tehnoloogiaid) ega usu selle lisandväärtusesse. Ta soovitab jätta välja liikmesriikide võimaluse kasutada riiklikke koopiaid.

Euroopa andmekaitseinspektor tuletab meelde, et riiklike koopiate väljatöötamise korral tuleb selliste koopiate riikliku kasutamise suhtes kohaldada ranget eesmärgi piiramise põhimõtet. Analoogselt sellele ei tohi riiklikus koopias kunagi teostada päringuid muul viisil kui keskses andmebaasis.

Isikuandmete töötlemise seaduslikkus põhineb andmete tervikluse ja turvalisuse rangel austamisel. Euroopa andmekaitseinspektor saab neid protsesse tõhusalt jälgida, kui tal on lisaks andmete turvalisusega seotud järelevalvele võimalik olemasolevaid registreid analüüsides teostada järelevalvet ka andmete tervikluse üle. Seega tuleb artikli 14 lõikesse 6 lisada ka "andmete terviklus".

9. **KOMITEEMENETLUS**

Ettepanekutega sätestatakse komiteemenetluse kasutamine mitmel sellisel juhul, kui SIS II rakendamiseks või haldamiseks tuleb teha tehnilised otsused. Nagu märgiti samadel põhjustel VISi käsitlevas arvamuses, mõjutavad need otsused märkimisväärselt eesmärgipärasuse ja proportsionaalsuse põhimõtte nõuetekohast rakendamist.

Euroopa andmekaitseinspektor soovitab andmekaitset oluliselt mõjutavad otsused, mis käsitlevad näiteks andmetele juurdepääsu ja andmete sisestamist, lisateabe vahetamist, andmete kvaliteeti ja hoiatusteadete ühilduvust, siseriiklike koopiate tehnilist vastavust jne, teha määruse või otsuse kujul, kasutades soovitatavalt kaasotsustamismenetlust [1].

[1] Vt samuti Euroopa andmekaitseinspektori arvamust viisainfosüsteemi kohta (punkt 3.12) ja Euroopa andmekaitseinspektori arvamust direktiivi ettepaneku kohta, mis käsitleb selliste andmete säilitamist, mida on töödeldud elektrooniliste üldkasutatavate sideteenuste osutamisel, 26. september 2005, punkt 60.

Kõigil muudel andmekaitset mõjutavatel juhtudel tuleks Euroopa andmekaitseinspektorile anda võimalus nõustada asjaomaseid komiteesid valikute tegemisel.

Euroopa andmekaitseinspektori nõuandev roll tuleks ära märkida otsuse artiklites 60 ja 61 ning määruse artiklis 35.

Hoiatusteadete vahelist linkimist käsitlevate tehniliste eeskirjadega (määruse artikkel 26 ja otsuse artikkel 46) seoses tuleb selgitada vajadust kasutada erinevaid komiteemenetlusi (nõuandemenetlus otsuse puhul ja regulatiivkomitee menetlus määruse puhul).

10. **KOOSTALITLUSVÕIME**

Kuna komisjon ei ole veel esitanud teatist uute ELi süsteemide koostalitlusvõime kohta, on raske nõuetekohaselt hinnata, milline võiks olla ettenähtud, kuid veel määratlemata koostoimete lisandväärtus.

Sellega seoses sooviks andmekaitseinspektor samuti viidata terrorismivastast võitlust käsitlevale Euroopa Ülemkogu 25. märtsi 2004. aasta deklaratsioonile, milles komisjonil palutakse esitada ettepanekuid infosüsteemide (SIS, VIS ja Eurodac) koostalitlusvõime parandamiseks ja koostoime suurendamiseks. Inspektor soovib samuti viidata käimasolevale arutelule selle üle, millisele asutusele usaldada erinevate suuremõõtmeliste süsteemide juhtimine tulevikus (vt ka käesoleva arvamuse punkti 3.8).

Euroopa andmekaitseinspektor märkis juba oma arvamuses viisainfosüsteemi kohta, et koostalitlusvõime on selliste suurte IT-süsteemide nagu SIS II tõhususe esmatähtis eeltingimus. See annab võimaluse vähendada järjepidevalt üldkulusid ja vältida heterogeensete elementide loomulikku kattuvust.

— Samuti aitab koostalitlusvõime kaasa eesmärgile säilitada kõrgetasemeline turvalisus liikmesriikidevaheliste sisepiirikontrollideta alal, rakendades poliitika kõigi koostisosade suhtes sama menetlusstandardit. Siiski on oluline eristada koostalitlusvõime kahte tasandit:

  — ELi liikmesriikide koostöö on äärmiselt soovitav; ühe liikmesriigi asutuste edastatud hoiatusteated peavad olema koostalitlusvõimelised kõigi teiste liikmesriikide asutuste edastatud hoiatusteadetega.

