EIROPAS DATU AIZSARDZĪBAS UZRAUDZĪTĀJA

Eiropas Datu aizsardzības uzraudzītāja atzinums par priekšlikumu Eiropas Parlamenta un Padomes Regulai par Vīzu informācijas sistēmu (VIS) un datu apmaiņu starp dalībvalstīm saistībā ar īstermiņa vīzām (COM(2004)835 galīgā redakcija)

(2005/C 181/06)

EIROPAS DATU AIZSARDZĪBAS UZRAUDZĪTĀJS,

ņemot vērā Eiropas Kopienas dibināšanas līgumu un jo īpaši tā 286. pantu;

ņemot vērā Eiropas Savienības Pamattiesību hartu un jo īpaši tās 8. pantu;

ņemot vērā Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīvu 95/46/EK par indivīdu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti;

ņemot vērā Eiropas Parlamenta un Padomes 2000. gada 18. decembra Regulu (EK) Nr. 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti, un jo īpaši tās 41. pantu;

ņemot vērā no Komisijas 25. janvārī saņemto lūgumu dot atzinumu saskaņā ar Regulas (EK) Nr. 45/2001 28. panta 2. punktu,

IR PIEŅĒMUSI ŠO ATZINUMU.

1. **IEVADS**

1.1. **Provizoriskas piezīmes**

Vīzu informācijas sistēmas (VIS) izveide ir nozīmīga ES kopējās vīzu politikas daļu, un uz to attiecas vairāki savstarpēji saistīti instrumenti.

— 2003. gada aprīlī par VIS notika tehniska un ekonomiska izpēte ([1]), ko bija pasūtījusi Komisija.

— Komisija 2003. gada septembrī ierosināja veikt grozījumu agrākā regulā ([2]), ar ko nosaka vienotu vīzu formu. Galvenais mērķis ir ieviest biometrijas datus (sejas attēls un divi pirkstu nospiedumi) jaunajā vīzu formā. Šie biometrijas dati glabātos mikroshēmā.

([1]) Vīzu informācijas sistēma, nobeiguma ziņojums, ko sagatavojusi EK un ko vadījis *Trasys,* 2003. gada aprīlis.
([2]) COM(2003) 558 galīgā redakcija 2003/0217 (CNS) un 2003/0218 (CNS)

— 2004. gada jūnijā ar Padomes lēmumu ([1]) sākās Vīzu informācijas sistēmas izveide, nodrošinot tiesisku pamatu to iekļaut ES budžetā. Lēmumā bija ierosināts izveidot centrālu datu bāzi, kurā būtu ietverta informācija par vīzu pieteikumiem un paredzēto "komitoloģijas procesu", lai vadītu VIS tehnisku izstrādi.

Komisija 2004. gada decembrī pieņēma priekšlikumu Regulai par VIS un datu apmaiņu starp dalībvalstīm saistībā ar īstermiņa vīzām ([2]) (še turpmāk — "priekšlikums"), kas ir šī priekšlikuma subjekts. Priekšlikumam ir pievienota Izvērsta efektivitātes ekspertīze ([3]) (še turpmāk — "IEE"). .

Tomēr, kā izklāstīts paskaidrojuma rakstā, būs vajadzīgi vēl citi juridiski instrumenti, lai papildinātu šo regulu, jo īpaši, lai:

— veiktu grozījumus Kopīgās konsulārās instrukcijās attiecībā uz vīzām, kas adresētas Šengenas Konvencijas Līgumslēdzēju Pušu diplomātiskajām pārstāvniecībām un konsulārajām iestādēm (še turpmāk — "Kopīgās konsulārās instrukcijas"), kas attiecas uz biometrijas datu ieviešanu procedūrās;

— pilnīgotu jaunu mehānismu datu apmaiņai ar Īriju un Apvienoto Karalisti;

— apmainītos ar datiem par ilgtermiņa vīzām.

