EUROOPA ANDMEKAITSEINSPEKTOR

Euroopa andmekaitseinspektori arvamus ettepaneku kohta koostada Euroopa Parlamendi ja nõukogu määrus, mis käsitleb viisainfosüsteemi (VIS) ja liikmesriikidevahelist teabevahetust lühiajaliste viisade kohta (KOM(2004)835 lõplik)

(2005/C 181/06)

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 25. jaanuari 2005. aasta taotlust arvamuse esitamise kohta kooskõlas määruse (EÜ) nr 45/2001 artikli 28 lõikega 2;

ON VASTU VÕTNUD KÄESOLEVA ARVAMUSE:

1. **SISSEJUHATUS**

1.1. **Sissejuhatavad märkused**

Viisainfosüsteemi (VIS) kehtestamine on ELi ühise viisapoliitika oluline osa ning seda on käsitletud mitmetes omavahel tihedalt seotud dokumentides.

— 2003. aasta aprillis teostati komisjoni tellitud VISi käsitlev teostatavusuuring ([1]).

— 2003. aasta septembris tegi komisjon ettepaneku muuta ([2]) varasemat määrust ühtse viisavormi kehtestamise kohta. Määruse põhiline eesmärk oli lisada uuele viisavormile biomeetrilised andmed (näokujutis ja sõrmejäljed). Biomeetrilised andmed salvestataks mikrokiipidel.

([1]) Viisainfosüsteem, lõpparuanne, Euroopa Komisjoni tellitud ning osaühingu Trasys teostatud, aprill 2003.
([2]) KOM(2003) 558 lõplik koos dokumentidega 2003/0217 (CNS) ja 2003/0218 (CNS)

— 2004. aasta juunis käivitas nõukogu otsus ([1]) viisainfosüsteemi väljatöötamise protsessi, moodustades õigusliku aluse VISi lisamiseks ELi eelarvesse. Nimetatud otsuses tehti ettepanek luua keskandmebaas, mis sisaldaks teavet viisataotluste kohta, ning nähti ette komiteemenetlus VISi tehnilise väljaarendamise juhtimiseks.

2004. aasta detsembris võttis komisjon vastu ettepaneku määruse kohta, mis käsitleb VISi ja liikmesriikidevahelist teabevahetust lühiajaliste viisade kohta ([2]) (edaspidi "ettepanek"), mis on käesoleva arvamuse esemeks. Ettepanekule on lisatud laiendatud mõjuanalüüs ([3]) (edaspidi "mõjuanalüüs").

Vastavalt ettepaneku seletuskirjas täheldatule on aga käesoleva määruse täiendamiseks vaja uusi õigusakte, eelkõige selleks, et:

— muuta viisasid käsitlevaid ühiseid konsulaarjuhiseid, mis on ette nähtud Schengeni konventsiooni osaliste diplomaatilistele ja konsulaaresindustele (edaspidi "ühised konsulaarjuhised") seoses menetlustes biomeetriliste andmete kasutuselevõtmisega;

— töötada välja uus mehhanism Iirimaa ja Ühendkuningriigiga andmete vahetamiseks;

— vahetada andmeid pikaajaliste viisade kohta.

Vastavalt justiits- ja siseküsimuste nõukogu 5.—6. juuni 2003. aasta istungil otsustatule ja nagu kirjeldatud eespool nimetatud 2004. aasta juuni nõukogu otsuse artikli 1 lõikes 2, ehitatakse viisainfosüsteem üles tsentraliseeritult ning see sisaldab andmebaasi, kus säilitatakse viisataotluste faile; andmebaas koosneb viisade keskinfosüsteemist (CS-VIS) ja liikmesriikides asuvast riigi liidesest (NI-VIS). Liikmesriigid määravad ([4]) siseriikliku keskasutuse, mis on ühendatud siseriikliku liidesega ning mille kaudu on liikmesriikide vastavatel pädevatel asutustel juurdepääs viisade keskinfosüsteemile.

1.2. **Ettepaneku põhielemendid andmekaitse seisukohast**

Ettepaneku eesmärk on parandada ühise viisapoliitika haldamist, hõlbustades keskandmebaasi loomisega liikmesriikide vahelist teabevahetust. Määruses nähakse ette, et viisataotluse menetluse käigus hakatakse koguma biomeetrilis andmeid (foto ja sõrmejäljed), mis säilitatakse keskandmebaasis.

Biomeetrilisi andmeid võidakse kasutada ka viisakleebisel, nagu on ette nähtud komisjoni ettepanekus määruse kohta, millega muudetakse määrust ühtse viisavormi kehtestamise kohta, et võtta kasutusele mikrokiibile salvestatud foto ja sõrmejäljed (oodates poolelioleva analüüsi tulemusi, ei ole nõukogu veel otsust vastu võtnud).

Ettepanekus kirjeldatakse üksikasjalikult andmetega teostatavaid erinevaid toiminguid (sisestamine, muutmine, kustutamine ja päringute teostamine) ning erinevaid VISi sisestatavaid andmeid sõltuvalt taotluse tulemustest (heakskiitmine, tagasilükkamine jne).

Ettepanekus on sätestatud viieaastane periood, mille jooksul säilitatakse kõigi taotlustega seotud andmeid.

Ettepanekus on piiravana loetletud, millised muud pädevad asutused peale viisa-asutuste saavad juurdepääsu VISile, ning selles määratletakse neile antavad juurdepääsuõigused:

— pädevad asutused, kes teostavad viisakontrolli välispiiridel ning liikmesriigi territooriumil;

— pädevad immigratsiooniasutused;

([1]) 2004/512/EÜ (ELT L 213, 15.6.2004, lk 5)
([2]) KOM(2004) 835 lõplik koos dokumendiga 2004/0287 (COD)
([3]) Viisainfosüsteemi laiendatud mõjuanalüüs, Euroopa poliitika hindamise konsortsiumi (EPEC) lõpparuanne, detsember 2004.
([4]) Ettepaneku artikli 24 lõige 2

— pädevad varjupaigaasutused;

VISi toimist ja sellega seotud kohustusi kirjeldades rõhutatakse ettepanekus, et komisjon töötleb liikmesriikide nimel VISis sisalduvaid andmeid. Ettepanekus rõhutatakse vajadust kasutada andmetöötlustoimingute kirjendamist, et tagada andmete turvalisus, ning määratletakse üksikasjalikumalt vastutus vajaliku turvalisuse astme tagamise eest.

Ettepanek sisaldab andmekaitset käsitlevat peatükki, milles kirjeldatakse nii siseriiklike ametiasutuste kui ka Euroopa andmekaitseinspektori ülesandeid.

Ettepanekus tehakse VISi tehniline rakendamine ja vajalike tehnoloogiate valimine ülesandeks teise põlvkonna Schengeni infosüsteemi (SIS II) väljatöötamist käsitleva määruse (EÜ) nr 2424/2001 artikli 5 lõikega 1 asutatud komiteele.

Ettepanekule on lisatud komisjoni tellitud ja Euroopa poliitika hindamise konsortsiumi (EPEC) poolt läbi viidud VISi laiendatud mõjuanalüüs. Selles järeldatakse, et VIS koos biomeetriliste andmete kasutamisega on parim võimalik lahendus ühise viisapoliitika parandamiseks.

2. **ASJAKOHANE RAAMISTIK**

Ettepanek avaldab märkimisväärset mõju üksikisikute eraelu puutumatusele ja teistele põhiõigustele; seetõttu tuleb kontrollida ettepaneku vastavust andmekaitse põhimõtetele. Peamised hindamisalused on siinkohal järgmised:

— 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 seda õigust 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.

  Aluspõhimõtted üksikisikute kaitse kohta isikuandmete töötlemisel on välja töötatud inimõiguste konventsioonis, mille Euroopa Nõukogu valmistas ette ja võttis 1981. aastal vastu.

— Pärast seda on inimeste õigus eraelule ja isikuandmete kaitsele sätestatud Euroopa Liidu põhiõiguste harta artiklites 7 ja 8 ning harta on lisatud ELi uue põhiseaduse II osasse.