  — Erineval eesmärgil loodud süsteemide koostalitlusvõime või koostalitlusvõime kolmandate riikide süsteemidega on palju küsitavam.

Süsteemi eesmärgi piiramiseks ja "funktsioonide ülekandumise" (*function creep*) vältimiseks kasutatavatest olemasolevatest kaitsemeetmetest võib sellist piirangut toetada erinevate tehnoloogiliste standardite kasutamine. Lisaks sellele tuleks igasugune kahe erineva süsteemi koostoime põhjalikult dokumenteerida. Koostalitlusvõime ei tohiks kunagi viia olukorrani, kus asutus, millel pole õigust pääseda juurde teatud andmetele või neid kasutada, võib saada sellise juurdepääsu mõne teise infosüsteemi kaudu. Ettepanekutest võib järeldada, et näiteks automaatset sõrmejälgede tuvastamise süsteemi (AFIS) SIS IIs esimestel aastatel ei kasutata; ettepanekutes üksnes viidatakse tulevikus loodavale biomeetriliste andmete otsingusüsteemile. Kui kavatsetakse kasutada muudest ELi süsteemidest pärit automaatset sõrmejälgede tuvastamise süsteemi, tuleks see selgelt dokumenteerida ja võtta kasutusele sellise koostoime puhul nõutavad vajalikud kaitsemeetmed.

Euroopa andmekaitseinspektor soovib veelkord rõhutada, et süsteemide koostalitlusvõimet ei saa rakendada, rikkudes eesmärgi piiramise põhimõtet, ning et kõik selleteemalised ettepanekud tuleb esitada talle.

11. **JÄRELDUSTE KOKKUVÕTE**

11.1. **Üldosa**

1. Euroopa andmekaitseinspektor tervitab ettepanekute mitmeid positiivseid aspekte, mis teatavas osas kujutavad endast parandusi võrreldes olemasoleva olukorraga. Andmekaitseinspektor tunnistab, et andmekaitset käsitlevad sätted on koostatud äärmiselt hoolikalt.

2. Euroopa andmekaitseinspektor rõhutab, et uus õiguslik kord — kuigi olemuselt keeruline — peaks:

   — tagama andmekaitse kõrge taseme,

   — olema usaldusväärne nii kodanike kui ka andmeid vahetavate asutuste jaoks,

   — olema järjepidev erinevas kontekstis (esimene või kolmas sammas) kohaldamisel.

3. Lisaks sellele tuleks SIS IIte selliste uute elementide lisamisel, mis suurendavad süsteemi võimalikku mõju üksikisikutele, järgida arvamuses kirjeldatud rangemaid kaitsemeetmeid. Eelkõige tuleks pöörata tähelepanu järgmisele.

— Juurdepääs SIS II andmetele antakse uutele asutustele ainult siis, kui selleks on äärmiselt veenev põhjendus. Juurdepääsuõigusi tuleks piirata nii palju kui võimalik, seda nii juurdepääsetavate andmete kui volitatud isikute osas.

— Hoiatusteadete omavaheline seostamine ei või isegi kaudselt põhjustada juurdepääsuõiguste muutumist.

— Vastuvõtmata õigusakte ei saa käsitada mõjuva põhjusena SIS IIte andmete lisamiseks (hoiatusteated sisenemise keelamiseks).

— Uuesti tuleks läbi vaadata õiguslik alus, millel põhineb sõidukite registreerimistunnistuste väljaandmise eest vastutavate asutuste juurdepääsuõigus, kuna selle peamine eesmärk on võidelda kuritegevusega.

— Euroopa andmekaitseinspektor tunnistab, et biomeetriliste andmete kasutamine võib parandada süsteemi toimivust ja aidata identiteedi varguse ohvreid. Siiski tundub, et selle lisasätte mõju on piisavalt läbi kaalumata ja nende andmete usaldusväärsus ülehinnatud.

11.2. **Erimärkused**

1. Euroopa andmekaitseinspektor tervitab asjaolu, et komisjon tunnistab määruse (EÜ) nr 45/2001 kohaldatavust kõikide komisjoni poolt SIS II raames teostatavate andmetöötlustoimingute suhtes, kuna selle abil tagatakse isikuandmete töötlemisel üksikisikute põhiõiguste ja vabaduste kaitset käsitlevate eeskirjade järjepidev ja ühtne kohaldamine.

