EUROOPAN TIETOSUOJAVALTUUTETTU

Euroopan tietosuojavaltuutetun lausunto ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi viisumitietojärjestelmästä (VIS) ja lyhytaikaista oleskelua varten myönnettäviä viisumeja koskevasta jäsenvaltioiden välisestä tietojenvaihdosta (KOM(2004) 835 lopull.)

(2005/C 181/06)

EUROOPAN TIETOSUOJAVALTUUTETTU, joka

ottaa huomioon Euroopan yhteisön perustamissopimuksen ja erityisesti sen 286 artiklan,

ottaa huomioon Euroopan unionin perusoikeuskirjan ja erityisesti sen 8 artiklan,

ottaa huomioon yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 24 päivänä lokakuuta 1995 annetun Euroopan parlamentin ja neuvoston direktiivin 95/46/EY,

ottaa huomioon yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 18 päivänä joulukuuta 2000 annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 45/2001 ja erityisesti sen 41 artiklan,

ottaa huomioon 25 päivänä tammikuuta 2005 komissiolta saamansa asetuksen (EY) N:o 45/2001 28 artiklan 2 kohdan mukaisen lausuntopyynnön,

ON ANTANUT SEURAAVAN LAUSUNNON:

1. **JOHDANTO**

1.1 **Taustaa**

Viisumitietojärjestelmän (VIS) perustaminen on tärkeä osa EU:n yhteistä viisumipolitiikkaa, ja siitä on annettu useita toisiinsa liittyviä säädöksiä.

— Huhtikuussa 2003 tehtiin komission tilaama VIS:ää koskeva toteutettavuustutkimus ([1]).

— Syyskuussa 2003 komissio antoi ehdotuksen yhtenäisestä viisumin kaavasta aiemmin annetun asetuksen muuttamisesta ([2]). Pääasiallisena tarkoituksena oli ottaa käyttöön biometriset tiedot (kasvokuva ja kaksi sormenjälkeä) uudessa viisumin kaavassa. Nämä biometriset tiedot tallennettaisiin mikrosirulle.

([1]) Viisumitietojärjestelmää (VIS) koskeva loppuraportti, EY:n tilaama ja Trasysin tekemä tutkimus, huhtikuu 2003.
([2]) KOM(2003) 558 lopull. (2003/0217 (CNS) ja 2003/0218 (CNS)).

— Kesäkuussa 2004 neuvosto teki päätöksen ([1]), jolla käynnistettiin viisumitietojärjestelmän (VIS) kehittäminen. Päätös muodostaa oikeusperustan, jonka nojalla VIS voidaan sisällyttää EU:n talousarvioon. Tässä päätöksessä ehdotettiin keskustietokantaa, johon viisumihakemukseen liittyvät tiedot tallennettaisiin, ja säädettiin komiteamenettelystä VIS:n teknisen kehittämisen hallinnoimiseksi.

Joulukuussa 2004 komissio antoi ehdotuksen asetukseksi viisumitietojärjestelmästä (VIS) ja lyhytaikaista oleskelua varten myönnettäviä viisumeja koskevasta jäsenvaltioiden välisestä tietojenvaihdosta ([2]) (jäljempänä 'ehdotus'), jota tämä lausunto käsittelee. Asiaa koskeva laaja vaikutusarviointi ([3]) (jäljempänä 'vaikutusarviointi') on ehdotuksen liitteenä.

Tätä asetusta on kuitenkin täydennettävä muilla säädöksillä, kuten ehdotuksen perusteluissa todetaan. Näissä on käsiteltävä erityisesti seuraavia kysymyksiä:

— Schengenin yleissopimuksen osapuolten diplomaatti- ja konsuliedustustojen yhteisen konsuliohjeiston (jäljempänä 'yhteinen konsuliohjeisto') muuttaminen biometristen tietojen huomioon ottamiseksi eri menettelyissä

— uuden järjestelyn kehittäminen Irlannin ja Yhdistyneen kuningaskunnan kanssa käytävää tietojenvaihtoa varten

— tietojenvaihto pitkäaikaisista viisumeista.

Kuten oikeus- ja sisäasioiden neuvosto päätti 5.—6.6.2003 ja kuten edellä mainitun kesäkuussa 2004 tehdyn neuvoston päätöksen 1 artiklassa todetaan, viisumitietojärjestelmä perustuu keskitettyyn arkkitehtuuriin ja käsittää tietokannan, johon viisumihakemusten tiedot tallennetaan: siinä on keskusviisumitietojärjestelmä (CS-VIS) ja kussakin jäsenvaltiossa käytössä olevat kansalliset käyttöliittymät (NI-VIS). Jäsenvaltiot nimeävät ([4]) kansallisen viranomaisen, joka on liitetty kansalliseen käyttöliittymään ja jonka kautta jäsenvaltion toimivaltaiset viranomaiset pääsevät käyttämään CS-VIS:ää.

1.2 **Ehdotuksen keskeiset osatekijät tietosuojan kannalta**

Ehdotuksen tarkoituksena on parantaa yhteisen viisumipolitiikan hallintoa helpottamalla jäsenvaltioiden välistä tietojenvaihtoa keskustietojärjestelmän avulla. Asetuksessa esitetään, että biometriset tiedot (valokuva ja sormenjäljet) otetaan käyttöön hakemusmenettelyssä ja että ne tallennetaan keskustietojärjestelmään.

Biometrisiä tietoja voitaisiin käyttää myös viisumitarrassa, kuten yhtenäisestä viisumin kaavasta annetun asetuksen muuttamista koskevassa komission asetusehdotuksessa esitetään. Kasvokuva ja sormenjäljet tallennettaisiin mikrosirulle (neuvosto ei vielä ole tehnyt päätöstä asiasta; asiaa tarkastellaan parhaillaan).

Ehdotuksessa kuvataan yksityiskohtaisesti erilaisia tietojenkäsittelyoperaatioita (tallentaminen, muuttaminen, poistaminen ja haku) ja mitä eri tietoja VIS:ään tallennetaan viisumihakemuksen eri käsittelyvaiheissa (hyväksyminen, epääminen jne.).

Ehdotuksessa säädetään kunkin hakemuksen tietojen säilyttämisajaksi viisi vuotta.

Ehdotuksessa luetellaan ne muut viranomaiset kuin viisumiviranomaiset, jotka voivat käyttää VIS:ää, ja määritellään heille myönnettävät käyttöoikeudet:

— ulkorajoilla ja jäsenvaltion alueella suoritettavista tarkastuksista vastaavat toimivaltaiset viranomaiset

— toimivaltaiset maahanmuuttoviranomaiset

([1]) 2004/512/EY, EUVL L 213, 15.6.2004, s. 5.
([2]) KOM(2004) 835 lopull. (2004/0287 (COD))
([3]) Viisumitietojärjestelmän laaja vaikutusarviointi, EPECin loppuraportti, joulukuu 2004.
([4]) Ehdotuksen 24 artiklan 2 kohta.

— toimivaltaiset turvapaikkaviranomaiset.

Ehdotuksen VIS:n toimintaa ja siihen liittyviä vastuualueita koskevassa kuvauksessa korostetaan, että komissio käsittelee VIS:n tiedot jäsenvaltioiden puolesta. Siinä todetaan, että tietojenkäsittelytapahtumat on kirjattava tietoturvallisuuden takaamiseksi, ja määritellään vastuualueet tämän turvallisuustason varmistamiseksi.

Ehdotuksessa on tietosuojaa koskeva luku, jossa määritellään kansallisten viranomaisten ja Euroopan tietosuojavaltuutetun (jäljempänä 'tietosuojavaltuutettu') tehtävät.

Ehdotuksen mukaan VIS:n teknisestä toteutuksesta ja tarvittavien teknisten ratkaisujen valinnasta vastaa toisen sukupolven Schengenin tietojärjestelmän (SIS II) kehittämisestä annetun asetuksen (EY) N:o 2424/2001 5 artiklan 1 kohdan mukainen komitea.

Ehdotukseen on liitetty komission tilaama ja EPECin toteuttama laaja vaikutusarviointi. Siinä todetaan, että VIS yhdessä biometristen tietojen käytön kanssa on paras käytettävissä oleva ratkaisu yhteisen viisumipolitiikan parantamiseksi.

2. **OIKEUDELLISET PUITTEET**

Ehdotuksella on huomattava vaikutus henkilön yksityisyyteen ja muihin perusoikeuksiin; tästä syystä sitä tarkastellaan tietosuojaperiaatteiden pohjalta. Tarkastelussa olemme keskittyneet seuraaviin seikkoihin:

— Oikeus nauttia yksityiselämän kunnioitusta on varmistettu Euroopassa vuodesta 1950 lähtien, jolloin Euroopan neuvosto hyväksyi ihmisoikeuksien ja perusvapauksien suojaamista koskevan yleissopimuksen (jäljempänä 'ECHR'). Kyseisen yleissopimuksen 8 artiklassa määrätään oikeudesta nauttia yksityis- ja perhe-elämän kunnioitusta.