  Harta artikli 52 kohaselt võib neid õigusi piirata samadel tingimusel, mis kehtivad vastavalt EIPKK artiklile 8. Nimetatud tingimuste täitmist tuleb võtta arvesse iga kord, kui hinnatakse ettepanekut võimalikuks õiguse kasutamisse sekkumiseks.

Hetkel on ELi õigusaktides andmekaitse põhieeskirjad sätestatud järgmistes dokumentides:

— 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". Direktiivis on sätestatud üksikasjalikud põhimõtted, millele vastavuse suhtes ettepanekut kontrollitakse selles ulatuses, milles seda liikmesriikidele kohaldatakse. See on eriti oluline, kuna ettepanekut kohaldatakse koos siseriiklike õigusaktidega direktiivi jõustamise kohta. Soovitatud sätete ja tagatiste tõhusus sõltub seega nimetatud kombinatsiooni tõhususest iga üksikjuhtumi puhul.

— 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". Määruses sätestatakse sarnased põhimõtted nagu direktiivis 95/46/EÜ ning see on siinkohal oluline selles ulatuses, milles ettepanekut koos määruse sätetega kohaldatakse komisjoni tegevusele. Seega tuleb tähelepanu pöörata ka sellele kombinatsioonile.

Direktiivi 95/46/EÜ ja määrust 45/2001 tuleb tõlgendada koos teiste õigusaktidega. Teisisõnu tuleb direktiivi ja määrust selles ulatuses, milles neis käsitletakse põhivabadusi, eelkõige eraelu puutumatust, piirata võivate isikuandmete töötlemist, tõlgendada põhiõiguste valguses. Sama tuleneb ka Euroopa Kohtu praktikast ([1]).

— Peale selle lisab andmekaitseinspektor oma analüüsile artikliga 29 loodud andmekaitse töörühma ([2]) 11. augusti 2004. aasta arvamuse nr 7/2004 "biomeetriliste elementide lisamise kohta elamislubadele ja viisadele, võttes arvesse Euroopa viisainfosüsteemi (VIS) kehtestamist." Oma arvamuses väljendas töörühm muret ettepaneku mitme elemendi osas. Andmekaitseinspektor kavatseb kontrollida, kas ja kuidas on tõstatud küsimusi ettepanekus arvesse võetud.

3. **ETTEPANEKU ANALÜÜS**

3.1. **Üldosa**

Euroopa andmekaitseinspektor tunnistab, et ühise viisapoliitika edasiarendamine eeldab asjakohaste andmete tõhusat vahetamist. VIS on üks mehhanismidest, mis võib tagada teabe sujuva liikumise. Samas peaks aga selline uus vahend piirduma andmete kogumise ja vahetamisega sel määral, mil andmete kogumine või vahetamine on ühise viisapoliitika väljaarendamise seisukohalt vajalik ning selle eesmärgiga proportsionaalne.

VISi kehtestamine võib omada positiivseid tagajärgi muudele õigustatud avalikele huvidele, kuid see ei muuda VISi eesmärki. Süsteemi piiratud eesmärk mängib olulist rolli süsteemi õiguspärase sisu ning kasutuse määratlemisel ning seega ka VISile (või osadele selle andmetest) juurdepääsuõiguse andmisel liikmesriikide ametiasutustele lähtuvalt õigustatud avalikest huvidest.

Lisaks sellele kehtestatakse ettepanekuga biomeetriliste andmete kasutamine VISis. Andmekaitseinspektor tunnustab biomeetriliste andmete kasutamise eeliseid, kuid rõhutab selliste andmete kasutamise märkimisväärset mõju ning teeb ettepaneku lisada biomeetriliste andmete kasutamise ranged kaitsemeetmed.

Arvamust tuleb lugeda nimetatud põhiliste kaalutluste valguses. Märgitakse, et käesolevat arvamust tuleks mainida määruse preambulas enne põhjendusi ("võttes arvesse…").

([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, milles 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.

([2]) Tegemist on sõltumatu nõuanderühmaga, kuhu kuuluvad liikmesriikide andmekaitseasutuste esindajad, andmekaitseinspektor ja komisjon ning mis asutati direktiiviga 95/46/EÜ.

3.2. **Eesmärk**

VISi eesmärk on esmatähtis nii EIPKK artikli 8 kui ka üldise andmekaitseraamistiku seisukohast. Direktiivi 95/46/EÜ artikli 6 kohaselt kogutakse isikuandmeid "täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ega töödelda hiljem viisil, mis on vastuolus kõnealuste eesmärkidega". Ainult eesmärkide selge määratlemine võimaldab anda isikuandmete töötlemise proportsionaalsusele ning piisavusele õige hinnangu, mis on andmete (sealhulgas biomeetriliste andmete) iseloomu ning kavandatud töötlustoimingute ulatuse tõttu oluline.

VISi eesmärk on selgelt määratletud ettepaneku artikli 1 lõikes 2:

> "VIS parandab ühise viisapoliitika haldamist, konsulaarkoostööd ning kesksete konsulaarasutuste vaheliste päringute teostamist, lihtsustades taotlusi ja nendekohaseid otsuseid käsitleva teabe vahetamist liikmesriikide vahel".

Seega peavad kõik VISi elemendid olema vajalikud ja proportsionaalsed vahendid selle eesmärgi saavutamiseks ühise viisapoliitika huvides.

Ettepaneku artikli 1 lõikes 2 loetletakse ka viisapoliitika tõhustamise lisaväärtused, sealhulgas:

a) sisejulgeolekut ähvardava ohu ärahoidmine,

b) pettustevastase võitluse hõlbustamine,

c) kontrolli hõlbustamine välispiiril paiknevates piiripunktides.

Euroopa andmekaitseinspektori arvates on eespool nimetatud juhtumid näited VISi kehtestamise ning ühise viisapoliitika tõhustamise positiivsetest tagajärgedest, kuid ta ei pea neid eraldiseisvateks eesmärkideks iseeneses.

Sellel on antud olukorras kaks põhilist tagajärge:

— Andmekaitseinspektor on teadlik sellest, et õiguskaitseorganid on huvitatud VISile juurdepääsu saamisest; Sellekohased nõukogu järeldused võeti vastu 7. märtsil 2005. Kuna VISi eesmärk on ühise viisapoliitika tõhustamine, tuleks märkida, et õiguskaitseorganite korrapärane juurdepääs VISile ei oleks selle eesmärgiga kooskõlas. Kui vastavalt direktiivi 95/46/EÜ artiklile 13 võidakse selline juurdepääs võimaldada ajutiselt eriolukordades ning nõuetekohaste kaitsemeetmete olemasolu korral, ei ole võimalik lubada süstemaatilist juurdepääsu.

  Üldiselt on proportsionaalsuse ja vajalikkuse hindamine esmatähtis, kui tulevikus tehakse otsuseid selle kohta, kas võimaldada teatud muudele ametiasutustele juurdepääs VISile. Ülesanded, mille täitmiseks juurdepääs võimaldatakse, peavad olema kooskõlas VISi eesmärkidega.

— Eesmärgi "hoida ära ohtu ükskõik millise liikmesriigi sisejulgeolekule" selgesõnaline mainimine punktis a on ebaõnnestunud. Põhiline VISist tulenev kasu tulevikus on pettuste ja võimalikult soodsa viisakohtlemise otsimise (*visa shopping*) tõkestamine (pettusevastane võitlus on ka peamine põhjus biomeetria kaasamiseks süsteemi) ([1]). Julgeolekut ähvardavate ohtude ärahoidmist tuleks seega vaadelda kui "teisejärgulist", olgugi et väga teretulnud lisaväärtust.