Kā nolemts Tieslietu un iekšlietu padomē 2003. gada 5. un 6. jūnijā un aprakstīts minētajā Padomes 2004. gada jūnija lēmuma 1. panta 2. punktā, VIS veidos, pamatojoties uz centralizētu arhitektūru, ietverot datu bāzi, kur glabās vīzu pieteikumus: Centrālā vīzu informācijas sistēma (CS-VIS) un attiecīgas valsts saskarne (NI-VIS), kas atrodas katrā dalībvalstī. Dalībvalstis izvēlēs ([4]) centrālu valsts iestādi, ko saistīt ar valstu saskarnēm un ar kuras starpniecību to attiecīgām kompetentām iestādēm būs piekļuve CS un VIS.

1.2. **Galvenie priekšlikuma aspekti no datu aizsardzības viedokļa**

Priekšlikuma mērķis ir uzlabot kopējās vīzu politikas administrēšanu, sekmējot datu apmaiņu starp dalībvalstīm, tādējādi veidojot centrālu datu bāzi. Regula paredz ieviest biometrijas datus (fotoattēls un pirkstu nospiedumi) vīzas pieteikuma iesniegšanas procedūras laikā, un glabāt tos centrālā datu bāzē.

Biometrijas datus var arī izmantot vīzu uzlīmēs, kā ir paredzēts, Komisijas ieteiktajos grozījumus regulā par vienotu vīzu formu, ieviešot fotoattēlus un pirkstu nospiedumus, ko glabāt mikroshēmā (kamēr vēl joprojām nav pieņemts Padomes lēmums, ko pamatos ar pašreiz notiekošās analīzes rezultātiem).

Priekšlikumā sīki aprakstītas dažādas darbības, ko veic ar datiem (to ievadīšana, grozījumu veikšana, dzēšana un izmantošana), un dažādi dati, kas jāpievieno Vīzu informācijas sistēmā, atkarībā no konkrēta pieteikuma (apstiprināšana, noraidīšana, utt.).

Priekšlikums paredz piecus gadus glabāt datus par katru pieteikumu.

Priekšlikumā uzskaitītas tikai kompetentās iestādes, izņemot par vīzām atbildīgās iestādes, kurām būs piekļuve VIS, kā arī definētas tām piešķirtās piekļuves tiesības:

— kompetentas iestādes, kas veic vīzu pārbaudi pie ārējām robežām un dalībvalstu teritorijā,

— kompetentas imigrācijas iestādes,

([1]) 2004/512/EK (OV L 213, 15. 6. 2004., 5. lpp.).
([2]) COM(2004)835 galīgā redakcija 2004/0287 (COD).
([3]) Pētījums vīzu informācijas sistēmas izvērstajam ietekmes novērtējumam, EPNK galīgais ziņojums, 2004. gada x decembrī.
([4]) Priekšlikuma 24. panta 2. punkts.

— kompetentas iestādes, kas ir atbildīgas par patvēruma jautājumu risināšanu.

Priekšlikumā par VIS darbības un attiecīgo atbildību aprakstu ir uzsvērts, ka Komisija apstrādā VIS datus dalībvalstu vārdā. Tajā aprakstīta vajadzību izmantot datu apstrādes reģistrus, lai garantētu datu drošību, un sīki uzskaitītas attiecīgās atbildības, lai nodrošinātu šo drošības līmeni.

Priekšlikumā ir nodaļa par datu aizsardzību, kurā sīki aprakstīta valsts iestāžu, kā arī Eiropas datu aizsardzības uzraudzītāja vieta (še turpmāk — "EDAU"). .

Priekšlikumā VIS tehniskā īstenošana un vajadzīgo tehnoloģiju izvēle uzticēta komitejai, kas izveidota saskaņā ar 5. panta 1. punktu Regulā (EK) Nr. 2424/2001 par otrās paaudzes Šengenas Informācijas sistēmas (SIS II) izveidošanu.