  Kyseisen yleissopimuksen 8 artiklan 2 kohdan mukaan "viranomaiset eivät saa puuttua tämän oikeuden käyttämiseen, paitsi silloin kun laki sen sallii ja se on demokraattisessa yhteiskunnassa välttämätöntä" tärkeiden etujen suojelemiseksi. Euroopan ihmisoikeustuomioistuimen oikeuskäytännössä nämä ehdot ovat johtaneet lisävaatimuksiin oikeuksiin puuttumisen oikeusperustan, toimenpiteiden suhteellisuuden ja väärinkäytöksiltä suojaamisen osalta.

  Perusperiaatteet yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä on annettu Euroopan neuvoston laatimassa yleissopimuksessa, joka hyväksyttiin vuonna 1981 (Yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä).

— Oikeus nauttia yksityiselämän kunnioitusta ja oikeus henkilötietojen suojeluun on sittemmin sisällytetty Euroopan unionin perusoikeuskirjaan (7 ja 8 artikla), joka muodostaa EU:n perustuslakisopimuksen II osan.

  Perusoikeuskirjan 52 artiklan mukaan näitä oikeuksia voidaan rajoittaa, mutta tällöin on täytettävä ECHR:n 8 artiklan mukaiset edellytykset. Nämä edellytykset on otettava aina huomioon arvioitaessa ehdotusta, jossa kyseisiin oikeuksiin puututaan.

EU:n tämänhetkisessä lainsäädännössä tietosuojaa koskevat säännöt annetaan seuraavissa säädöksissä:

— Euroopan parlamentin ja neuvoston direktiivi 95/46/EY, annettu 24.10.1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (EYVL L 281, s. 31), jäljempänä 'direktiivi 95/46/EY'. Direktiivissä säädetään yksityiskohtaisesti periaatteista, jotka on otettava huomioon tarkasteltaessa ehdotusta siltä osin kuin sitä on tarkoitus soveltaa jäsenvaltioihin. Tämä on erittäin tärkeää myös siksi, että ehdotusta sovelletaan yhdessä kansallisen lainsäädännön kanssa, jolla direktiivi on saatettu voimaan. Ehdotettujen säännösten ja suojatoimien tehokkuus riippuu näin ollen kyseisen yhdistelmän toimivuudesta kussakin yksittäistapauksessa.

— Euroopan parlamentin ja neuvoston asetus (EY) N:o 45/2001, annettu 18.12.2000, yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (EYVL L 8, s. 1), jäljempänä 'asetus 45/2001'. Asetuksessa säädetään samanlaisista periaatteista kuin direktiivissä 95/45/EY, ja se on tässä yhteydessä merkityksellinen siltä osin kuin ehdotusta on tarkoitus soveltaa komission toimintaan yhdessä asetuksen säännösten kanssa. Tämä yhdistelmä ansaitsee näin ollen myös jonkin verran huomiota.

Direktiiviä 95/45/EY ja asetusta 45/2001 on tarkasteltava yhdessä muiden välineiden kanssa. Toisin sanoen direktiiviä ja asetusta on tulkittava perusoikeuksien pohjalta siltä osin kuin nämä säädökset koskevat henkilötietojen käsittelyä, joka saattaa olla vastoin perusoikeuksia, erityisesti oikeutta yksityisyyteen. Tämä on myös Euroopan yhteisöjen tuomioistuimen oikeuskäytännön mukaista. ([1])

— Tietosuojavaltuutettu sisällyttää lausuntoonsa myös 29 artiklan mukaisen tietosuojatyöryhmän ([2]) lausunnon nro 7/2004 (11.8.2004) biometristen tietojen sisällyttämisestä oleskelulupiin ja viisumeihin VIS:n perustaminen huomioon ottaen. Lausunnossaan työryhmä ilmaisi huolensa useista ehdotuksen kohdista. Tietosuojavaltuutettu aikoo tarkistaa, onko nämä kysymykset otettu huomioon ehdotuksessa ja miten se on tehty.

3. EHDOTUKSEN ANALYYSI

3.1 Yleistä

Tietosuojavaltuutettu toteaa, että yhteisen viisumipolitiikan kehittäminen edellyttää tehokasta merkityksellisten tietojen vaihtoa. VIS on yksi mahdollinen järjestelmä sujuvan tiedonkulun varmistamiseksi. Tällainen uusi väline tulisi kuitenkin rajoittaa tietojen keruuseen ja vaihtoon, jos tällainen keruu tai vaihto on tarpeen yhteisen viisumipolitiikan kehittämiseksi ja on oikeassa suhteessa tähän tarkoitukseen.

VIS:n perustamisella voi olla myönteisiä vaikutuksia muun oikeutetun yleisen edun kannalta, mutta tämä ei muuta VIS:n tarkoitusta. Sillä, että järjestelmän tarkoitus on rajattu, on erittäin suuri merkitys määriteltäessä järjestelmän lainmukaista sisältöä ja käyttöä ja myös annettaessa jäsenvaltioiden viranomaisille oikeus käyttää VIS:iä (koko järjestelmää tai sen osia) oikeutetun yleisen edun mukaisiin tarkoituksiin.

Lisäksi ehdotuksessa esitetään biometristen tietojen käyttöön ottamista VIS:ssä. Tietosuojavaltuutettu myöntää, että biometriikan käytöllä on etunsa, mutta haluaa korostaa tällaisten tietojen käytön huomattavia vaikutuksia ja ehdottaa, että biometristen tietojen käyttöä varten määriteltäisiin tiukat suojatoimet.

Nämä pääasia olisi otettava huomioon tätä lausuntoa luettaessa. Huomattakoon, että tämä lausunto olisi mainittava asetuksen johdanto-osassa ennen varsinaisia johdanto-osan kappaleita ("ottavat huomioon … lausunnon").

([1]) Tässä yhteydessä on syytä viitata tuomioistuimen tuomioon asiassa Österreichischer Rundfunk ym. (yhdistetyt asiat C-465/00, C-138/01 ja C-139/01), tuomio 20.5.2003, tuomioistuimen täysistunto, (2003) Kok. I-4989. Tuomioistuin käsitteli Itävallan lakia, jonka mukaan julkisen sektorin palveluksessa olevien henkilöiden tulot on ilmoitettava Itävallan Rechnungshofille ja lisäksi julkistettava. Tuomiossaan tuomioistuin esittää joukon perusteita, jotka perustuvat ECHR:n 8 artiklaan ja joita tulisi käyttää sovellettaessa direktiiviä 95/46/EY siltä osin kuin tämä direktiivi antaa mahdollisuuden tiettyihin rajoituksiin, jotka koskevat oikeutta yksityisyyteen.

([2]) Tämä on itsenäinen neuvoa-antava työryhmä, joka koostuu jäsenvaltioiden tietosuojaviranomaisen, Euroopan tietosuojavaltuutetun ja komission edustajista. Työryhmä perustettiin direktiivillä 95/46/EY.

3.2 **Tarkoitus**

VIS:n tarkoitus on keskeisen tärkeä sekä ECHR:n 8 artiklan että yleisen tietosuojasäännöstön perusteella. Direktiivin 95/45/EY 6 artiklan mukaan ”henkilötiedot kerätään tiettyä nimenomaista ja laillista tarkoitusta varten, eikä niitä myöhemmin saa käsitellä näiden tarkoitusten kanssa yhteensopimattomalla tavalla”. Käyttötarkoituksen selkeä määrittely on ainoa tapa arvioida oikein henkilötietojen käsittelyn oikeasuhteisuutta ja asianmukaisuutta, mikä on ratkaisevaa ottaen huomioon tietojen laadun (biometriset tiedot mukaan luettuina) ja niiden suunnitellun käsittelyn laajuuden.

VIS:n tarkoitus on selkeästi määritelty ehdotuksen 1 artiklan 2 kohdassa:

> ”Viisumitietojärjestelmä parantaa yhteisen viisumipolitiikan hallinnointia, konsuliyhteistyötä ja keskuskonsuliviranomaisten keskinäistä kuulemista helpottamalla jäsenvaltioiden välistä tietojenvaihtoa viisumihakemuksista ja niihin liittyvistä päätöksistä.”

Tämän vuoksi kaikkien VIS:n osatekijöiden on oltava tämän tarkoituksen saavuttamisen kannalta tarpeellisia ja oikeasuhteisia yhteisen viisumipolitiikan edistämiseksi.

Ehdotuksen 1 artiklan 2 kohdassa luetellaan myös yhteisen viisumipolitiikan edistämisestä koituvia lisäetuja, joilla voidaan

a) ehkäistä jäsenvaltioiden sisäiseen turvallisuuteen kohdistuvia uhkia,

b) helpottaa petostentorjuntaa,

c) helpottaa ulkorajojen tarkastuspisteissä ja jäsenvaltioiden alueella tehtäviä tarkastuksia.

Tietosuojavaltuutettu pitää näitä tekijöitä esimerkkeinä VIS-järjestelmän perustamisesta koituvista myönteisistä vaikutuksista ja yhteisen viisumipolitiikan parantamisesta mutta ei itsenäisinä tarkoituksina sinänsä.