  Andmekaitseinspektor soovitab, et artikli 1 lõike 2 tekstis muudetaks erinevus "eesmärgi" ja "lisaväärtuste" vahel selgemaks, näiteks järgmiselt:

  "VISi eesmärgiks on parandada ühise viisapoliitika haldamist, konsulaarkoostööd ning kesksete konsulaarasutuste vaheliste päringute teostamist, lihtsustades taotlusi ja nendekohaseid otsuseid käsitleva teabe vahetamist liikmesriikide vahel. Seda tehes aitab VIS ühtlasi kaasa …"

([1]) Laiendatud mõjuanalüüsis on see väga selgelt sätestatud (lk 6, §2.7): *"Võimalikult soodsa viisakohtlemise otsimise ja pettuse vastase võitluse ning kontrollide teostamise puudused põhjustavad samuti puudujääke liikmesriikide sisejulgeolekus"*. Eespool nimetatu viitab sellele, et julgeolekuohud on osaliselt põhjustatud ebatõhusast viisapoliitikast. Esimeseks ülesandeks selles osas on viisapoliitika tõhustamine eelkõige pettusevastase võitluse ja tõhusamate kontrollide abil. Viisapoliitika tõhustamise tagajärjel paraneb ka julgeolek.

Sellega seoses tuleks ka märkida, et JSK nõukogu 13. juuni 2002. aasta istungil vastuvõetud suunistes ühise viisaandmete vahetamise süsteemi loomise kohta ([1]) asetati julgeolekuohtude ärahoidmine loetelu lõppu. See variant oleks samuti võimalik ja see oleks palju enam kooskõlas VISi eesmärgiga.

3.3. **Andmete kvaliteet**

Direktiivi 95/46/EÜ artikli 6 kohaselt peavad isikuandmed olema ka sellised, mis on "piisavad, asjakohased ega ületa selle otstarbe piire, mille tarvis neid kogutakse ja/või hiljem töödeldakse"; See on seotud VISi enda proportsionaalsusega, kuid samuti VISi raames kogutavate ja säilitatavate andmetega ning nende edasise kasutamisega ning samuti täiendavate kaitsemeetmetega, mida sellega seoses kohaldatakse. Need elemendid on sama olulised ettepaneku hindamiseks EIPKK artikli 8 seisukohalt.

VISi loomine tähendab kahtlemata olulist sekkumist eraelu puutumatuse õiguse kasutamisse juba üksnes töödeldavate isikuandmete ulatuse ja liikide tõttu. Seetõttu sooviski artikli 29 töörühm oma arvamuses nr 7/2004 teada, "millised nende nähtuste ulatust ja tõsidust käsitlevad uuringud tõid esile avaliku turvalisuse või avaliku korraga seotud kaalukaid põhjuseid, mis õigustaksid sellist lähenemisviisi".

Andmekaitseinspektor on tähelepanelikult võtnud arvesse mõjude hindamise aruandes esitatud tõendeid. Kuigi nimetatud tõendid ei ole päris lõplikud, näib olevat piisavalt põhjuseid, mis õigustavad VISi kehtestamist ühise viisapoliitika tõhustamise eesmärgil.

Sellega seoses näib otsuse tegemine VISi kui liikmesriikide poolt viisade väljastamise tingimuste parandamise vahendi kehtestamise kohta olevat seadusandja pädevuses. Selline süsteem võiks iseenesest hästi haakuda EÜ asutamislepingus ettenähtud vabadusel, turvalisusel ja õiglusel rajaneva ala järkjärgulise loomisega ning seda toetada;

Samas ei tohiks VISi kehtestamise ja kasutamise tulemuseks mitte mingil juhul olla see, et isikuandmete kõrgetasemelist kaitset ei saaks selles valdkonnas enam tagada. Andmekaitseinspektori nõuandva funktsiooni hulka kuulub analüüsida, mil määral VIS mõjutab andmesubjektide andmekaitse olemasolevat taset.

Sellega seoses keskendub andmekaitseinspektor käesolevas arvamuses järgmistele teemadele:

— andmete proportsionaalsus ja piisavus ning nende kasutamine (nt andmete liigid, iga asjaomase ametiasutuse juurdepääs andmetele ning andmete säilitamise aeg);

— süsteemi toimimine (nt kohustused ja turvalisus);

— andmesubjektide õigused (nt teave, võimalus ebatäpseid või ebaolulisi andmeid parandada või kustutada);

— süsteemi järelevalve ja jälgimine.

Peale järgmiste lõigete ei anna ettepanek põhjust olulisteks märkusteks seoses VISi sisestavate andmete liikide ja nende kasutamisega. Asjakohased sätted on koostatud nõuetekohase hoolikusega ning need paistavad olevat tervikuna üksteisega kooskõlas ja piisavad.

([1]) "Terrorismivastast võitlust käsitlev nõukogu 13. juuni 2002. aasta raamotsus (2002/475/JSK)", (*ELT*). 22.6.2002, nr L 164, lk 3.

3.4. **Biomeetria**

3.4.1. *Biomeetria kasutamise mõju*

Biomeetria kasutamine infosüsteemides ei ole kunagi kerge valik, eelkõige, kui kõnealune süsteem puudutab tohutut hulka üksikisikuid. Biomeetria ei ole lihtsalt üks infotehnoloogia harudest. See muudab pöördumatult keha ja identiteedi vahelist suhet, muutes inimkeha tunnused "masinloetavateks" ning edasise kasutamise objektiks. Isegi kui biomeetrilised tunnused ei ole inimsilmale loetavad, saab neid alati asjakohaste vahenditega lugeda ja kasutada kõikjal, kuhu isik läheb.

Vaatamata sellele, kui kasulikud biomeetrilised andmed võivad teatud otstarbel olla, avaldab nende laialdane kasutamine ühiskonnale märkimisväärset mõju ning selle üle tuleks alustada laiaulatuslikku ja avatud arutelu. Andmekaitseinspektor peab vajalikuks mainida, et enne kõnealuse ettepaneku väljatöötamist ei ole selline arutelu veel aset leidnud. See asjaolu rõhutab veelgi enam vajadust biomeetriliste andmete kasutamisel rakendatavate rangemate kaitsemeetmete ning hoolika kaalutlemise ja arutelu järele seadusandliku protsessi käigus.

3.4.2. *Biomeetria eripära*

Nagu on juba rõhutatud mitmes artikli 29 töörühma arvamuses ([1]), peab biomeetriliste andmete kasutamise ja töötlemisega kaasnema isikut tõendavate dokumentide puhul eriliselt järjekindlad ja tõsised kaitsemeetmed. Biomeetrilised andmed on oma teatava eripära tõttu tõepoolest äärmiselt tundlikud.

Vastab tõele, et vastupidiselt salasõnale või võtmele ei ole isikul võimalik oma biomeetrilisi andmeid kaotada. Nad võimaldavad *peaaegu täielikku eristatavust*, st igal üksikisikul on ainult temale omased biomeetrilised tunnused. Biomeetrilised andmed ei muutu inimese eluea jooksul peaaegu kunagi, mis muudab need tunnused *püsivateks*. Igaühel on olemas samad füüsilised tunnused, mis annab biomeetriale *universaalse* mõõtme.

Biomeetriliste andmete kustutamine on aga peaaegu võimatu: sõrme või nägu on raske muuta. See mitmes mõttes positiivne omadus põhjustab tõsiseid raskusi *identiteedi varguse* korral: andmebaasi salvestatud sõrmejäljed ja foto koos varastatud isikut tõendava dokumendiga võivad tekitada tõsiseid ja püsivaid probleeme vastava identiteedi tõelisele omanikule. Lisaks sellele *ei ole* biomeetrilised andmed oma iseloomult *salajased* ning võivad isegi *jälgi jätta* (sõrmejäljed, DNA), mis võimaldab neid andmeid koguda, ilma et nende omanik sellest midagi teaks.

Nende biomeetrilistele andmetele omaste riskide tõttu tuleb rakendada olulisi kaitsemeetmeid (eelkõige seoses eesmärgi piiramise põhimõtte austamise, juurdepääse piiramise ja turvameetmetega).