Priekšlikumam ir pievienota VIS izvērstas efektivitātes ekspertīze, ko bija pasūtījusi Komisija un veicis EPNK (*European Policy Evaluation Consortium*). Tajā secināts, ka vislabākais risinājums ir VIS, kurā izmanto biometrijas datus, lai uzlabotu kopējo vīzu politiku.

2. **ATTIECĪGĀ SISTĒMA**

Priekšlikumam būs lielākā ietekme uz personu privāto dzīvi un pamattiesībām, tādēļ ir jāpārbauda, vai tas nav pretrunā datu aizsardzības principiem. Galvenie atsauces punkti pārbaudei ir šādi:.

— cieņa attiecībā uz privāto dzīvi Eiropā ir nodrošināta kopš Eiropas Padome 1950. gadā pieņēmusi Cilvēktiesību un pamatbrīvību aizsardzības konvenciju (še turpmāk — "ECK"). ECK 8. pantā ir paredzētas "tiesības attiecībā uz cieņu uz privāto un ģimenes dzīvi".

  Saskaņā ar 8. panta 2. punktu katra valsts varas iestāžu iejaukšanās, īstenojot tās tiesības, ir atļauta tikai tad, ja tas notiek "saskaņā ar likumu" un ir "vajadzīgs demokrātiskā sabiedrībā" svarīgu interešu aizsargāšanai. Eiropas Cilvēktiesību tiesas prakses gadījumā šie nosacījumi ir likuši paredzēt papildu prasības par tiesiskā pamata kvalitāti, lai iejaukšanās varētu notikt, kā arī attiecībā uz jebkādu pasākumu samērīgumu un vajadzību pēc piemērotiem aizsardzības mehāniskiem pret datu ļaunprātīgu izmantošanu.

  Personu aizsardzības pamatprincipi attiecībā uz personas datu apstrādi izstrādāti Konvencijā par datu aizsardzību, ko sagatavojusi Eiropas Padome un kas pieņemta 1981. gadā.

— Tiesības attiecībā uz privāto dzīvi un personas datu aizsardzību nesen izklāstītas Eiropas Savienības Pamattiesību hartas 7. un 8. pantā, kas ir iekļauti ES Konstitūcijas II daļā.

  Saskaņā ar Hartas 52. pantu, atzīts, ka uz šīm tiesībām var attiekties ierobežojumi, ar nosacījumu, ka tiek ievēroti līdzīgi nosacījumi, ko piemēro saskaņā ar ECK 8. pantu. Ir jāapsver šie nosacījumi, kad vien izvērtē priekšlikumu par iespējamu iejaukšanos.

Tagad ES tiesību aktos pamatnoteikumi par datu aizsardzību ir izklāstīti:

— Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīvā 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (OV L 281., 31. lpp.). Šo direktīva būs "Direktīva 95/46/EK". Ar šo direktīvu ir paredzēti sīki izstrādāti principi, saskaņā ar kuriem pārbaudīs priekšlikumu, ciktāl tam jāattiecas uz dalībvalstīm. Tas ir vēl jo svarīgāk tāpēc, ka priekšlikumu piemēros kopā ar attiecīgas valsts tiesību aktiem, kas dod juridisku spēku šai direktīvai. Ierosināto noteikumu un aizsardzības mehānismu efektivitāte tādējādi katrā konkrētā gadījumā būs atkarīga no šī apvienojuma efektivitātes.

— Eiropas Parlamenta un Padomes 2000. gada 18. decembra Regulā (EK) 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti (OV L 8., 1. lpp.). Šo regulu sauks "Regula 45/2001". Ar to nosaka līdzīgus principus kā Direktīvā 95/46/EK, un tā ir būtiska šajā sakarā tiktāl, ciktāl priekšlikumu piemēro Komisijas darbībās līdz ar Regulu. Tādēļ apvienotajai piemērošanai arī jāpievērš uzmanība.