2. Selleks et tagada range eesmärgi piiramine siseriiklikul tasandil, teeb Euroopa andmekaitseinspektor ettepaneku lisada SIS II käsitlevatesse ettepanekutesse (täpsemalt kavandatava määruse artiklisse 21 ja kavandatava otsuse artiklisse 40) samasuguse mõjuga säte kui Schengeni konventsiooni artikli 102 praegune lõige 4, milles piiratakse liikmesriikide võimalust sätestada andmete kasutamine eesmärgil, mida ei ole mainitud SIS II käsitlevates tekstides.

3. SIS II andmetele mis tahes asutusele juurdepääsuõiguse andmisel tuleks kohaldada rangeid tingimusi:

— Juurdepääs peab olema kooskõlas SIS II üldise eesmärgi ning süsteemi õigusliku alusega.

— SIS II andmetele juurdepääsu vajadus tuleb tõendada.

— Andmete kasutamine tuleb määratleda selgesõnaliselt ja piiritlevalt.

— Juurdepääsu tingimused peavad olema täpselt määratletud ja piiratud. Eelkõige tuleks koostada ajakohastatav nimekiri isikutest, sealhulgas Europoli ja Eurojusti töötajatest, kellel on SIS II-le juurdepääsu õigus.

— Asjaolu, et neil asutustel on juurdepääs SIS II andmetele, ei saa olla põhjendus andmete süsteemi sisestamiseks või nende säilitamiseks süsteemis, kui andmed ei ole vajalikud selle konkreetse hoiatusteate seisukohast, mille osaks nad on.

— Andmete säilitamise aega ei tohi pikendada, kui see ei ole vajalik sel eesmärgil, milleks andmed sisestati.

4. Konkreetsete Europoli ja Eurojusti puudutavate juhtudega seoses kutsub Euroopa andmekaitseinspektor komisjoni tungivalt üles piiritlema ülesanded, mille täitmiseks Europoli ja Eurojusti juurdepääs oleks õigustatud. Lisaks sellele tuleks Europoli ja Eurojusti juurdepääs piirata üksnes selliste isikute andmetega, kelle nimi juba esineb nende endi toimikutes. Samuti soovitas Euroopa andmekaitseinspektor anda Europolile ja Eurojustile ainult ühe juurdepääsupunkti.

5. Seoses hoiatusteadetega sisenemise keelamiseks tuleks seni vastuvõtmata õigusaktidel põhinevad sätted välja jätta või olemasolevate õigusaktide alusel ümber sõnastada, võimaldamaks isikutel teada, milliseid meetmeid asutused võivad tema suhtes võtta.

6. Andmete säilitamise tähtaegu on pikendatud ilma, et oleks esitatud piisavalt veenev põhjendus. Veenva põhjenduse puudumisel tuleks tähtaegu lühendada nende praeguse kestuseni, seda eelkõige varjatud jälgimiseks või erikontrolliks sisestatud hoiatusteadete puhul.

7. Komisjoni rollina nähakse süsteemi operatiivjuhtimise eest vastutamist. Koos komisjoni põhiülesandega, milleks on süsteemi arendamine ja hooldus, tuleks seda käsitada *sui generis* vastutava töötleja ülesandena. See ülesanne hõlmab enamat kui volitatud töötleja oma, kuid on samas piiratum kui tavamõistes vastutava töötleja roll, kuna komisjonil ei ole juurdepääsu SIS II raames töödeldud andmetele.

   Selle ülesande täitmiseks tuleks mõlema ettepaneku artiklisse 12 lisada, et komisjon peaks tegema korrapäraselt ettepanekuid selliste uute tehnoloogiate rakendamiseks, mis esindavad vastava valdkonna tehnika taset ning tõstavad andmekaitse ja turvalisuse taset.

8. Liikmesriikide rolli puhul tuleb selgitada, millised asutused tegutsevad vastutavate töötlejatena.

9. Andmesubjektiga seotud teave:

   — kavandatavas määruses tuleks loetelusse lisada mõningane teave: andmete säilitamise aeg, õigus taotleda hoiatusteate väljastamise otsuse läbivaatamist või kaevata see otsus edasi, võimalus saada abi andmekaitseasutuselt ning õiguskaitsevahendite olemasolu.

     Lisaks tuleb seoses teabe esitamise ajaga lisada kohustus anda hoiatusteate alast teavet otsuses, millel hoiatusteade algselt põhineb.

   — Kavandatava otsuse artiklit 50 tuleks muuta nii, et õigust teabele ei seataks sõltuvusse andmesubjekti taotlusest.

10. Tuleks tervitada ettepanekutes juurdepääsutaotlusele vastamise tähtaegade kehtestamist. Kui liikmesriigi õigusaktidega sätestatakse samuti tähtajad, tuleks selgitada, et kohaldatakse andmesubjektile kõige soodsamaid tähtaegu.