Tästä aiheutuu tässä vaiheessa kaksi olennaista seurausta:

— Tietosuojavaltuutettu on tietoinen siitä, että lainvalvontaviranomaiset ovat kiinnostuneita VIS:n käyttöoikeudesta; neuvoston tämänsuuntaiset päätelmät asiasta annettiin 7.3.2005. Koska VIS:n tarkoituksena on parantaa yhteistä viisumipolitiikkaa, on huomattava, että lainvalvontaviranomaisten automaattinen pääsy VIS:ään ei vastaa tätä tarkoitusta. Vaikka pääsy voitaisiinkin direktiivin 95/46/EY 13 artiklan mukaisesti antaa satunnaisesti, tietyissä olosuhteissa ja tarvittavin oikeudellisin takein, järjestelmällistä pääsyä ei voida sallia.

  Yleisemmin voidaan todeta, että oikeasuhteisuuden ja tarpeellisuuden arviointi on olennaista, kun vastaisuudessa päätetään, sallitaanko tiettyjen viranomaisten pääsy VIS:ään. Tehtävien, joita varten pääsy myönnetään, on vastattava VIS:n tarkoitusta.

— Ehdotuksessa mainittu tarkoitus ”ehkäistä jäsenvaltioiden sisäiseen turvallisuuteen kohdistuvia uhkia” on epäonnistunut. VIS:n pääasialliset hyödyt ovat petosten torjunta ja edullisimman viisumikohtelun valinnan estäminen (petosten torjunta on myös tärkein syy siihen, miksi biometrisiä tietoja halutaan sisällyttää järjestelmään). ([1]) Turvallisuusuhkien ehkäiseminen olisi näin ollen nähtävä toissijaisena vaikkakin erittäin tervetulleena hyötynä.

  Tietosuojavaltuutettu suosittaa, että ero ”tarkoituksen” ja ”hyötyjen” välillä tehdään selvemmäksi 1 artiklan 2 kohdassa esimerkiksi seuraavasti:

  ”Viisumitietojärjestelmän tarkoituksena on parantaa yhteisen viisumipolitiikan hallinnointia, konsuliyhteistyötä ja keskuskonsuliviranomaisten keskinäistä kuulemista helpottamalla jäsenvaltioiden välistä tietojenvaihtoa viisumihakemuksista ja niihin liittyvistä päätöksistä. Näin se osaltaan edistää …”

([1]) Tämä todetaan selvästi vaikutusarvioinnissa (s.6. kohta 2.7.): *tehottomuus visa shopping -ilmiön estämisessä, petosten torjunnassa ja tarkastuksissa voi aiheuttaa puutteita myös jäsenvaltioiden turvallisuudessa.* Tämän mukaan turvallisuusuhkat johtuisivat osittain tehottomasta viisumipolitiikasta. Tällöin ensimmäinen tehtävä on tehostaa viisumipolitiikkaa, varsinkin petosten torjunnalla ja tehokkaammilla tarkastuksilla. Turvallisuus paranee viisumipolitiikan parantamisen myötä.

Tässä yhteydessä on myös syytä mainita, että asiakirjassa ”Suuntaviivat yhteisen viisumeja koskevan tietojenvaihtojärjestelmän perustamiseksi”, jonka neuvosto (oikeus- ja sisäasiat) hyväksyi 13.6.2002 [1], sisäistä turvallisuutta koskevien uhkien torjunta on luettelon viimeisenä kohtana. Tämä olisi myös tässä mahdollista ja lisäksi paljon johdonmukaisempaa VIS:n tarkoituksen kannalta.

3.3 **Tietojen laatu**

Direktiivin 95/46/EY 6 artiklan mukaan henkilötietojen on oltava ”asianmukaisia, olennaisia eikä liian laajoja siihen tarkoitukseen, mihin ne on kerätty ja missä niitä myöhemmin käsitellään”. Tämä liittyy itse VIS:n oikeasuhteisuuteen mutta myös niiden tietojen oikeasuhteisuuteen, jotka on tarkoitus kerätä ja tallentaa VIS:ään, ja niiden myöhempään käyttöön sekä lisäsuojatoimiin, joita sovelletaan siinä yhteydessä. Nämä seikat ovat tärkeitä myös tarkasteltaessa ehdotusta ECHR:n 8 artiklan perusteella.

VIS:n perustaminen on eittämättä ristiriidassa yksityisyyden suojaa koskevan oikeuden kanssa jo pelkästään järjestelmän laajuuden ja siinä käsiteltävien henkilötietoluokkien vuoksi. Siksi 29 artiklan mukainen työryhmä kysyi lausunnossaan nro 7/2004, mitkä selvitykset näiden ilmiöiden laajuudesta ja vakavuudesta ovat antaneet aihetta vedota yleiseen turvallisuuteen tai yleiseen järjestykseen ja oikeuttaisivat tällaisen lähestymistavan.

Tietosuojavaltuutettu on pannut tarkoin merkille vaikutusarvioinnissa esitetyt perustelut. Vaikkakaan perustelut eivät ole täysin vakuuttavia, ne näyttävät riittäviltä oikeuttamaan VIS:n perustamisen yhteisen viisumipolitiikan parantamiseksi.

Edellä esitetty huomioon ottaen päätös siitä, perustetaanko VIS välineeksi, jonka avulla parannetaan jäsenvaltioiden viisuminmyöntämismenettelyjä, näyttäisi kuuluvan lainsäätäjän harkintavaltaan. Tällainen järjestelmä voisi sinänsä sopia hyvin EY-perustamissopimuksessa määrättyyn vapauden, turvallisuuden ja oikeuden alueeseen ja tukea sen asteittaista luomista.

VIS:n perustamisesta ja käytöstä ei kuitenkaan koskaan saisi olla seurauksena, että henkilötietojen korkeatasoista suojaa ei enää voida taata tällä alalla. Tietosuojavaltuutetun neuvoa-antavana tehtävänä on selvittää, missä määrin VIS vaikuttaa asianomaisten rekisteröityjen henkilöiden tietosuojan nykytasoon.

Tätä taustaa vasten tietosuojavaltuutettu keskittyy lausunnossaan seuraaviin kysymyksiin:

— tietojen oikeasuhteisuus ja asianmukaisuus ja niiden käyttö (esim. tietoluokat, kunkin viranomaisen pääsy tietoihin ja tietojen säilyttämisaika)

— järjestelmän toiminta (esim. vastuualueet ja turvallisuus)

— rekisteröityjen henkilöiden oikeudet (esim. tiedonsaanti, mahdollisuus oikaista tai poistaa epätarkkoja tai turhia tietoja)

— järjestelmän seuranta ja valvonta.

Seuraavia kappaleita lukuun ottamatta ehdotus ei anna aihetta merkittäviin huomautuksiin tietoluokista, joita on tarkoitus sisällyttää VIS:ään tai niiden käytöstä. Asiaa koskevat säännökset on laadittu huolella ja ne näyttävät olevan kokonaisuutena johdonmukaisia ja asianmukaisia.

[1] Neuvoston puitepäätös terrorismin torjumisesta, tehty 13.6.2002 (2002/475/YOS), EYVL L 164, 22.6.2002, s. 3.

3.4 **Biometriset tiedot**

3.4.1 *Biometristen tietojen käytön vaikutukset*

Biometristen tietojen käyttö tietojärjestelmissä ei koskaan ole merkityksetön valinta eikä varsinkaan silloin, kun järjestelmä koskee valtavaa määrää henkilöitä. Biometriset tiedot eivät ole vain yksi tietotekniikan ala, vaan ne muuttavat peruuttamattomasti ruumiin ja henkilöllisyyden suhdetta, sillä biometristen tietojen avulla ihmisruumiin piirteistä tulee "koneellisesti luettavia" mahdollista myöhempää käyttöä varten. Vaikka biometrisiä tietoja ei voi lukea ihmissilmällä, niitä voidaan lukea ja käyttää soveltuvilla välineillä milloin tahansa ja minne tahansa henkilö meneekin.

Biometriset tiedot voivat olla erittäin hyödyllisiä tiettyihin tarkoituksiin, mutta niiden laajamittainen käyttö vaikuttaa merkittävästi yhteiskuntaan ja siitä tulisi keskustella avoimesti ja mahdollisimman laajalti. Tietosuojavaltuutetun on todettava, että tätä keskustelua ei ole varsinaisesti käyty ennen ehdotuksen laatimista. Tämän vuoksi on sitäkin tärkeämpää, että biometristen tietojen käytölle asetetaan tiukat suojatoimet ja että lainsäädäntömenettelyn aikana asioita pohditaan ja niistä keskustellaan perusteellisesti.

3.4.2 *Biometristen tietojen erityislaatu*

Kuten 29 artiklan mukainen työryhmä on useaan otteeseen painottanut ([1]), biometristen tietojen käyttöönotto ja käsittely henkilöasiakirjoissa on suojattava erityisen johdonmukaisesti ja huolellisesti. Biometriset tiedot ovat hyvin arkaluonteisia tiettyjen erityispiirteidensä vuoksi.

On sanomattakin selvää, että biometrisiä tietoja on lähes mahdotonta kadottaa, toisin kuin salasanaa tai avainta. Biometriset tiedot ovat *lähes täydellisen erottelevia*, ts. jokaisella henkilöllä on ainutlaatuiset biometriset piirteet. Nämä piirteet eivät myöskään juuri koskaan muutu henkilön eliniän aikana, joten tiedot ovat *pysyviä*. Jokaisella on samat fyysiset "tekijät", minkä ansiosta biometriset tiedot ovat *universaaleja*.