Direktīva 95/46/EK un Regula 45/2001 jālasa kopā ar citiem tiesību aktiem. Citiem vārdiem sakot, direktīva un regula, ciktāl tajās risināti jautājumi par personu datu apstrādi, kas var radīt pamattiesību pārkāpumus, jo īpaši tiesības uz privāto dzīvi, ir jāinterpretē, ņemot vērā pamattiesības. Tas izriet arī no Eiropas Tiesas precedentu tiesībām ([1]).

— Visbeidzot EDAU analīzē iekļaus arī 29. panta Datu aizsardzības darbagrupas ([2]) 2004. gada 11. augusta atzinumu Nr. 7/2004 "par biometrijas elementu iekļaušanu uzturēšanās atļaujās un vīzās, ņemot vērā Eiropas vīzu informācijas sistēmas (VIS) izveidošanu". Atzinumā darbagrupa pauda bažas par vairākiem priekšlikuma elementiem. EDAU ir iecerējis pārbaudīt, vai šajā priekšlikumā ir tās ņemtas vērā.

3. **PRIEKŠLIKUMA ANALĪZE**

3.1. **Vispārēji noteikumi**

EDAU atzīst, ka turpmākai kopējās vīzu politikas izstrādāšanai ir vajadzīga efektīva attiecīgu datu apmaiņa. Viens no mehānismiem, kas var nodrošināt vienmērīgu informācijas plūsmu, ir VIS. Tomēr šādam jaunam instrumentam vajadzētu aprobežoties ar datu vākšanu un to apmaiņu, ciktāl vākšana un apmaiņa ir vajadzīga, lai izstrādātu kopējo vīzu politiku, un atbilst šim mērķim.

VIS izveidošanai var būt pozitīva ietekme uz citām likumīgām valsts interesēm, bet tas nemaina VIS mērķi. Sistēmas ierobežotam mērķim ir būtiska nozīme, nosakot likumīgo saturu un sistēmas izmantojumu, un tādēļ arī — piešķirot dalībvalstu iestādēm tiesības piekļūt VIS (vai daļai datu) to likumīgu valsts interešu dēļ.

Turklāt ar priekšlikumu ievieš biometrijas datu izmantošanu VIS. EDAU atzīst biometrijas datu izmantošanas priekšrocības, tomēr uzsver tādu datu izmantošanas lielo ietekmi, un ierosina ieviest stingrākus aizsardzības mehānismus biometrijas datu izmantošanai.

Šis priekšlikums jāinterpretē, ņemot vērā šos galvenos apsvērumus. Jāņem vērā, ka pašreizējo atzinumu vajadzētu minēt regulas preambulā pirms apsvērumiem ("ņemot vērā … atzinumu").

([1]) Šajā sakarā ir lietderīgi atsaukties uz Tiesas spriedumu par *Österreichischer Rundfunk* (Austrijas radio) un citiem (Apvienotās lietas C-465/00, C-138/01 un C-139/01, 2003. gada 20. maija spriedums, Tiesas plēnums (2003) ECR I-4989). Tiesa aplūkoja Austrijas tiesību aktus par algu maksājumu pārskaitīšanas detaļām Austrijas Revīzijas palātas valsts sektora darbiniekiem un to publicēšanu. Tiesa spriedumā ir noteikti vairāki kritēriji, pamatojoties uz Eiropas Cilvēktiesību konvencijas 8. pantu, ko vajadzētu izmantot, piemērojot Direktīvu 95/46/EK, ciktāl šī direktīva pieļauj konkrētus ierobežojumus attiecībā uz tiesībām uz privāto dzīvi.

([2]) Tā ir neatkarīga konsultatīva grupa, kurā ietilpst dalībvalstu datu aizsardzības iestādes, EDAU un Komisija; tā izveidota ar Direktīvu 95/46 EK.

3.2. **Mērķis**

VIS mērķis ir ļoti būtisks, gan no ECK 8. panta aspekta, gan no vispārējas datu aizsardzības sistēmas viedokļa. Saskaņā ar Direktīvas 95/46/EK 6. pantu, personas datiem jābūt "vāktiem konkrētiem, precīzi formulētiem un likumīgiem nolūkiem, un tos nedrīkst tālāk apstrādāt ar šiem nolūkiem nesavienojamā veidā". Tikai skaidra mērķu definēšana ļaus veikt pareizu personas datu apstrādes samērīguma un atbilstības novērtēšanu, kas ir būtiski datu būtības (tostarp biometrijas datu) un paredzēto apstrādes operāciju apjoma dēļ.