3.4.3. *Sõrmejälgede tehnilised puudujäägid*

Biomeetriliste andmete eespool kirjeldatud põhilised eelised (andmete universaalsus, eristatavus, kasutatavus jne) ei ole kunagi absoluutsed. See mõjutab otseselt määruses ettenähtud biomeetriliste andmete registreerimise ning isikusamasuse tuvastamise menetluste tõhusust.

Arvatakse ([2]), et hinnanguliselt kuni 5 % inimeste andmeid ei ole võimalik registreerida (kuna nende sõrmejäljed ei ole loetavad või neil ei ole üldse sõrmejälgi). Ettepanekule lisatud laiendatud mõjuanalüüsis ennustatakse umbes 20 miljonit viisataotlust 2007. aastal, mis tähendab, et kuni miljoni inimese andmeid ei ole võimalik "normaalselt" registreerida, millel on ilmselged tagajärjed viisataotlusele ja piirikontrollile.

([1]) Arvamus nr 7/2004 biomeetriliste elementide lisamise kohta elamislubadele ja viisadele, võttes arvesse Euroopa viisainfosüsteemi (VIS) kehtestamist (Markt/11487/04/EN - WP 96) ning biomeetriat käsitlev töödokument (MARKT/10595/03/EN - WP 80).

([2]) A. Sasse, *Cybertrust and CrimePrevention: Usability and Trust in Information Systems*, "Foresight cybertrust and crime prevention project". 04/1151, 10. juuni 2004, lk 7, ja *Technology Assessment*, "Using Biometrics for Border Security", *United States General Accounting Office*, GAO-03-174, november 2002.

Biomeetriline isiku tuvastamine on oma olemuselt samuti statistiline protsess. 0,5 kuni 1 %-ne veamäär on normaalne ([1]), mis tähendab, et kontrollisüsteemil välispiiridel on taotluste valedel alustel tagasilükkamise määr 0,5 kuni 1 %. Nimetatud määr sõltub pädevate asutuste riskipoliitikal põhinevast künnisest (see vastab valedel alustel tagasi saadetud ja valedel alustel riiki lubatud isikute suhtele). Seega on tegemist liialdusega, kui väita, et see tehnoloogia tagab andmesubjektide "korrektse tuvastamise", nagu on märgitud kavandatava määruse 9. põhjenduses.

Vastavalt hiljutisele Euroopa Parlamendi kodanikuvabaduste, justiits- ja siseasjade komisjoni tellitud tuleviku-uuringule ([2]) peaksid eksisteerima *varumenetlused*, mis tagaksid vajalikud kaitsemeetmed seoses biomeetria kasutuselevõtuga, sest biomeetrilised andmed ei ole kõigile kättesaadavad ega täiel määral täpsed. Nimetatud menetlusi peaks rakendama ja kasutama, et austada nende isikute väärikust, kelle andmeid ei olnud võimalik registreerida, ning vältida seda, et nad kannataksid süsteemi puuduste all ([3]).

Andmekaitseinspektor soovitab seega töötada välja varumenetlused ning lisada need ettepanekusse. Need menetlused ei tohiks vähendada viisapoliitika turvalisuse taset ega häbimärgistada üksikisikut, kelle sõrmejäljed ei ole loetavad.

3.5. **Andmete eriliigid**

Teatud andmeliikidele (lisaks biomeetrilistele andmetele) tuleb pöörata erilist tähelepanu: andmed, mis puudutavad viisa andmisest keeldumise põhjuseid (3.4.1) ja teiste grupi liikmetega seotud andmed (3.4.2).

3.5.1. *Viisa andmisest keeldumise põhjused*

Ettepaneku artikli 10 lõige 2 sisaldab viisa andmisest keeldumise põhjustega seotud andmete töötlemist käsitlevaid sätteid, kui on vastu võetud otsus viisa andmisest keelduda. Need viisa andmisest keeldumise põhjused on täielikult standardiseeritud.

— Punktides a ja b sätestatud kaks esimest põhjust on oma olemuselt üsna administratiivsed: kehtiva reisidokumendi või kavatsetava viibimise eesmärki ja tingimusi tõendavate kehtivate dokumentide mitteesitamine.

— Punktis c märgitakse, et "taotlejale on kehtestatud sissesõidukeeld", mis eeldab andmete kontrollimist SISi andmebaasis.

— Punktis d märgitakse viisa andmisest keeldumise põhjusena asjaolu, et "taotleja kujutab ohtu avalikule korrale, sisejulgeolekule, rahvatervisele või mis tahes liikmesriigi rahvusvahelistele suhetele".

([1])

Biomeetria	Nägu	Sõrm	Silma vikerkest
FTE % Failure To Enrol	Ei kohaldata	4	7
FNMR % rejection rates	4	2,5	6
FMR1 % verification match error rate	10	< 0,01	< 0,001
FMR2 % identification error rates for dB size > 1 m	40	0,1	Ei kohaldata
FMR3 % screening match error rate for dB sizes = 500	12	<1	Ei kohaldata

A. K. Jain et al., *Biometrics: A grand Challenge, Proceedings of International Conference on Pattern Recognition, Cambridge*, Ühendkuningriik, august 2004.

([2]) *Biometrics at the frontiers: assessing the impact on Society*, veebruar 2005, Tulevikutehnoloogiate instituut, Teadusuuringute Ühiskeskus, EÜ.

([3]) *Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data*, Euroopa Nõukogu, 2005, lk 11.

Kõiki keeldumise põhjuseid tuleb kohaldada äärmise ettevaatlikkusega, arvestades nende tagajärgi isikule. Mõned neist põhjustest, täpsemalt punktides c ja d esitatud põhjused, toovad kaasa direktiivi 95/46/EÜ tähenduses "tundlike andmete" töötlemise.

Andmekaitseinspektor soovib juhtida erilist tähelepanu rahvatervisega seotud põhjusele, mis näib olevat ebamäärane ja nõuab äärmiselt tundlike andmete käsitlemist. Vastavalt ettepanekule lisatud kommentaarile artiklite kohta põhineb viide rahvatervist ähvardavale ohule "ettepanekul nõukogu määruse kohta, millega kehtestatakse isikute üle piiri liikumist reguleerivad ühenduse eeskirjad" (KOM(2004) 391 lõplik).

Andmekaitseinspektor on teadlik, et "rahvatervise" kriteeriumit kasutatakse laialdaselt isikute vaba liikumist käsitlevates ühenduse õigusaktides ning et seda kohaldatakse väga rangelt, nagu on näidanud Euroopa Parlamendi ja nõukogu 29. aprilli 2004. aasta direktiiv 2004/38/EÜ, mis käsitleb liidu kodanike ja nende perekonnaliikmete õigust vabalt liikuda ja elada liikmesriikide territooriumil. Nimetatud direktiivi artiklis 29 sätestatakse tingimused rahvatervist ähvardava ohu arvessevõtmiseks: "Ainsad haigused, mis õigustavad liikumisvabadust piiravaid meetmeid, on Maailma Terviseorganisatsiooni asjaomastes dokumentides määratletud epideemiaohuga haigused ja muud nakkushaigused või nakkuslikud parasitaarhaigused, kui nende kohta kehtivad vastuvõtva liikmesriigi kodanike suhtes kohaldatavad kaitsesätted."

— Sellele vaatamata tuleb märkida, et eespool nimetatud ettepanek on hetkel ainult ettepanek ning et rahvatervisele ohu mittekujutamise tingimuse lisamine VISi määrusesse sõltub ühenduse eeskirjade vastuvõtmisest.

— Isegi kui eeskirjad vastu võetakse, tuleks seda riiki lubamise keelu põhjust tõlgendada piiratult. Ettepanek ühenduse eeskirjade kohta põhineb aga omakorda äsja mainitud direktiivil 2004/38/EÜ.

Andmekaitseinspektor soovitab seega lisada viide direktiivi 2004/38/EÜ artiklile 29 ettepaneku teksti, et tagada "rahvatervist ähvardava ohu" mõistmine nimetatud sättes valguses. Igal juhul tuleks andmeid, võttes arvesse nende tundlikkust, käsitleda ainult juhul, kui oht tervisele on tõeline, vahetu ja piisavalt tõsine.