Biometrisiä tietoja on lähes mahdotonta kumota: sormia tai kasvoja on vaikea muuttaa. Tämä monessa suhteessa myönteinen ominaisuus on kuitenkin suuri epäkohta, kun on kyse *henkilöllisyyden väärinkäytöstä*: sormenjälkien ja valokuvan tallentaminen tietokantaan silloin, kun asiaan liittyy henkilöllisyyden väärinkäyttö, voi aiheuttaa suuria ja pysyviä ongelmia sille henkilölle, josta oikeasti on kyse. Biometriset tiedot *eivät* myöskään laatunsa vuoksi *ole salaisia* vaan niistä voi jopa *jäädä jälkiä* (sormenjäljet, DNA), jolloin niitä voidaan kerätä *ilman, että kyseinen henkilö on asiasta tietoinen*.

Koska nämä riskit ovat biometrisille tiedoille ominaisia, on otettava käyttöön huomattavia suojatoimia (erityisesti käyttötarkoituksen rajoittamisen periaate, pääsyn rajoittaminen ja turvatoimet).

3.4.3 *Sormenjälkien tekniset puutteet*

Biometristen tietojen tärkeimmät edut kuvailtiin edellä (tietojen universaalisuus, erottelevuus, pysyvyys, käytettävyys jne.) mutta ne eivät koskaan ole absoluuttisia. Tämä vaikuttaa suoraan asetuksessa ehdotettujen biometristen tietojen rekisteröinnin ja tarkistusmenettelyjen tehokkuuteen.

Arvioiden mukaan ([2]) noin 5 prosenttia ihmisistä on sellaisia, joiden tietoja ei voida rekisteröidä (koska heidän sormenjälkensä eivät ole luettavissa tai heillä ei ole sormenjälkiä). Ehdotukseen liitetyssä vaikutusarvioinnissa todetaan, että jos vuonna 2007 arviolta 20 miljoonaa henkilöä hakee viisumia, näistä noin 1 miljoonan tietoja ei voida rekisteröidä tavanomaisin menettelyin, millä on tietenkin seurauksia viisumien hakemusmenettelyille ja rajatarkastuksille.

([1]) Lausunto nro 7/2004 biometristen tekijöiden sisällyttämisestä oleskelulupiin ja viisumeihin VIS:n perustaminen huomioon ottaen (Markt/11487/EN – WP 96) ja biometrisiä tietoja koskeva valmisteluasiakirja (MARKT/10595/EN – WP 80).

([2]) A. Sasse, *Cybertrust and CrimePrevention:Usability and Trust in Information System*, julkaisussa "Foresight cybertrust and crime prevention project". 04/1151, 10.6.2004, s. 7, ja Technology Assessment, "Using Biometrics for Border Security", United States General Accounting Office, GAO-03-174, marraskuu 2002.

Biometrinen tunnistus on myös tilastollinen menettely. Normaali virhemarginaali ([1]) on 0,5—1 %, mikä tarkoittaa, että ulkorajoilla tapahtuvissa tarkastuksissa väärin perustein tapahtuvan hylkäämisen aste (False Rejection rate, FFR) on 0,5—1 %. Tämä luku on riippuvainen siitä, millainen on toimivaltaisten viranomaisten riskipolitiikassaan soveltama kynnys (vastaa väärin perustein hylättyjen ja väärin perustein hyväksyttyjen välistä suhdetta). Onkin liioiteltua todeta, että näiden tekniikoiden avulla on mahdollista tunnistaa asianomainen henkilö ”täsmällisesti”, kuten asetusehdotuksen johdanto-osassa todetaan.

Euroopan parlamentin kansalaisvapauksien sekä oikeus- ja sisäasioiden valiokunnan (LIBE) tilaaman äskettäisen selvityksen ([2]) mukaan olisi oltava käytettävissä *varajärjestelmämenettelyjä*, jotka ovat olennaisia suojatoimia biometristen tietojen käyttöönotossa, sillä ne eivät ole kaikkien käytettävissä eivätkä täysin tarkkoja. Tällaisia menettelyjä olisi otettava käyttöön ja käytettävä sellaisten henkilöiden huomioon ottamiseksi, joiden tietoja ei voida rekisteröidä normaalimenettelyin. On vältettävä tilanne, jossa nämä henkilöt joutuvat kärsimään järjestelmän puutteellisuuksista ([3]).

Tietosuojavaltuutettu suosittaa tästä syystä, että kehitetään varajärjestelmämenettelyjä ja sisällytetään ne ehdotukseen. Nämä menetelmät eivät saisi alentaa viisumipolitiikan turvallisuustasoa eivätkä aiheuttaa ongelmia henkilöille, joiden sormenjäljet eivät ole luettavissa.

3.5 **Erityiset tietoluokat**

Jotkin tietoluokat (biometristen tietojen lisäksi) on otettava erityisesti huomioon: tiedot, jotka koskevat viisumin epäämistä (3.5.1) ja ryhmän muta jäseniä koskevat tiedot (3.5.2).

3.5.1 *Viisumin epäämisen perustelut*

Ehdotuksen 10 artiklan 2 kohdassa säädetään, että kun viisumihakemus on päätetty evätä, hakemuksen epäämisen perustelut on lisättävä hakemustiedostoon. Epäämisen syyt on vakioitu.

— Ensimmäiset kaksi syytä (a ja b alakohta) ovat lähinnä hallinnollisia: hakija ei ole esittänyt voimassa olevaa matkustusasiakirjaa tai asiakirjoja, jotka osoittavat suunnitellun oleskelun tarkoituksen ja edellytykset.

— c alakohdassa mainitaan, että ”hakija on määrätty maahantulokieltoon”, mikä tarkoittaa, että SIS-tietokantaan on tehty haku.

— d alakohdassa syynä on se, että ”hakija muodostaa uhkan jonkin jäsenvaltion yleiselle järjestykselle, sisäiselle turvallisuudelle, kansanterveydelle tai kansainvälisille suhteille”.

([1])

Biometriset tiedot	Kasvot	Sormi	Iiris
FTE % ei voida rekisteröidä	—	4	7
FNMR % hylkäämisaste	4	2.5	6
FMR1 % tarkistusvirheaste	10	< 0,01	< 0,001
FMR2 % tunnistusvirheaste, kun dB > 1 m	40	0,1	—
FMR3 % karsintatarkastusvirheaste, kun dB = 500	12	< 1	—

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

([2]) *Biometrics at the frontiers: assessing the impact on Society*, February 2005, Institute for Prospective Technological Studies, Yhteinen tutkimuskeskus, Euroopan komissio.

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

Kaikkia epäämisen syitä on sovellettava hyvin huolellisesti hakijalle mahdollisesti aiheutuvien seurausten vuoksi. Lisäksi jotkin niistä, kuten c ja d alakohdassa mainitut, johtavat direktiivin 95/46/EY 8 artiklan mukaiseen "arkaluonteisten tietojen" käsittelyyn.

Tietosuojavaltuutettu haluaa erityisesti kiinnittää huomiota kansanterveyteen liittyvään edellytykseen, joka vaikuttaa epämääräiseltä ja edellyttää hyvin arkaluonteisten tietojen käsittelyä. Ehdotukseen liitettyjä artikloja koskevien kommenttien mukaan viittaus kansanterveyteen kohdistuvaan uhkaan perustuu ehdotukseen neuvoston asetukseksi henkilöiden toimesta tapahtuvaa rajojen ylittämistä koskevasta yhteisön säännöstöstä (KOM (2004) 391 lopull.).

Tietosuojavaltuutettu on tietoinen siitä, että kansanterveyskriteeriä käytetään laajalti henkilöiden vapaata liikkuvuutta koskevassa yhteisön lainsäädännössä ja että sitä sovelletaan hyvin tiukasti, kuten Euroopan unionin kansalaisten ja heidän perheenjäsentensä oikeudesta liikkua ja oleskella vapaasti jäsenvaltioiden alueella 29 päivänä huhtikuuta 2004 annetussa Euroopan parlamentin ja neuvoston direktiivistä 2004/38/EY voidaan todeta. Kyseisen direktiivin 29 artiklassa säädetään edellytyksistä kansanterveyteen kohdistuvan uhkan huomioon ottamiseksi: "Vain sellaisen taudin perusteella, joka on jokin Maailman terveysjärjestön asiaankuuluvissa asiakirjoissa määritelty, mahdollisesti epidemian aiheuttava tauti tai muu tarttuva tauti tai tarttuva loistauti, ovat vapaata liikkuvuutta rajoittavat toimenpiteet oikeutettuja, edellyttäen, että näistä taudeista säädetään suojaa koskevissa säännöksissä, joita sovelletaan vastaanottavan jäsenvaltion kansalaisiin."

— On kuitenkin huomattava, että ehdotus, johon tässä viitataan, on toistaiseksi vain ehdotus, ja että sellaisen edellytyksen lisääminen VIS-asetukseen, jossa todetaan ettei kansanterveydelle saa aiheutua uhkaa, edellyttää mainitun yhteisön säännöstön hyväksymistä.

— Lisäksi, jos ehdotus hyväksytään, tätä perustetta maahantulon epäämiselle olisi tulkittava rajoittavasti. Edellä mainittu ehdotus yhteisön säännöstöksi perustuu näet puolestaan edellä mainittuun direktiiviin 2004/38/EY.