VIS mērķis ir skaidri noteikts priekšlikuma 1. panta 2. punktā.

> "VIS uzlabo kopējās vīzu politikas administrēšanu, konsulāro sadarbību un konsultācijas starp centrālajām konsulārajām iestādēm, atvieglinot datu apmaiņu starp dalībvalstīm saistībā ar pieteikumiem un ar tiem saistītajiem lēmumiem".

Tādēļ ir vajadzīgi visi VIS elementi un samērīgi instrumenti, lai sasniegtu politikas mērķi kopējas vīzu politikas interesēs.

Priekšlikuma 1. panta 2. punktā uzskaitīti šādi vīzu politikas pilnīgošanas papildu ieguvumi:

a) novērst iekšējas drošības apdraudējumus,

c) atvieglot cīņu pret viltojumiem,

d) atvieglot pārbaudes ārējo robežu kontrolpunktos.

EDAU uzskata šos elementus par piemēriem, kas liecina par VIS izveidošanas un pilnīgotas kopējās vīzu politikas pozitīvu iznākumu, bet neuzskata tos par neatkarīgiem mērķiem.

Tātad šajā stadijā rodas divi šādi secinājumi:

— EDAU apzinās, ka tiesībaizsardzības iestāde ir ieinteresētas, lai tām piešķirtu piekļuvi VIS; Padomes secinājumi par to ir pieņemti 2005. gada 7. martā. tā kā VIS mērķis ir uzlabot kopējo vīzu politiku, vajadzētu ņemt vērā, ka regulāra tiesībaizsardzības iestāžu piekļuve VIS nesaskanētu ar šo mērķi. ja saskaņā ar Direktīvas 65/46/EK 13. punktu šādu piekļuvi varētu sniegt *ad hoc*, īpašos apstākļos un saskaņā ar attiecīgiem drošības mehānismiem, sistemātisku piekļuvi VIS nedrīkst atļaut.

  Vispārinot, ir būtiski veikt samērīguma un vajadzīguma novērtējumu, ja nākotnē pieņem lēmumus par to, vai ļaut dažām citām iestādēm piekļūt VIS. Uzdevumiem, kuru risināšanai piešķir piekļuvi, ir jāatbilst VIS mērķiem.

— a) punktā skaidri minētā "draudu novēršana dalībvalstu iekšējai drošībai" nav izdevusies. VIS galvenie ieguvumi būs krāpniecības un vīzu pārdošanas novēršana (cīņa pret krāpniecību ir galvenais iemesls, lai sistēmā iekļautu biometrijas datus) ([1]). Drošības draudu novēršanu tādēļ vajadzētu uztvert kā "sekundāru", tomēr ļoti vēlamu ieguvumu.

  EDAU iesaka 1. panta 2. punktā "mērķa" atšķirību no "ieguvumiem" skaidrot labāk, piemēram:

  > "VIS mērķis ir uzlabot kopējās vīzu politikas administrēšanu, konsulāro sadarbību un centrālo konsulāro iestāžu konsultācijas, dalībvalstu starpā atvieglot datu apmaiņu saistībā ar pieteikumiem un ar tiem saistītiem lēmumiem. Tādējādi tā dos ieguldījumu arī ...."

([1]) Izvērstajā efektivitātes ekspertīzē ir skaidri pateikts (6. lpp. §2. 7).: *"neefektivitāte, apkarojot vīzu pārdošanu, krāpšanu un veicot pārbaudes, arī rada neefektivitāti saistībā ar dalībvalstu iekšējo drošību"*. Tas nozīmē, ka draudus drošībai daļēji rada neefektīva vīzu politika. Pirmais, kas šajā sakarā ir jādara, ir jāuzlabo vīzu politika, galvenokārt, apkarojot krāpniecību un veicot labākas pārbaudes. Uzlabojumus drošības jomā var panākt, uzlabojot vīzu politiku.