3.5.2. *Andmed grupi teiste liikmete kohta*

Artikli 2 lõikes 7 määratletakse "grupi liikmed" kui "teised taotlejad, kellega koos taotleja reisib, sealhulgas abikaasa ja taotlejaga kaasas olevad lapsed". Kommentaaris artiklite kohta märgitakse, et ettepaneku artiklis 2 sisalduvad määratlused viitavad asutamislepingule või viisapoliitikat käsitlevale Schengeni *acquis*'le, välja arvatud mõned mõisted, sealhulgas "grupi liikmed", mis on määratletud konkreetselt käesoleva määruse eesmärke silmas pidades. Seega võib oletada, et eespool nimetatud määratlus ei viita ühiste konsulaarjuhiste artiklis 2.1.4 sisalduvale "grupiviisa" määratlusele. Kommentaaris artiklite kohta osutatakse taotlejatele, "kes reisivad grupina koos teiste taotlejatega, nt heakskiidetud sihtriigi staatust käsitleva kokkuleppe raames, või koos teiste pereliikmetega".

Andmekaitseinspektor rõhutab, et määruses tuleks sätestada "grupi liikmete" täpne ja kõikehõlmav määratlus. Andmekaitseinspektori arvates on nimetatud määratlus praeguses ettepanekus liiga ebamäärane, kuna puudub viide asutamislepingule või Schengeni *acquis*'le. Praeguse sõnastuse kohaselt võivad "grupi liikmete" hulka kuuluda kolleegid, organiseeritud ringreisil osalevad reisibüroo teised kliendid, jne. Selle tagajärjed võivad tõepoolest väga tõsised olla:

määruse ettepaneku artikli 5 kohaselt seotakse taotleja taotlus teiste grupiliikmete taotlustega.

3.6. **Andmete säilitamine**

Ettepaneku eelnõu artiklis 20 sätestatakse, et iga taotluse faili säilitatakse viis aastat. See on poliitika, mis on valitud selleks, et ühenduse õigusaktides oleks võimalik ette näha mõistlikud tähtajad.

Eelkõige lähtuvalt artikleid käsitlevates kommentaarides nimetatud põhjustest ei ole tõendeid, mis viitaksid sellele, et käesolevas ettepanekus tehtud poliitiline otsus oleks põhjendamatu või et sellel oleksid vastuvõetamatud tagajärjed, tingimusel et kõik võimalikud korrektsioonimehhanismid on kasutusele võetud. See tähendab, et tuleb tagada andmete parandamine või kustutamine, kui andmed ei ole enam täpsed ning eelkõige, kui isik on saanud liikmesriigi kodakondsuse või kui ta on omandanud staatuse, mis ei eelda tema andmete süsteemis hoidmist.

Lisaks sellele, kui andmed on endiselt süsteemis alles, ei tohi nad mingil juhul avaldada mõju uuele otsusele. Mõned keeldumise põhjused (eelkõige taotlejale kehtestatud sissesõidukeeld, oht rahvatervisele) on piiratud kehtivusajaga. Asjaolu, et need on mingil ajavahemikul olnud riiki sisenemise keelu mõjuvateks põhjusteks, ei tohiks avaldada mõju uuele otsusele. Olukorda tuleb iga uue viisataotluse puhul täielikult uuesti hinnata ning see tuleks sobivates kohtades määruses selgesõnaliselt sätestada.

3.7. **Juurdepääs andmetele ja nende kasutamine**

3.7.1. *Eelmärkused*

Eelmärkusena tunnustab andmekaitseinspektor pühendumust, millega VISis sisalduvatele andmetele juurdepääsu ja nende andmete kasutamist reguleeriv süsteemi on üles ehitatud. Igal ametiasutusel on juurepääs erinevatele andmetele erinevatel eesmärkidel. See on sobiv lähenemine, mida andmekaitseinspektor igati toetab. Järgmiste tähelepanekute eesmärk on sellise lähenemisviisi täieulatuslik kohaldamine.

3.7.2. *Viisade kontroll välispiiridel ja riigi territooriumil*

Viisade kontrollimisel välispiiridel sätestatakse kavandatud määruse artiklis 16 selgelt kaks konkreetset eesmärki:

— "tuvastada isiku samasus", mis esitatud määratluse kohaselt tähendab "üks-ühele" võrdlust;

— "viisa autentsuse kontrollimine". ICAO standardites soovitatu kohaselt võiks viisa mikrokiip autentimisprotsessi läbiviimiseks kasutada avalikku/isiklikku võtmesüsteemi (PKI).

Need kaks eesmärki on võimalik nõuetekohaselt saavutada, kui pädevatele asutustele antakse viisade kontrollimiseks juurdepääs üksnes kaitstud mikrokiibile. Juurdepääs VISi keskandmebaasile oleks antud konkreetsel juhul ebaproportsionaalne. Viimasena nimetatud võimalus eeldaks, et VISiga on ühendatud rohkem ametiasutusi, mis suurendaks väärkasutuse ohtu. See oleks tõenäoliselt ka kallim variant, sest turvaliste ja kontrollitud juurdepääsude arv VISile ning selle juurdepääsuga seotud konkreetse koolituse vajadus suureneks samuti märkimisväärselt.

Lisaks sellele on ka kahtlusi seoses artikli 16 teises punktis ettenähtud andmetele juurdepääsu piisavusega. Lõike 2 punktis a on tõepoolest sätestatud, et kui pärast esimest päringut selgub, et taotleja kohta käivad andmed on VISis registreeritud (mis peaks põhimõtteliselt nii olema), võib pädev asutus isikusamasuse tuvastamise eesmärgil teostada päringuid muude andmete kohta. Need andmed puudutavad kogu teavet, mis on seotud taotluse, fotode, sõrmejälgede ning varem välja antud, kehtetuks tunnistatud, tühistatud või pikendatud viisadega.

Kui isikusamasuse tuvastamine on õnnestunud, siis pole selge, mis põhjusel peaks vaja olema veel ülejäänud andmeid. Ülejäänud andmetele peaks lubatama juurdepääsu ainult juhul, kui isikusamasuse tuvastamine on ebaõnnestunud. Sellisel juhul saaks artikli 16 lõikes 2 nimetatud andmeid kasutada varumenetluses, mis aitaks tuvastada isiku samasust. Need andmed ei tohiks olla kättesaadavad igale piiripunkti töötajale, vaid teatavate piirangutega keerulisemate juhtumite eest vastutavatele ametnikele.

Lisaks sellele peaks juurdepääsu omavate ametiasutuste määratlus olema täpsem. Eriti selgusetuks jääb, millised on "liikmesriikide territooriumitel kontrolle teostavad pädevad asutused". Andmekaitseinspektor oletab, et tegemist on *viisa*kontrolli teostavate pädevate asutustega ning artiklit 16 tuleks sellest lähtuvalt muuta.

3.7.3. *Andmete kasutamine ebaseaduslike sisserändajate tuvastamiseks ja tagasisaatmiseks ning varjupaigamenetlusteks*

Artiklites 17, 18 ja 19 (ebaseaduslike sisserändajate tagasisaatmine ja varjupaigamenetlus) kirjeldatud juhtudel kasutatakse VISi isikusamasuse tuvastamise eesmärgil. Fotod moodustavad osa andmetest, mida saab kasutada isikusamasuse tuvastamiseks. Praeguse automaatset näo tuvastamist puudutava tehnilise olukorra juures ei saa sellistes suurtes IT süsteemides fotosid isikusamasuse tuvastamiseks kasutada (üks mitmele); need ei suuda tagada usaldusväärset tulemust. Fotosid ei saa seega pidada isikusamasuse tuvastamise eesmärgil kasutatavateks piisavateks andmeteks.

Andmekaitseinspektor soovitab tungivalt, et "fotod" jäetaks nende artiklite esimesest osast välja ning jäetaks alles teises osas (fotosid saab kasutada isikusamasuse tuvastamise vahendina, kuid mitte kasutades suuremahulist andmebaasi).