Tietosuojavaltuutettu suosittaa tästä syystä, että ehdotuksen tekstiin sisällytetään viittaus direktiivin 2004/38/EY 29 artiklaan, jotta olisi selvää, että "uhka kansanterveydelle" tarkoittaa kyseisessä säännöksessä tarkoitettua uhkaa. Joka tapauksessa tietojen arkaluonteisuuden vuoksi niitä tulisi käsitellä vain sellaisessa tapauksessa, että uhka kansanterveydelle on todellinen, ajankohtainen ja riittävän vakava.

3.5.2 *Ryhmän muita jäseniä koskevat tiedot*

Ehdotuksen 2 artiklan 7 kohdan mukaan 'ryhmän jäsenellä' tarkoitetaan "muita hakijoita, joiden kanssa hakija matkustaa yhdessä, mukaan luettuina hakijan mukana oleva puoliso ja lapset." Artikloja koskevissa kommenteissa todetaan, että ehdotuksen 2 artiklan määritelmissä viitataan perustamissopimuksen tai Schengenin säännöstön viisumipolitiikkaa koskeviin kohtiin, lukuun ottamatta joitain termejä, kuten 'ryhmän jäsen', jotka on määritelty nimenomaan tämän asetuksen soveltamista varten. Tästä voidaan olettaa, että tämä määritelmä ei perustu yhteisissä konsuliohjeissa annettuun 'ryhmäviisumin' määritelmään (artikla 2.1.4). Artikloja koskevissa kommenteissa viitataan hakijoihin, jotka matkustavat ryhmänä muiden hakijoiden kanssa, esim. ADS-sopimuksen puitteissa tai yhdessä perheenjäsenten kanssa.

Tietosuojavaltuutettu haluaa painottaa, että asetuksessa olisi annettava 'ryhmän jäsenen' tarkka ja kattava määritelmä. Nykyisessä ehdotuksessa oleva määritelmä on liian epämääräinen, koska selkeä viittaus perustamissopimukseen tai Schengenin säännöstöön puuttuu. Nykyisen sanamuodon mukaan 'ryhmän jäsen' voisi olla esimerkiksi kollega, muu saman matkatoimiston asiakas, joka osallistuu järjestettyyn matkaan jne. Tällä on merkittäviä seurauksia:

asetusehdotuksen 5 artiklan mukaan hakijan viisumihakemustiedosto linkitetään ryhmän muiden jäsenten tiedostoihin.

3.6 **Tietojen säilyttäminen**

Asetusehdotuksen 20 artiklassa säädetään, että kaikki hakemustiedostot on säilytettävä viisumitietojärjestelmässä viiden vuoden ajan. Yhteisön lainsäätäjän on tehtävä tämä toimintapoliittinen valinta ja määriteltävä sopivaksi katsomansa aika.

Ei ole perustetta — ei varsinkaan artikloihin liittyvissä kommenteissa esitettyjen perusteiden pohjalta — esittää, että ehdotuksessa tehty valinta olisi kohtuuton tai että sillä olisi seurauksia, joita ei voida hyväksyä, edellyttäen, että kaikki asianmukaiset oikaisujärjestelyt on luotu. Tämä tarkoittaa sitä, että tietoja on voitava oikaista ja poistaa silloin, kun tiedot eivät ole enää paikkansapitäviä, ja erityisesti silloin, kun henkilö on saanut jonkin jäsenvaltion kansalaisuuden tai aseman, joka ei edellytä hänen tietojensa tallentamista järjestelmään.

Lisäksi jos tiedot ovat vielä järjestelmässä, ne eivät saa vaikuttaa uuteen päätökseen. Jotkin epäämisperusteet ovat voimassa vain rajoitetun ajan (erityisesti hakijan maahantulokielto, uhka kansanterveydelle). Se, että nämä syyt ovat aikanaan olleet päteviä perusteita maahantulon kieltämiselle, ei saa vaikuttaa uuteen päätökseen. Tilanne on arvioitava kokonaisuudessaan uudelleen jokaisen uuden viisumihakemuksen yhteydessä, ja tämä olisi tuotava selvästi esiin asetuksessa aina asiaankuuluvissa kohdissa.

3.7 **Pääsy tietoihin ja tietojen käyttö**

3.7.1 *Alustavat huomiot*

Tietosuojavaltuutettu haluaa ensiksi todeta, että VIS:ään pääsyä ja sen tietojen käyttöä koskevat säännökset on selvästikin laadittu huolella. Kullakin viranomaisella on pääsy eri tietoihin eri tarkoituksia varten. Tämä on hyvä lähestymistapa, jota tietosuojavaltuutettu kannustaa käyttämään. Seuraavien huomioiden tarkoituksena on kehittää edelleen tätä lähestymistapaa.

3.7.2 *Viisumien tarkastaminen ulkorajoilla sijaitsevissa tarkastuspisteissä ja jäsenvaltion alueella*

Ulkorajoilla suoritettavilla viisumitarkastuksilla on asetusehdotuksen 16 artiklan mukaan kaksi eri tarkoitusta, jotka on tuotu selkeästi ilmi:

— ”henkilöllisyyden tarkistaminen”, mikä tarkoittaa annetun määritelmän mukaan ”yksi yhteen” -tarkistusta;

— ”viisumin aitouden tarkistaminen”. ICAO-standardien mukaan viisumin mikrosirussa voitaisiin käyttää julkista/yksityistä avainjärjestelmää (PKI) tämän todentamismenettelyn suorittamiseksi.

Nämä kaksi tarkoitusta voidaan varsin hyvin saavuttaa niin, että viisumitarkastuksista vastaavilla toimivaltaisilla viranomaisilla on pääsy pelkästään suojattuun mikrosiruun. Pääsy koko VIS-keskustietojärjestelmään olisi tätä tarkoitusta varten suhteeton. Jos näin toimittaisiin, VIS:ään pääsisi enemmän viranomaisia, mikä voisi lisätä väärinkäytön vaaraa. Se olisi myös kalliimpi vaihtoehto kuin valvottu ja suojattu pääsy VIS:ään ja edellyttäisi myös yhä enemmän erityiskoulutusta.

Lisäksi voidaan kysyä, onko 16 artiklan 2 kohdan mukainen pääsy tietoihin aiheellinen. Kyseisen artiklan 2 kohdan a alakohdassa todetaan, että jos ensimmäinen haku osoittaa, että hakijan tiedot on tallennettu viisumitietojärjestelmään (niin kuin asia periaatteessa on), toimivaltaiselle viranomaiselle on annettava oikeus tutustua muihin tietoihin henkilöllisyyden tarkistamista varten. Nämä muut tiedot voivat koskea kaikkia tietoja, jotka liittyvät viisumihakemukseen, ja voivat olla valokuvia, sormenjälkiä sekä liittyä mahdolliseen aiemmin myönnettyyn, mitätöityyn, peruutettuun tai pidennettyyn viisumiin.

Kun henkilöllisyys on tarkistettu, ei ole lainkaan selvää, mihin näitä muita tietoja enää tarvitaan. Pääsy niihin tulisi todellakin antaa rajoitetuin edellytyksin ainoastaan, jos tarkistusmenettely epäonnistuu. Silloin 16 artiklan 2 kohdassa mainitut tiedot toimisivat osaltaan varajärjestelmänä henkilöllisyyden varmistamisessa. Niihin pääsyä ei tulisi antaa jokaiselle rajavalvontapisteessä työskentelevälle vaan ainoastaan vaikeista tapauksista vastaavalle henkilöstölle.

Myös ne viranomaiset, joille annetaan pääsy VIS:ään, olisi määriteltävä tarkemmin. Erityisesti ilmaisu ”jäsenvaltion alueella suoritettavista tarkastuksista vastaavat toimivaltaiset viranomaiset” on epäselvä. Tietosuojavaltuutettu olettaa sen tarkoittavan *viisumitarkastuksista* vastaavia toimivaltaisia viranomaisia. 16 artiklaa olisi muutettava tähän suuntaan.

3.7.3 *Tietojen käyttö laittomien maahanmuuttajien tunnistamista ja palauttamista varten ja turvapaikkahakemuksen käsittelyä varten*

Ehdotuksen 17, 18 ja 19 artiklassa kuvatuissa tapauksissa (laittomien maahanmuuttajien palauttaminen ja turvapaikkahakemuksen käsittely) VIS:ää käytetään tunnistamiseen. Tunnistamisessa käytetään muun muassa valokuvia. Automaattiseen kasvojen tunnistamiseen käytettävä tekniikka näin laajamittaisessa tietotekniikkajärjestelmässä ei nykyisellään salli valokuvan käyttöä tunnistamiseen (yksi moneen -vertailu); valokuva ei takaa luotettavaa tulosta. Valokuvia ei näin ollen voida pitää soveltuvina tietoina tunnistamisessa.

Tästä syystä tietosuojavaltuutettu ehdottaakin painokkaasti, että ilmaisu ’valokuvat’ poistetaan näiden artiklojen 1 kohdasta ja säilytetään vain 2 kohdassa (valokuvia voidaan käyttää välineenä henkilöllisyyden tarkistamiseen, mutta ei tunnistamistarkoitukseen laajassa tietokannassa).