Vēl šajā sakarā ir vērts pieminēt to, ka "Pamatnostādnēs kopējas vīzi datu apmaiņas sistēmas iesviešanai", ko 2002. gada 13. jūnijā [1] pieņēma Tieslietu un iekšlietu Padome, iekšējās drošības draudu novēršana ierindota saraksta pēdējā vietā. Tas arī būtu iespējams un vairāk atbilstu VIS mērķim.

3.3. **Datu kvalitāte**

Saskaņā ar Direktīvas 95/46/EK 6. pantu personas datiem jābūt "adekvātiem, attiecīgiem un ne pārmērīgā apjomā attiecībā uz nolūkiem, kādiem tie savākti un/vai tālāk apstrādāti". Tas attiecas uz VIS samērīgumu, kā arī uz datiem, kas jāvāc un jāglabā Vīzu informācijas sistēmā, un uz to turpmāku izmantošanu, kā arī uz papildu aizsardzības pasākumiem, ko piemērot šajā sakarā. Šie elementi ir vienādi būtiski priekšlikuma novērtēšanai, ņemot vērā ECK 8. pantu.

VIS izveidošana noteikti ir svarīga iejaukšanās tiesībās uz privāto dzīvi, kaut vai tās mērogu un apstrādājamo personas datu kategoriju dēļ. Tādēļ 29. pantā darbagrupa atzinumā Nr. 7/2004 vēlējās zināt, "kādi šīs parādības mērogu un nopietnības pētījumi būtu atklājuši pamatotus iemeslus valsts drošības vai sabiedriskās kārtības jomā, lai apstiprinātu tādu pieeju".

EDAU ir rūpīgi ņēmis vērā pierādījumus, kas doti Izvērstajā efektivitātes ekspertīzē. Lai arī pierādījumi nav gluži neapstrīdami, acīmredzot ir pietiekami daudz iemeslu, lai pamatotu VIS izveidošanu, lai uzlabotu kopējo vīzu politiku.

Šajā sakarā likumdevējai iestādei izveidotā VIS būtu jāizvērtē kā instruments, kas uzlabo nosacījumus vīzu izsniegšanai dalībvalstīs. Tāda sistēma pati par sevi varētu labi iederēties un apstiprināt brīvības, drošības un tiesiskuma telpas pakāpenisku izveidi, kā paredzēts EK līgumā.

Tomēr VIS izveidošanai un izmantošanai noteikti nevarētu būt tāds iespaids, ka personas datiem šajā jomā nevarētu nodrošināt augsta līmeņa aizsardzību. EDAU kā padomdevēja uzdevums ir pārbaudīt, ciktāl VIS ietekmēs pašreizējo attiecīgo datu subjektu datu aizsardzības līmeni.

Ņemot vērā šo informāciju, EDAU šajā atzinumā uzmanību veltīs šādiem jautājumiem:

— datu samērīgums un atbilstība, un to izmantošana (piem. datu kategorijas, katras attiecīgās iestādes piekļuve datiem, un glabāšanas laiks);

— sistēmas darbība (piem. pienākumi un drošība);

— datu subjektu tiesības (piem. informēšana, iespēja labot vai dzēst neprecīzus vai nebūtiskus datus);

— sistēmas uzraudzīšana un kontrole.

Priekšlikumā, izņemot punktus, par ko še turpmāk būs runāts, nav iemesla būtiskiem komentāriem par datu kategorijām, kas jāiekļauj Vīzu informācijas sistēmā, un to izmantošanu. Attiecīgie noteikumi ir rūpīgi sastādīti un šķiet, ka kopumā tie ir konsekventi un adekvāti.