Teine variant oleks muuta artiklit 36 selliselt, et fotode töötlemise funktsioone isikusamasuse tuvastamise eesmärgil rakendataks alles siis, kui vastavat tehnoloogiat saab pidada usaldusväärseks (võimalik, et pärast tehnilise komitee nõuannet).

3.7.4. *Juurdepääsu omavate ametiasutuste avalikustamine*

Määruse eelnõu artiklis 4 nähakse ette, et igas liikmesriigis määratud VISile juurdepääsu omavate pädevate asutuste nimetused avaldatakse *Euroopa Liidu Teatajas*. Nimetused tuleks avaldada korrapäraselt (kord aastas), et teavitada siseriiklike olude muutumisest. Andmekaitseinspektor rõhutab asutuste nimetuste avaldamise olulisust, kuivõrd see on asendamatu kontrollivahend nii Euroopa tasandil kui riiklikul või kohalikul tasandil.

3.8. **Kohustused**

Siinkohal meenutatakse, et VISi aluseks on tsentraliseeritud süsteem, kuhu kuuluvad keskne andmebaas, kus säilitatakse kogu viisasid puudutavat teavet, ning liikmesriikides asuvad siseriiklikud liidesed, mis võimaldavad pädevatel asutustel kesksüsteemile juurde pääseda. Vastavalt määruse eelnõu põhjendustele 14 ja 15 kohaldatakse direktiivi 95/46/EÜ isikuandmete töötlemisel liikmesriikide poolt seoses määruse rakendamisega ning määrust 45/2001 kohaldatakse komisjoni tegevusele seoses isikuandmete kaitsega. Nagu sellega seoses on nimetatud põhjendustes märgitud, on ettepaneku eesmärk teatud punkte selgitada, muu hulgas seoses kohustustega andmete kasutamisel ning andmekaitse üle teostatava järelevalvega.

Nimetatud punktid näivad nimelt olevat seotud mõningate oluliste üksikasjadega, milleta ei saaks direktiivis 95/46/EÜ ja määruses 45/2001 ettenähtud kaitsemeetmete süsteemi kohaldada või see ei oleks täielikult ettepanekuga kooskõlas. Kui siseriiklike õigusaktide kohaldatavus vastavalt direktiivile eeldab selles liikmesriigis määratud vastutava töötleja olemasolu (artikkel 4), siis määruse kohaldatavus sõltub isikuandmete töötlemisest ühenduse institutsiooni või asutuse poolt toimingute teostamisel, mis tervikuna või osaliselt kuuluvad ühenduse õigusaktide rakendusalasse (artikkel 3).

Vastavalt määruse eelnõu artikli 23 lõikele 2 töödeldakse VISis "andmeid liikmesriikide nimel". Vastavalt artikli 23 lõikele 3 määravad liikmesriigid asutuse, mis on vastutavaks töötlejaks direktiivi 95/46/EÜ artikli 2 punkti d tähenduses. See näib osutavat, et direktiivi süsteemi kohaselt peaks komisjoni pidama volitatud töötlejaks. See leiab kinnitust selgituses artiklite kohta ([1]).

Tekstis ei tähtsustata piisavalt komisjoni äärmiselt tähtsat ja tegelikult keskset rolli nii süsteemi väljatöötamise kui selle tavapärase toimimise faasis. Komisjoni rolli on raske siduda vastutava töötleja või volitatud töötleja mõistega; ta on kas erandlike volitustega volitatud töötleja (muu hulgas süsteemi väljatöötamisel) või piiratud volitustega vastutav töötleja (kuna andmeid sisestavad ja kasutavad liikmesriigid). Komisjonil on VISis tegelikult *sui generis* roll ([2]).

Komisjoni tähtsat rolli peaks tunnustatama tema ülesannete põhjaliku kirjelduse ning mitte sõnastuse kaudu, mis ei vasta päriselt tegelikkusele, kuna see on liiga piirav, ei muuda midagi VISi toimimises ja tekitab ainult segadust. See on oluline ka VISi järjekindla ja tõhusa järelevalve seisukohalt (vt ka lõige 3.11). Andmekaitseinspektor teeb seega ettepaneku artikli 23 lõige 2 välja jätta.

Andmekaitseinspektor soovib rõhutada, et komisjoni VISiga seotud ülesannete täielik kirjeldus on veelgi tähtsam, kui komisjon kavatseb süsteemi juhtimise teisele organile üle anda. Ettepanekule lisatud finantsaruandes mainitakse võimalust anda need ülesanded üle Euroopa Piirivalveagentuurile. Sellega seoses on esmatähtis, et komisjon teavitaks oma järglast täpselt oma pädevuste ulatusest, et viimane teaks, millistes piirides tegutseda.

3.9. **Turvalisus**

VISi optimaalse turvalisuse taseme hoidmine ja austamine on eelduseks andmebaasi salvestatud isikuandmete vajaliku kaitse tagamisele. Sellise rahuldava turvalisuse taseme saavutamiseks tuleb rakendada asjakohased kaitsemeetmed, et tulla toime süsteemi infrastruktuuri ja sellesse kaasatud isikutega seotud võimalike riskidega. Antud teemat käsitletakse ettepaneku erinevates osades ning seda tuleks mõnevõrra täiendada.

Ettepaneku artiklid 25 ja 26 sisaldavad erinevaid andmekaitsemeetmeid ning nendes selgitatakse, millist väärkasutust tuleks vältida. Neid sätteid oleks aga kasulik täiendada meetmetega, mis näevad ette juba mainitud turvameetmete tõhususe järelevalve ja selle kohta aruannete esitamise. Andmekaitseinspektor soovitab konkreetsemalt, et nimetatud artiklitele lisataks sätted turvameetmete süstemaatilise (sise)kontrolli kohta.

See on seotud ettepaneku artikliga 40, milles nähakse ette järelevalve ja hindamine. Eespool nimetatu ei puuduta mitte ainult tulemusi, kulutasuvust ja teenuste kvaliteeti, vaid ka vastavust õigusaktides sätestatud nõuetele, eelkõige andmekaitse valdkonnas. Andmekaitseinspektor soovitab seega, et artikli 40 reguleerimisala tuleks laiendada andmete töötlemise seaduslikkuse jälgimisele ja selle kohta aruannete esitamisele.

Lisaks sellele tuleks nõuetekohaselt volitatud personali käsitlevat artikli 24 lõike 4 punkti c või artikli 26 lõike 2 punkti e täiendada, lisades, et liikmesriigid 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: Artikli 25 lõike 2 punkti b tuleks seetõttu vastavalt täiendada.

([1]) Vt ettepaneku lk 37.

([2]) Kuigi vastutava töötleja määratluses direktiivis 95/46/EÜ ja määruses 45/2001 nähakse ette ka võimalus määrata rohkem vastutavaid töötlejaid, kellel on erinevad ülesanded.

Nimetatud turvameetmeid tuleb täiendada järelevalve ja organisatsiooniliste tagatistega. Ettepaneku artiklis 28 kirjeldatakse kõigi andmetöötlustoimingute salvestamise tingimusi ja eesmärke. Nimetatud salvestisi ei säilitata mitte ainult andmekaitse järelevalveks ja andmete turvalisuse tagamiseks, vaid ka VISi süstemaatilise sisekontrolli läbiviimiseks. Enesekontrolli tulemusel koostatud aruanded aitavad kaasa tõhusale ülesannete täitmisele järelevalveasutuste poolt, kes suudavad seejärel tuvastada nõrku kohti ning keskenduda neile oma auditit läbi viies.

3.10. **Andmesubjekti õigused**

3.10.1. *Andmesubjekti teavitamine*

Andmesubjekti teavitamine andmete õiglase töötlemise tagamise eesmärgil on ülimalt tähtis. See on üksikisiku õiguste kaitse seisukohast hädavajalik. Selleks järgib ettepaneku artikkel 30 nüüd põhiliselt direktiivi 95/46/EÜ artiklit 10.