Toinen vaihtoehto olisi muuttaa 36 artiklaa niin, että valokuvien käsittelyyn tarvittavat toiminnot tunnistamista varten toteutetaan järjestelmässä vasta sitten, kun kyseistä tekniikkaa pidetään luotettavana (mahdollista teknisen komitean lausunnon jälkeen).

3.7.4 *Niitä viranomaisia koskevien tietojen julkaiseminen, joilla on pääsy VIS:ään*

Asetusehdotuksen 4 artiklassa säädetään, että luettelot jäsenvaltioiden nimeämistä toimivaltaisista viranomaisista, joilla on pääsy VIS:ään, julkaistaan Euroopan unionin virallisessa lehdessä. Tiedot olisi julkaistava säännöllisesti (vuosittain) kansallisten tilanteiden muutoksista tiedottamiseksi. Tietosuojavaltuutettu korostaa, että julkaiseminen on välttämätöntä niin Euroopan unionin kuin kansallisella ja paikallistasolla toteutettavan valvonnan vuoksi.

3.8 **Vastuualueet**

On syytä muistaa, että VIS perustuu keskitettyyn arkkitehtuuriin, jossa on keskustietokanta, johon kaikki tiedot viisumeista tallennetaan, ja kansalliset käyttöliittymät, jotka sijaitsevat jäsenvaltioissa ja joiden kautta toimivaltaiset viranomaiset pääsevät keskusjärjestelmään. Asetusehdotuksen johdanto-osan 14 ja 15 kappaleen mukaan jäsenvaltioiden on sovellettava asetuksen mukaisesti toteuttamassaan henkilötietojen käsittelyssä direktiiviä 95/46/EY, ja asetusta 45/2001 on sovellettava henkilötietojen suojelua koskeviin komission toimiin. Kuten näissä johdanto-osan kappaleissa todetaan, ehdotuksella pyritään selventämään eräitä näkökohtia, jotka koskevat tietojen käyttöön liittyvää vastuuta ja tietosuojan valvontaa.

Nämä kohdat näyttävät todellakin liittyvän joihinkin keskeisiin yksityiskohtiin, joita ilman direktiivin 95/46/EY ja asetuksen 45/2001 suojatoimia ei sovellettaisi tai ne eivät olisi täysin yhdenmukaisia ehdotuksen kanssa. Direktiivin mukaisen kansallisen lainsäädännön soveltaminen edellyttää yleensä kyseiseen jäsenvaltioon sijoittautunutta rekisterinpitäjää (4 artikla), kun taas asetusta sovelletaan yhteisön toimielimen tai elimen suorittamaan henkilötietojen käsittelyyn silloin, kun käsittely suoritetaan yhteisön oikeuden soveltamisalaan kokonaan tai osittain kuuluvien toimien toteuttamiseen (3 artikla).

Asetusehdotuksen 23 artiklan 2 kohdan mukaan ”Viisumitietojärjestelmä käsittelee tiedot jäsenvaltioiden puolesta.” 23 artiklan 3 kohdan mukaan kunkin jäsenvaltion on nimettävä viranomainen, joka toimii direktiivin 95/46/EY 2 artiklan d kohdassa tarkoitettuna rekisterinpitäjänä. Tämä näyttäisi tarkoittavan, että direktiivin järjestelmän mukaan komissiota olisi pidettävä tietojen käsittelijänä. Tämä vahvistetaan myös artiklojen perusteluissa ([1]).

Tämä muotoilu ei korosta tarpeeksi komission erittäin tärkeää ja itse asiassa keskeistä tehtävää sekä järjestelmän kehitysvaiheessa että sen normaalin toiminnan aikana. On vaikea yhdistää komission tehtävä rekisterinpitäjän tai tietojen käsittelijän rooliin. Komissio ei ole tietojen käsittelijä, jolla on epätavallinen toimivalta (muun muassa järjestelmän suunnittelussa) eikä myöskään rekisterinpitäjä, johon kohdistuu rajoituksia (koska jäsenvaltiot tallentavat ja käyttävät tietoja). Komissiolla on todellisuudessa *sui generis* -rooli ([2]) VIS:ssä.

Tämä tärkeä tehtävä olisi otettava huomioon muotoilussa niin, että komission tehtävät kuvaillaan kattavasti eikä sanamuodoin, jotka eivät täysin vastaa todellisuutta, koska tehtävät on esitetty liian rajoitettuina, ne eivät muuta mitään VIS:n toiminnassa ja pelkästään johtavat sekaannuksiin. Tämä on tärkeää myös VIS:n johdonmukaisen ja tehokkaan valvonnan kannalta (ks. myös 3.11. kohta). Tästä syystä tietosuojavaltuutettu suosittaa, että 23 artiklan 2 kohta poistetaan.

Tietosuojavaltuutettu haluaa painottaa, että komission tehtävistä on tärkeää antaa täydellinen kuvaus myös siksi, että komissio aikoo antaa järjestelmän hallinnoinnin jollekin muulle elimelle. Ehdotukseen liitetyssä rahoitusselvityksessä mainitaan mahdollisuus siirtää nämä tehtävät ulkorajavirastolle. Tässä yhteydessä on erittäin tärkeää, että komissio ei jätä mitään epäselvyyttä tehtävistään, jotta sen seuraaja tietää toimivaltansa rajat.

3.9 **Turvallisuus**

VIS:n optimaalisen turvatason hallinta ja noudattaminen ovat perusedellytys sen tietokantaan tallennettujen henkilötietojen tarvittavan suojan varmistamiseksi. Tämän tyydyttävän turvatason toteuttamiseksi on otettava käyttöön asianmukaisia suojatoimenpiteitä järjestelmän infrastruktuuriin ja sitä käyttäviin henkilöihin liittyvien mahdollisten riskien varalta. Tätä kysymystä käsitellään ehdotuksen useissa kohdissa, mutta muotoilua on vielä parannettava.

Ehdotuksen 25 ja 26 artiklassa esitetään useita tietoturvaa koskevia toimenpiteitä ja erilaisia väärinkäyttötilanteita, jotka olisi estettävä. Näitä säännöksiä olisi kuitenkin hyvä täydentää toimenpiteillä, joilla valvotaan järjestelmällisesti jo mainittujen turvatoimien tehokkuutta ja raportoitaisiin siitä. Tietosuojavaltuutettu suosittaa erityisesti, että säännöksiä turvatoimenpiteiden säännöllisestä (sisäisestä) valvonnasta lisätään näihin artikloihin.

Tämä liittyy ehdotuksen 40 artiklaan, jossa säädetään seurannasta ja arvioinnista. Tämän ei tulisi koskea pelkästään toiminnan tulosten, kustannustehokkuuden ja palvelujen laadun seurantaa ja arviointia vaan myös lakisääteisten vaatimusten noudattamista, erityisesti tietosuojan alalla. Tietosuojavaltuutettu suosittaa tästä syystä, että 40 artiklan soveltamisalaa laajennetaan tietojen käsittelyn lainmukaisuuden valvontaan ja siitä raportointiin.

Lisäksi 24 artiklan 4 kohdan c alakohtaa ja 26 artiklan 2 kohdan e alakohtaa olisi täydennettävä. Olisi lisättävä, että jäsenvaltioiden on varmistettava, että asianmukaisesti valtuutetulla henkilöstöllä, jolla on pääsy tietoihin, on tarkat käyttäjäprofiilit (jotka olisi pidettävä kansallisten valvontaviranomaisten saatavilla tarkastuksia varten). Näiden käyttäjäprofiilien lisäksi jäsenvaltioiden on laadittava täydellinen luettelo käyttäjistä ja pidettävä se jatkuvasti ajan tasalla. Sama koskee komissiota: 25 artiklan 2 kohdan b alakohtaa olisi täydennettävä samansuuntaisesti.

([1]) Ks. ehdotuksen sivu 37.

([2]) Vaikka direktiivissä 95/46/EY ja asetuksessa 45/2001 annettu rekisterinpitäjän määritelmä mahdollistaakin sen, että rekisterinpitäjiä voi olla useita eri vastuualuein.

Näitä turvatoimenpiteitä täydennetään seurannalla ja organisatorisilla turvajärjestelyillä. Ehdotuksen 28 artiklassa esitetään kaikkien tietojenkäsittelytapahtumien kirjaamisen edellytykset ja tarkoitus. Tietoja ei rekisteröidä vain tietosuojan valvomiseksi ja tietoturvan varmistamiseksi vaan myös VIS:n säännöllistä sisäistä valvontaa varten. Valvontaraportit auttavat osaltaan valvontaviranomaisia hoitamaan tehtävänsä tehokkaasti, määrittämään heikot kohdat sekä keskittymään niihin omissa valvontamenettelyissään.

3.10 **Rekisteröidyn henkilön oikeudet**

3.10.1 *Rekisteröidylle tiedottaminen*

Tietojen asianmukaisen käsittelyn varmistamiseksi on rekisteröidylle henkilölle tiedottaminen äärimmäisen tärkeää. Kyseessä on yksilön oikeuksien suojaamisen kannalta välttämätön suojatoimi. Ehdotuksen 30 artikla noudattaa tässä nykyisellään pääosin direktiivin 95/47/EY 10 artiklaa.