    Lisaks sellele oleks kasulik sätestada, et andmekaitseasutused peavad juurdepääsuõiguse kasutamisel tegema aktiivselt koostööd.

11. Seoses õiguskaitsevahendite kasutamise õigusega teeb Euroopa andmekaitseinspektor ettepaneku jätta artiklist 30 ja artiklist 52 välja territoriaalset kohaldamist käsitlev säte.

12. Riiklike andmekaitseasutuste volitused:

   — määruses võetakse arvesse, et riiklikud andmekaitseasutused võivad kasutada seoses SIS IIga kõiki neile direktiivi 95/46/EÜ artikliga 28 antud pädevusi; seda tuleks kavandatava määruse tekstis selgitada.

   — Kavandatavas otsuses tuleks järelevalveasutustele anda samad volitused nagu määruses/direktiivis.

13. Euroopa andmekaitseinspektori pädevused: Euroopa andmekaitseinspektoril peaks olema võimalik täita kõiki talle määrusega 45/2001 antud volitusi, võttes siiski arvesse komisjoni piiratud volitusi andmete eneste osas.

14. Kooskõlastatud järelevalve: ettepanekutes tunnistatakse vajadust kooskõlastada süsteemiga seotud erinevate asutuste järelevalvetegevust. Euroopa andmekaitseinspektor tervitab asjaolu, et ettepanekud sisaldavad põhijoontes elemente, mis on vajalikud siseriiklikul ja Euroopa tasandil tegutsevate järelevalveasutuste vaheliseks koostööks. Neid sätteid (kavandatava määruse artikkel 31 ja kavandatava otsuse artikkel 53) oleks siiski kasulik muuta selgemaks tehtava koostöö sisu osas.

15. Artiklid 10 ja 13 sisaldavad erinevaid andmekaitsemeetmeid; tervitatav on turvameetmete süstemaatilist (sise)kontrolli käsitlevate sätete lisamine.

   — Kavandatava otsuse artikkel 59 ja kavandatava määruse artikkel 34, millega nähakse ette järelevalve ja hindamine, ei peaks käsitlema ainult tulemusi, kulutasuvust ja teenuste kvaliteeti, vaid samuti vastavust õigusaktides sätestatud nõuetele, eelkõige andmekaitse valdkonnas. Neid sätteid tuleks vastavalt muuta.

   — Lisaks sellele tuleks kavandatava otsuse artikli 10 lõike 1 punkti f või artiklit 18 ja kavandatava määruse artiklit 17 täiendada, lisades, et liikmesriigid, Europol ja Eurojust peaksid tagama täpsete kasutajaprofiilide olemasolu (need peaksid olema kontrollimiseks riiklike järelevalveasutuste käsutuses). Lisaks kasutajaprofiilidele peavad liikmesriigid koostama kasutajate täieliku nimekirja ja seda pidevalt ajakohastama. Sama kehtib komisjoni kohta:

   — Isikuandmete töötlemise seaduslikkus põhineb andmete tervikluse ja turvalisuse rangel austamisel. Euroopa andmekaitseinspektoril peaks lisaks andmete turvalisusega seotud järelevalvele olema võimalik olemasolevaid registreid analüüsides teostada järelevalvet ka andmete tervikluse üle. Seega tuleb artikli 14 lõikesse 6 lisada ka "andmete terviklus".

16. Riiklike koopiate kasutamine võib tuua kaasa mitmeid lisariske. Euroopa andmekaitseinspektor ei ole veendunud riiklike koopiate kasutamise vajalikkuses (arvestades olemasolevaid tehnoloogiaid) ega usu selle lisandväärtusesse. Ta soovitab vältida või vähemalt rangelt piirata liikmesriikide võimalust kasutada riiklikke koopiaid. Riiklike koopiate väljatöötamise korral tuleb selliste koopiate riikliku kasutamise suhtes kohaldada ranget eesmärgi piiramise põhimõtet. Riiklikus koopias ei tohi teha päringuid muul viisil kui keskses andmebaasis.

17. Komiteemenetlus: — andmekaitsele olulist mõju avaldavad otsused tuleks vastu võtta määruse või otsusega, kasutades eelistatavalt kaasotsustamismenetlust. Komiteemenetluse kasutamise korral tuleks Euroopa andmekaitseinspektori nõuandev roll ära märkida otsuse artiklites 60 ja 61 ning määruse artiklis 35.

18. Süsteemide koostalitlusvõimet ei saa rakendada, rikkudes eesmärgi piiramise põhimõtet, ja kõik selleteemalised ettepanekud tuleb esitada Euroopa andmekaitseinspektorile.

Brüssel, 19. oktoober 2005

Peter HUSTINX

Euroopa andmekaitseinspektor