See säte vajaks aga mõningaid muudatusi, et sobitada seda paremini VISi raamistikku. Direktiiv kohustab küll edastama teatud teavet, kuid võimaldab vajaduse korral edastada ka rohkem teavet ([1]). Seega tuleks artiklit 30 muuta selliselt, et see sisaldaks järgmisi punkte:

— Andmesubjekti tuleks teavitada ka tema andmete suhtes kehtivast säilitamise tähtajast.

— Artikli 30 lõike 1 punktis e käsitletakse "õigust tutvuda enda kohta käivate andmetega ning neid parandada". Täpsem oleks rääkida "õigusest tutvuda enda kohta käivate andmetega ning õigusest *nõuda* nende parandamist *või kustutamist*". Sellega seoses tuleks andmesubjekti teavitada võimalusest taotleda nõu või abi asjaomastelt järelevalveasutustelt.

— Lõpuks mainitakse artikli 30 lõike 1 punktis a teavet vastutava töötleja ja tema võimaliku esindaja andmete kohta. Kuna vastutav töötleja paikneb alati Euroopa Liidu territooriumil, siis ei ole viimatimainitud võimaluse järele vajadust.

3.10.2. *Õigus andmetega tutvuda, neid parandada ja kustutada*

Artikli 31 lõike 1 viimases lauses märgitakse, et "loa andmetega tutvumiseks võib anda üksnes liikmesriik". Võib eeldada, et see tähendab, et luba andmetega tutvuda (või neid edastada) ei saa anda keskne üksus vaid iga liikmesriik. Euroopa andmekaitseinspektor soovitab selgesõnaliselt väljendada, et sellist andmete edastamist võib taotleda igas liikmesriigis.

Lisaks näib selle sätte sõnastus mõista andvat, et andmetega tutvumist ei saa keelata ning seda võimaldatakse ilma vastutava liikmesriigi loata. See selgitaks, miks liikmesriikide asutused peavad tegema koostööd artikli 31 lõigetes 2, 3 ja 4 sätestatud õiguste jõustamiskeks, kuid mitte artikli 31 lõike 1 puhul ([2]).

3.10.3. *Järelevalveasutuste pakutav abi*

Artikli 33 lõikes 2 sätestatakse, et riiklike järelevalveasutuste kohustus abistada ja nõustada asjaomast isikut kehtib kogu menetluse jooksul (kohtus). Selle lõike tähendus ei ole selge. Riiklikel järelevalveasutustel on erinev suhtumine oma rolli kohtumenetluse ajal. Praegusest sõnastusest jääb mulje, nagu peaksid nad etendama kohtus kaebuse esitaja nõustaja rolli, mis on paljudes riikides võimatu.

([1]) Selles mainitakse *"täiendava teabe avaldamist (…) kuivõrd selline täiendav teave on vajalik, et tagada andmesubjekti suhtes õiglane andmete töötlemine, võttes arvesse andmete kogumise konkreetseid asjaolusid"*.

([2]) Seega võiks artikli 31 lõiget 3, mis käsitleb riiklike asutuste koostööd andmete parandamise või kustutamise õiguse kasutamisel, muuta suurema selguse saavutamiseks järgmiselt: "kui *artikli 31 lõikes 2 nimetatud* nõue". Artikli 31 lõikes 1 nimetatud (tutvumis)nõuetega ei kaasne asutustevahelist koostööd.

3.11. **Järelevalve**

Ettepanekus jagatakse järelevalve ülesanne riiklike järelevalveasutuste ja andmekaitseinspektori vahel. See on kooskõlas ettepaneku lähenemisviisiga kohaldatavale õigusele ja VISi toimimisele ja kasutamisele, ning tõhusa järelevalve vajadusega. Seetõttu tervitab andmekaitseinspektor sellist lähenemisviisi artiklites 34 ja 35.

Riiklikud järelevalveasutused jälgivad isikuandmete töötlemise, *sealhulgas andmete VISi ja VISist edastamise* seaduslikkust liikmesriikides. Euroopa andmekaitseinspektor jälgib komisjoni tegevust *(…), et isikuandmete edastamine siseriiklike liideste ja viisade keskinfosüsteemi vahel toimub seaduslikult*. See võib kaasa tuua kattumise, sest siseriiklike liideste ja viisade keskinfosüsteemi vahel toimuva andmeedastuse seaduslikkuse jälgimise eest vastutavad samal ajal nii riiklikud järelevalveasutused kui ka Euroopa andmekaitseinspektor.

Seetõttu teeb andmekaitseinspektor ettepaneku muuta artiklit 34, et täpsustada, et riiklikud järelevalveasutused jälgivad isikuandmete töötlemise seaduslikkust liikmesriigis, sealhulgas andmete VISi ja VISist edastamist.

VISi järelevalvega seoses on samuti oluline rõhutada, et riiklike järelevalveasutuste ja Euroopa andmekaitseinspektori järelevalvealane tegevus peaks olema teatud ulatuses kooskõlastatud, et tagada piisav järjepidevus ja üldine tõhusus. Määruse rakendamist on vaja ühtlustada ning töötada välja ühine lähenemisviis ühistele probleemidele. Turvalisusega seoses võib veel lisada, et VISi turvalisuse taseme määrab lõpuks selle nõrgima lüli turvalisuse tase. Sellega seoses on samuti vaja struktureerida ja parandada koostööd andmekaitseinspektori ja riiklike järelevalveasutuste vahel. Seega peaks artikkel 35 sisaldama sätet, et Euroopa andmekaitseinspektor korraldab vähemalt kord aastas kohtumise kõigi riiklike järelevalveasutustega.

3.12. **Rakendamine**

Ettepaneku artikli 36 lõikes 2 sätestatakse: *"Lõikes 1 osutatud funktsioonide tehniliseks rakendamiseks vajalikud meetmed võetakse vastu artikli 39 lõikes 2 osutatud korras."* Artiklis 39 viidatakse komisjoni abistavale komiteele, mis loodi 2001. aasta detsembris ([1]) ja mida on kasutatud mitmete õigusaktide puhul.

VISi funktsioonide (suhtlemine pädevate asutustega ja ühtne viisavorm) tehniline rakendamine toob kaasa mitmeid andmekaitsele potentsiaalselt ohtlikke mõjusid. Näiteks see, kas viisad varustatakse mikrokiibiga või mitte, avaldab mõju keskse andmebaasi kasutamise viisile, samuti sõltub andmekaitsepoliitika väljatöötamine biomeetriliste andmete vahetamiseks valitavast standardvormist ([2]).

Tehnoloogia valikul on määrav mõju sihipärasuse ja proportsionaalsuse põhimõtete korrektsele rakendamisele ja järelikult tuleks selle üle järelevalvet teostada. Seetõttu peaksid andmekaitsele olulist mõju avaldavad tehnoloogilised valikud toimuma määruse alusel ja kooskõlas kaasotsustamismenetlusega. Ainult selliselt on võimalik tagada vajalik poliitiline kontroll. Kõigil muudel andmekaitset mõjutavatel juhtudel tuleks Euroopa andmekaitseinspektorile anda võimalus nõustada kõnesolevat komiteed valikute tegemisel.

3.13. **Koostoimivus**

Koostoimivus on VISi taoliste suurte IT süsteemide tõhususe kriitiliselt esmatähtis eeltingimus. See annab võimaluse vähendada järjepidevalt üldkulusid ja vältida heterogeensete elementide loomulikku kattuvust. Koostoimivus tuleb samuti kasuks ühise viisapoliitika eesmärgile, rakendades poliitika kõigi koostisosade suhtes sama menetlusstandardit. Siiski on oluline eristada koostoimivuse kahte tasandit:

— Koostoimivus ELi liikmesriikide vahel on äärmiselt soovitav; ühe liikmesriigi asutuste esitatud viisataotlused peavad ju toimima koos kõigi teiste liikmesriikide esitatud viisataotlustega.

([1]) Nõukogu 6. detsembri 2001. aasta määrus nr 2424/2001 teise põlvkonna Schengeni infosüsteemi (SIS II) väljatöötamise kohta.