Säännöstä voitaisiin kuitenkin hieman muuttaa, jotta se soveltuisi paremmin VIS:n puitteisiin. Direktiivissä säädetään tiettyjen tietojen antamisesta, mutta lisätietoja annetaan, jos se tarpeen ([1]). Ehdotuksen 30 artiklaa olisi muutettava niin, että seuraavat seikat lisätään:

— Rekisteröidylle tulisi ilmoittaa myös hänen tietojensa säilyttämisaika.

— Ehdotuksen 30 artiklan 1 kohdan e alakohta koskee oikeutta ”tutustua itseään koskeviin tietoihin ja oikaista niitä”. Tämän voisi ilmaista täsmällisemmin seuraavasti: ”oikeus tutustua itseään koskeviin tietoihin ja oikeus *pyytää niiden oikaisua tai poistoa*”. Rekisteröidyille tulisi ilmoittaa mahdollisuudesta pyytää neuvoja tai apua asiasta asianomaisilta valvontaviranomaisilta.

— Ehdotuksen 30 artiklan 1 kohdan a alakohdassa mainitaan rekisterinpitäjän ja tämän mahdollisen edustajan henkilöllisyys. Koska rekisterinpitäjän on aina oltava sijoittautunut Euroopan unionin alueelle, viimeksi mainittua mahdollisuutta ei tarvitse ottaa huomioon.

3.10.2 *Oikeus tutustua tietoihin, oikaista niitä ja poistaa ne*

Ehdotuksen 31 artiklan 1 kohdan viimeisessä virkkeessä todetaan: ”Ainoastaan jäsenvaltio voi antaa luvan tutustua tietoihin.” Tämän voidaan olettaa tarkoittavan, että keskusyksikkö ei voi antaa oikeutta tutustua tietoihin (tai ilmoittaa niistä) vaan ainoastaan jäsenvaltiot voivat tehdä sen. Tietosuojavaltuutettu suosittaa, että ilmaistaisiin selvästi, että tietojen ilmoittamista voidaan pyytää missä tahansa jäsenvaltiossa.

Lisäksi tämä säännös on muotoiltu niin, että se näyttäisi tarkoitettavan, että oikeutta tutustua tietoihin ei voi evätä ja että se voidaan antaa ilman vastuussa olevan jäsenvaltion suostumusta. Tämä näyttäisi selittävän sen, miksi kansallisten viranomaisten on tehtävä yhteistyötä valvoakseen 31 artiklan 2, 3 ja 4 kohdassa säädettyjen oikeuksien mutta ei 31 artiklan 1 kohdassa säädettyjen oikeuksien toteutumista ([2]).

3.10.3 *Valvontaviranomaisten apu*

Ehdotuksen 33 artiklan 2 kohdassa säädetään, että kansallisten valvontaviranomaisten velvollisuus auttaa ja neuvoa asianomaista henkilöä säilyy asian koko (oikeus)käsittelyn ajan. Tämä kohta on epäselvä. Kansalliset valvontaviranomaiset suhtautuvat eri tavoin rooliinsa oikeuskäsittelyssä. Nykyinen sanamuoto saa asian kuulostamaan siltä kuin heidän olisi toimittava kantajan oikeudellisina neuvonantajina oikeudessa, mikä ei ole mahdollista monissa maissa.

([1]) Direktiivissä todetaan: ”(…) siltä osin kuin nämä lisätiedot ovat tarpeen ottaen huomioon erityiset olosuhteet, joissa tiedot kerätään, rekisteröidyn kannalta asianmukaisen tietojenkäsittelyn takaamiseksi.”

([2]) Tästä seuraa, että 31 artiklan 3 kohtaa, joka koskee kansallisten viranomaisten yhteistyötä tietojen oikaisun ja poiston suhteen, olisi muutettava tämän suuntaisesti asian selventämiseksi: ”Jos *31 artiklan 2 kohdan mukainen* pyyntö (…)”. 31 artiklan 1 kohdan mukainen pyyntö (oikeus tutustua tietoihin) ei edellytä viranomaisten välistä yhteistyötä.

3.11 **Valvonta**

Ehdotuksessa valvontatehtävä jaetaan kansallisten valvontaviranomaisten ja Euroopan tietosuojavaltuutetun kesken. Tämä on yhdenmukaista ehdotuksessa omaksutun sovellettavaa lainsäädäntöä ja VIS:n toimintaan ja käyttöön liittyvää vastuuta koskevan lähestymistavan kanssa ja tehokkaan valvonnan vaatimuksen kanssa. Tietosuojavaltuutettu pitää tätä lähestymistapaa hyvänä 34 ja 35 artiklassa.

Kansalliset valvontaviranomaiset valvovat, että jäsenvaltiot käsittelevät henkilötietoja lainmukaisesti, *mukaan luettuna näiden tietojen siirtäminen viisumitietojärjestelmään ja sieltä muualle*. Tietosuojavaltuutettu valvoo komission toimintaa, niin *että henkilötietojen siirtäminen kansallisten käyttöliittymien ja keskusviisumitietojärjestelmän välillä tapahtuu lainmukaisesti*. Tästä saattaa aiheutua toiminnan päällekkäisyyttä, sillä sekä kansallinen valvontaviranomainen että Euroopan tietosuojavaltuutettu ovat samanaikaisesti vastuussa siitä, että tietojen siirtäminen kansallisten käyttöliittymien ja keskusviisumitietojärjestelmän välillä tapahtuu lainmukaisesti.

Tietosuojavaltuutettu ehdottaa tästä syystä, että 34 artiklaa muutetaan sen selventämiseksi, että kansallinen valvontaviranomainen valvoo henkilötietojen käsittelyn lainmukaisuutta jäsenvaltioissa, mukaan luettuna niiden siirtäminen kansallisten käyttöliittymien ja keskusviisumitietojärjestelmän välillä.

VIS:n valvonnan suhteen on tärkeää myös korostaa, että kansallisen valvontaviranomaisen valvontatoimia ja tietosuojavaltuutetun valvontatoimia olisi koordinoitava tietyssä määrin, jotta taataan riittävä johdonmukaisuus ja yleinen tehokkuus. Asetus olisi pantava täytäntöön yhdenmukaisesti, ja yhteisiin ongelmiin olisi hyvä löytää ratkaisu yhdessä. Lisäksi voidaan todeta turvallisuuden osalta, että VIS:n turvataso määräytyy lopulta sen heikoimman lenkin mukaan. Tässä mielessä myös tietosuojavaltuutetun ja kansallisten viranomaisten välinen yhteistyö on organisoitava ja sitä on tehostettava. Ehdotuksen 35 artiklassa tulisi olla säännös siitä, että tietosuojavaltuutettu kutsuu koolle kaikki kansalliset valvontaviranomaiset vähintään kerran vuodessa.

3.12 **Täytäntöönpano**

Ehdotuksen 36 artiklan 2 kohdassa säädetään: *"Edellä 1 kohdassa tarkoitettujen toimintojen teknistä toteuttamista varten tarvittavat toimenpiteet hyväksytään 39 artiklan 2 kohdassa tarkoitetun menettelyn mukaisesti."* 39 artiklassa viitataan joulukuussa 2001 perustettuun komiteaan ([1]), joka avustaa komissiota ja jota on käytetty usean säädöksen yhteydessä.

VIS:n toimintojen teknisellä toteuttamisella (vuorovaikutus toimivaltaisten viranomaisten kanssa ja yhtenäinen viisumin kaava) on useita mahdollisesti huolestuttavia vaikutuksia tietosuojaan. Esimerkiksi se, liitetäänkö viisumiin mikrosiru, vaikuttaa siihen, miten keskustietokantaa käytetään, ja samoin se, mitä formaattistandardia biometristen tietojen vaihdossa käytetään, vaikuttaa tietosuojapolitiikan toteuttamiseen ja suunnitteluun. ([2])

Tekniset valinnat vaikuttavat merkittävällä tavalla tarkoitusperiaatteen ja suhteellisuusperiaatteen toteuttamiseen, ja näitä valintoja tulisi tästä syystä valvoa. Teknisistä valinnoista, joilla on huomattava vaikutus tietosuojaan, tulisikin säätää asetuksella yhteispäätösmenettelyn mukaisesti. Vain näin voidaan taata tarvittava poliittinen valvonta. Kaikissa muissa tapauksissa, joilla on vaikutusta tietosuojaan, tietosuojavaltuutetulle tulisi antaa mahdollisuus antaa lausunto komitean tekemistä valinnoista.

3.13 **Yhteentoimivuus**

Yhteentoimivuus on keskeinen perusedellytys VIS:n tapaisten laajamittaisten tietotekniikkajärjestelmien tehokkuudelle. Se auttaa vähentämään kokonaiskustannuksia johdonmukaisesti ja välttämään heterogeenisten elementtien aiheuttamaa redundanssia. Yhteentoimivuus voi myös osaltaan edistää yhteisen viisumipolitiikan tavoitetta, sillä tällöin samaa menettelyä sovelletaan kaikkiin politiikan keskeisiin osiin. On kuitenkin tärkeää erottaa toisistaan kaksi yhteentoimivuuden tasoa:

— Yhteentoimivuus EU:n jäsenvaltioiden välillä on erittäin toivottavaa; yhden jäsenvaltion lähettämien viisumihakemusten tulee olla yhteentoimivia jonkin toisen jäsenvaltion viranomaisten lähettämien hakemusten kanssa.