([2]) 2003. aasta septembris esitatud ettepanek nõukogu määruse (EÜ) 1683/95 (ühtne viisavorm) muutmiseks sisaldas samasugust artiklit.

— Erinevaks otstarbeks loodud süsteemide koostoime või koostoime kolmandate riikide süsteemidega on palju küsitavam.

Süsteemi otstarbe piiramiseks ja "funktsioonide ülekandumise" vältimiseks kasutatavatest olemasolevatest kaitsemeetmetest võib sellist piirangut toetada erinevate tehnoloogiliste standardite kasutamine. Lisaks sellele tuleks igasugune kahe erineva süsteemi koostoimimine põhjalikult dokumenteerida. Koostoime ei tohiks kunagi viia olukorrani, kus asutus, millel pole õigust pääseda juurde teatud andmetele või neid kasutada, võib saada sellise juurdepääsu mõne teise teabesüsteemi kaudu.

Sellega seoses tahaks andmekaitseinspektor viidata terrorismivastast võitlust käsitlevale Ülemkogu 25. märtsi 2004. aasta deklaratsioonile, milles komisjonil palutakse esitada ettepanekuid teabesüsteemide (SIS, VIS ja Eurodac) koostoime parandamiseks ja sünergia suurendamiseks.

Inspektor soovib samuti viidata käimasolevale arutelule selle üle, millisele asutusele usaldada erinevate suurte süsteemide juhtimine tulevikus (vt ka käesoleva arvamuse punkti 3.8).

Euroopa andmekaitseinspektor tahab veelkord rõhutada, et süsteemide koostoimet ei saa rakendada, rikkudes otstarbe piiramise põhimõtet, ning et kõik selleteemalised ettepanekud tuleb esitada talle.

4. **JÄRELDUSED**

4.1. **Üldosa**

1. Euroopa andmekaitseinspektor tunnistab, et ühise viisapoliitika edasiarendamine eeldab asjakohaste andmete tõhusat vahetamist. VIS on üks mehhanism, mis võib tagada teabe sujuva liikumise. Andmekaitseinspektor on tähelepanelikult võtnud arvesse mõjuanalüüsis esitatud tõendid. Kuigi nimetatud tõendid ei ole küll täiesti vaieldamatud, näib olevat piisavalt põhjuseid, mis õigustavad VISi loomist eesmärgiga tõhustada ühist viisapoliitikat.

   See uus õigusakt peaks siiski piirduma vaid andmete kogumise ja vahetamisega, niivõrd kui selline andmete kogumine ja vahetamine on vajalik ühise viisapoliitika väljatöötamiseks ja on selle eesmärgi suhtes proportsionaalne.

2. VISi loomine võib omada positiivseid tagajärgi muudele õigustatud avalikele huvidele, kuid see ei muuda VISi eesmärki. Seega peavad kõik VISi elemendid olema vajalikud ja proportsionaalsed vahendid, et saavutada eespool nimetatud poliitilist eesmärki. Lisaks sellele:

   — Korrapärane õiguskaitseorganite juurdepääs ei oleks selle eesmärgiga kooskõlas.

   — Andmekaitseinspektor soovitab, et artikli 1 lõike 2 tekstis muudetaks erinevus "eesmärgi" ja "lisaväärtuste" vahel selgemaks.

   — Koostoimet teiste süsteemidega ei saa rakendada rikkudes otstarbe piiramise põhimõtet.

3. Andmekaitseinspektor tunnistab biomeetria kasutamise eeliseid, kuid rõhutab taoliste andmete kasutamise suurt mõju ning soovitab kehtestada biomeetriliste andmete kasutamisele ranged kaitsemeetmed. Lisaks nõuavad sõrmejälgede tehnilised puudujäägid, et töötataks välja varumenetlused ning et need lisataks ettepanekusse.

4. Käesolevat arvamust tuleks mainida määruse preambulas enne põhjendusi ("võttes arvesse…").

4.2. **Muud asjaolud**

5. Seoses viisataotluse rahuldamatajätmise põhjustega: ettepaneku teksti tuleks lisada viide direktiivi 2004/58/EÜ artiklile 29, et tagada "rahvatervisele kujutava ohu" mõistmine nimetatud sätte valguses.

6. Ettepanekus on eriline tähendus grupi liikmeid puudutavatel andmetel: seetõttu tuleks esitada "grupi liikmete" täpne ja kõikehõlmav määratlus.

7. Puuduvad tõendid selle kohta, et käesolevas ettepanekus tehtud poliitikaotsus andmete säilitamise pikendamiseks oleks põhjendamata või et sellel oleksid vastuvõetamatud tagajärjed, tingimusel et kõik võimalikud korrektsioonimehhanismid on kasutusele võetud.

   Lisaks sellele tuleks ettepanekus selgesõnaliselt sätestada, et isikuandmeid tuleb iga uue viisataotluse puhul täielikult uuesti hinnata.

8. Seoses viisakontrolliga välispiiridel: Ettepaneku artiklit 16 tuleks muuta, sest juurdepääs VISi keskandmebaasile oleks nendel juhtudel ebaproportsionaalne. Viisade kontrollimiseks piisab pädevatele asutustele juurdepääsust andmisest üksnes kaitstud mikrokiibile.

   Pealegi kui isiku tuvastamine on õnnestunud, siis pole selge, mis põhjusel peaks vaja olema veel ülejäänud andmeid.

9. Seoses andmete kasutamisega ebaseaduslike sisserändajate tuvastamiseks ja tagasisaatmiseks ning varjupaigamenetlusteks: artiklite 17, 18 ja 19 esimesest osast tuleks välja jätta "fotod" ning alles jätta teise osasse.

10. Seoses komisjoni ja liikmesriikide kohustustega: artikli 23 lõige 2 jäetakse välja.

11. Ettepanekusse tuleks lisada sätted turvameetmete süstemaatilise (enese)kontrolli kohta. Artikli 40 reguleerimisala tuleks laiendada andmete töötlemise seaduslikkuse jälgimisele ja aruandlusele. Lisaks sellele:

   — peavad liikmesriigid koostama kasutajate täieliku nimekirja ja seda pidevalt ajakohastama. Sama kehtib komisjoni kohta: artikli 25 lõike 2 punkti b tuleks seetõttu vastavalt täiendada.

   — Ettepaneku artiklis 28 kirjeldatakse kõigi andmetöötlustoimingute kirjendamise tingimusi ja eesmärke. Neid kirjeid säilitatakse mitte üksnes andmekaitse jälgimise ja andmete turvalisuse tagamiseks, vaid ka korrapärase sisekontrolli läbiviimiseks VISis.

12. Seoses andmesubjekti õigustega:

   — Artiklit 30 tuleks muuta, et tagada andmesubjektide teavitamine neid puudutavate andmete säilitamise ajast.

   — Artikli 30 lõike 1 punktis e tuleks mainida "õigust tutvuda enda kohta käivate andmetega ning õigust nõuda nende parandamist või kustutamist".

   — Artikli 31 lõikes 1 tuleks selgesõnaliselt sätestada, et teatud andmete edastamist võib nõuda igas liikmesriigis.

13. Seoses järelevalvega:

— Artiklit 34 tuleks muuta, et täpsustada, et riiklikud järelevalveasutused jälgivad isikuandmete töötlemise seaduslikkust liikmesriigis, sealhulgas andmete VISi ja VISist edastamist.

— Seega peaks artikkel 35 sisaldama sätet, et Euroopa andmekaitseinspektor korraldab vähemalt kord aastas kohtumise kõigi riiklike järelevalveasutustega.

14. Seoses rakendamisega:

— andmekaitsele olulist mõju avaldavad tehnoloogilised valikud peaksid toimuma määruse alusel ja kooskõlas kaasotsustamismenetlusega.

— muudel juhtudel tuleks Euroopa andmekaitseinspektorile anda võimalus nõustada ettepanekus nimetatud komiteed valikute tegemisel.

Brüssel, 23. märts 2005

Euroopa andmekaitseinspektor

Peter HUSTINX