([1]) Neuvoston asetus (EY) N:o 2424/2001, annettu 6 päivänä joulukuuta 2001, toisen sukupolven Schengenin tietojärjestelmän (SIS II) kehittämisestä.

([2]) Syyskuussa 2003 annettu ehdotus yhtenäisestä viisumin kaavasta annetun neuvoston asetuksen muuttamisesta sisälsi samanlaisen artiklan.

— Eri tarkoituksiin rakennettujen järjestelmien yhteentoimivuus tai yhteentoimivuus kolmansien maiden järjestelmien kanssa on paljon kyseenalaisempi asia.

Yksi järjestelmän tarkoituksen rajaamiseen tarkoitettuja suojatoimia, joilla estetään ns. *function creep* (tietojen käyttö muuhun kuin alkuperäiseen tarkoitukseen), on eri teknisten standardien käyttö. Lisäksi kahden eri järjestelmän vuorovaikutus olisi syytä dokumentoida perusteellisesti. Yhteentoimivuus ei saisi koskaan johtaa siihen, että viranomainen, jolla ei ole pääsyä järjestelmään eikä oikeutta käyttää joitakin tietoja, voi päästä järjestelmään toisen tietojärjestelmän kautta.

Tässä yhteydessä tietosuojavaltuutettu viittaa terrorismin torjunnasta annettuun neuvoston julkilausumaan (25.3.2004), jossa komissiota pyydetään esittämään ehdotuksia tietojärjestelmien (SIS, VIS ja Eurodac) yhteentoimivuuden ja yhteisvaikutuksen parantamiseksi.

Tietosuojavaltuutettu haluaa myös mainita parhaillaan käytävät keskustelut siitä, mikä elin voisi huolehtia vastaisuudessa erilaisten laajojen järjestelmien hallinnoinnista (ks. myös tämän lausunnon 3.8 kohta).

Tietosuojavaltuutettu haluaa jälleen kerran painottaa, että järjestelmien yhteentoimivuutta ei voi toteuttaa niin, että toimitaan vastoin tarkoituksen rajoittamisen periaatetta, ja että kaikki tämänsuuntaiset ehdotukset tulisi toimittaa tietosuojavaltuutetulle.

4. **PÄÄTELMÄT**

4.1 **Yleiset seikat**

1. Euroopan tietosuojavaltuutettu toteaa, että yhteisen viisumipolitiikan kehittäminen edellyttää tehokasta merkityksellisten tietojen vaihtoa. VIS on yksi mahdollinen järjestelmä sujuvan tiedonkulun varmistamiseksi. Tietosuojavaltuutettu on pannut tarkoin merkille vaikutusarvioinnissa esitetyt perustelut. Vaikkakaan nämä perustelut eivät ole täysin vakuuttavia, ne näyttävät riittäviltä oikeuttamaan VIS:n perustamisen yhteisen viisumipolitiikan parantamiseksi.

   Tämä uusi väline tulisi kuitenkin rajoittaa tietojen keruuseen ja vaihtoon, jos tällainen keruu tai vaihto on tarpeen yhteisen viisumipolitiikan kehittämiseksi ja on oikeassa suhteessa tähän tarkoitukseen.

2. VIS:n perustamisella voi olla myönteisiä vaikutuksia muun oikeutetun yleisen edun kannalta, mutta tämä ei muuta VIS:n tarkoitusta. Tämän vuoksi VIS:n kaikkien osatekijöiden on oltava edellä mainitun poliittisen tavoitteen kannalta tarpeellisia ja oikeasuhteisia.

   Lisäksi:

   — Lainvalvontaviranomaisten automaattinen pääsy VIS:ään ei vastaa edellä mainittua tarkoitusta.

   — Tietosuojavaltuutettu suosittaa, että ero ”tarkoituksen” ja ”hyötyjen” välillä tehdään selvemmäksi 1 artiklan 2 kohdassa.

   — Yhteentoimivuutta muiden järjestelmien kanssa ei voi toteuttaa, jos se on vastoin tarkoituksen rajoittamisen periaatetta.

3. Tietosuojavaltuutettu myöntää biometristen tietojen käytön edut, mutta painottaa näiden tietojen käytön huomattavia vaikutuksia ja ehdottaa, että näiden tietojen käytölle säädetään tiukat suojatoimet. Lisäksi sormenjälkien tekniset puutteet edellyttävät, että kehitetään varajärjestelmämenettelyjä, jotka otetaan huomioon ehdotuksessa.

4. Tämä lausunto olisi mainittava asetuksen johdanto-osassa ennen varsinaisia johdanto-osan kappaleita (”ottavat huomioon … lausunnon”).

4.2 **Muut seikat**

5. Viisumin epäämisperusteet: Ehdotukseen olisi lisättävä viittaus direktiivin 2004/38/EY 29 artiklaan, jotta olisi selvää, että 'kansanterveyteen kohdistuvalla uhkalla' tarkoitetaan kyseisen säännöksen mukaista uhkaa.

6. Ryhmän jäseniä koskevilla tiedoilla on ehdotuksessa erityismerkitys: 'ryhmän jäsen' olisi määriteltävä tarkasti ja kattavasti.

7. Ei ole perustetta esittää, että ehdotuksessa tehty valinta tietojen säilyttämisajasta olisi kohtuuton tai että sillä olisi seurauksia, joita ei voida hyväksyä, edellyttäen, että kaikki asianmukaiset oikaisumekanismit on luotu.

   Lisäksi ehdotuksessa olisi selvennettävä, että henkilötiedot on arvioitava kokonaisuudessaan uudelleen joka kerta, kun on kyse uudesta viisumihakemuksesta.

8. Viisumitarkastukset ulkorajoilla: Ehdotuksen 16 artiklaa olisi muutettava, sillä VIS:ään pääsy olisi mainituissa tapauksissa suhteeton. Riittää, että viisumitarkastuksista vastaavilla toimivaltaisilla viranomaisilla on pääsy pelkästään suojattuun mikrosiruun.

   Lisäksi, jos henkilöllisyyden tarkastus on onnistunut, ei ole selvää, mitä varten muita tietoja vielä tarvitaan.

9. Tietojen käyttö laittomien maahanmuuttajien tunnistamiseen ja palauttamiseen sekä turvapaikkamenettelyissä: ilmaisu "valokuvat" tulisi poistaa 17, 18 ja 19 artiklan 1 kohdasta ja säilyttää 2 kohdassa.

10. Komission ja jäsenvaltioiden vastuut: 23 artiklan 2 kohta olisi poistettava.

11. Ehdotukseen tulisi lisätä säännökset turvatoimenpiteiden järjestelmällisestä (sisäisestä) valvonnasta. 40 artiklan soveltamisalaa on laajennettava käsittelyn laillisuuden valvontaan ja siitä raportointiin. Lisäksi:

   — Jäsenvaltioiden on laadittava täydellinen luettelo käyttäjistä ja pidettävä se jatkuvasti ajan tasalla. Sama koskee komissiota: 25 artiklan 2 kohtaa olisi täydennettävä tämänsuuntaisesti.

   — Ehdotuksen 28 artiklassa kuvataan tietojenkäsittelytapahtumien kirjaamisen edellytyksiä ja tarkoitusta. Näitä tapahtumia ei tallenneta ainoastaan tietosuojan noudattamisen valvomiseksi ja tietoturvallisuuden varmistamiseksi vaan myös VIS:n säännöllisen sisäisen valvonnan vuoksi.

12. Rekisteröidyn henkilön oikeudet

   — 30 artiklaa olisi muutettava, jotta varmistettaisiin, että rekisteröidylle henkilölle ilmoitetaan hänen tietojensa säilyttämisajasta.

   — 30 artiklan 1 kohdan e alakohdassa olisi mainittava "oikeus tutustua tietoihin ja oikeus pyytää niiden oikaisua tai poistoa".

   — 31 artiklan 1 kohdassa on tehtävä selväksi, että tietojen ilmoittamista voidaan pyytää missä tahansa jäsenvaltiossa.

13. Valvonta:

— 34 artiklaa olisi muuttava sen selventämiseksi, että kansallinen valvontaviranomainen valvoo henkilötietojen käsittelyn lainmukaisuutta jäsenvaltioissa, mukaan luettuna niiden siirtäminen kansallisten käyttöliittymien ja keskusviisumitietojärjestelmän välillä.

— 35 artiklassa tulisi olla säännös siitä, että tietosuojavaltuutettu kutsuu koolle kaikki kansalliset valvontaviranomaiset vähintään kerran vuodessa.

14. Täytäntöönpano:

— Teknisistä valinnoista, joilla on huomattava vaikutus tietosuojaan, tulisi säätää asetuksella yhteispäätösmenettelyn mukaisesti.

— Kaikissa muissa tapauksissa, joilla on vaikutusta tietosuojaan, tietosuojavaltuutetulle tulisi antaa mahdollisuus antaa lausunto ehdotuksessa tarkoitetun komitean tekemistä valinnoista.

Tehty Brysselissä 23 päivänä maaliskuuta 2005

Peter HUSTINX

Euroopan tietosuojavaltuutettu