[1] "Padomes Pamatlēmums (2002. gada 13. jūnijs) par terorisma apkarošanu (2002/475/JHA)", (OV) 22.6.2002. , Nr. L 164., 3. lpp.

3.4. **Biometrija**

3.4.1. *Biometrijas izmatošanas efekts*

Biometrijas izmantošana informâcijas sistçmâs nekad nav nesvarîga izvçle, îpaði, ja konkrçta sistçma attiecas uz tik lielu personu skaitu. Biometrija nav tikai vçl viena informâcijas tehnoloìija. Tâs neatsaucami maina saistîbu starp íermeni un identitâti, ar ko tâs cilvçka íermeòa îpaðîbas padara iespçjamas "nolasît ar ierîci", ko turpmâk var izmantot. *Pat, ja biometriskâs îpaðîbas nav acîm saredzamas, tâs vienmçr var nolasît un izmantot ar attiecîgâm iekârtâm, lai kur persona ietu.*

Tomēr noderīgus biometrijas datus var izmantot konkrētiem mērķiem, to plašam izmantojumam var būt liela ietekme uz sabiedrību, un par to vajadzētu rīkot plašas un atklātas sarunas. EDAU jāapgalvo, ka tâdas sarunas patieðâm nav notikuðas pirms priekðlikuma izstrâdâðanas. Ar to vçl vairâk tiek uzsvçrta vajadzîba pçc stingrâkiem droðîbas pasâkumiem biometrijas datu izmantoðanai un rûpîgai atspoguïoðanai un sarunâm likumdoðanas procesâ.

3.4.2. *Biometrijas îpaðâ bûtîba*

Kā jau uzsvērts vairākos 29. panta darbagrupas ([1]) atzinumos, biometrijas datu ieviešana un apstrāde identitātes noteikšanai saistītiem dokumentiem jāpapildina ar jo īpaši konsekventiem un nopietniem aizsardzības mehānismiem. Biometrijas dati patiešām ir ļoti slepeni dažu konkrētu īpašību dēļ.

Tiesa, ka biometrijas datus par attiecīgo personu gandrīz nav iespējams pazaudēt, atšķirībā no paroles vai atslēgas. Tādi dati nodrošina *kvazipilnīgu atšķirīgumu*, t.i., katrai personai ir unikālas biometriskas īpašības. Tās (īpašības) gandrīz nekad nemainās cilvēka mūža laikā, un tas nodrošina šo iezīmju *nemainīgumu*. Katram ir vieni un tie paši "fiziskie elementi", kas biometriju dara *universālu*.

Turklāt biometrijas datus atsaukt gandrīz nav iespējams: pirkstu vai seju ir grūti mainīt. Šī pozitīvā īpašība no vairākiem viedokļiem rada lielu negatīvu iespaidu *identitātes zādzības* gadījumā: ar nozagtu identitāti saistītu pirkstu nospiedumu un fotoattēla glabāšana datu bāzē var radīt nopietnas un ilgas problēmas identitātes patiesajam īpašniekam. Turklāt biometrijas dati būtībā *nav slepeni* un tie pat var *atstāt pēdas* (pirkstu nospiedumi, DNS), un tas ļauj vākt šos datus, *pašam saimniekam to neapzinoties*.

Šādu biometrijai raksturīgu varbūtību dēļ būs jāīsteno nozīmīgi aizsardzības mehānismi (jo īpaši attiecībā uz mērķa precizitātes principa ievērošanu, piekļuves ierobežošanu un drošības pasākumiem).

3.4.3. *Pirkstu nospiedumu tehnisko aspektu trûkums*

Galvenās biometrijas priekšrocības, kā iepriekš minēts (datu universālums, iezīmība, nemainība, izmantojamība), nekad nav absolūtas. Tas tieši ietekmē regulā plānotās biometrijas iesaistes un pārbaudes procedūru efektivitāti.

Ir aprēķināts, ka līdz 5 % cilvēku ([2]) nevar iekļaut šajos datos (jo viņiem nav nolasāmu pirkstu nospiedumu vai nav pirkstu nospiedumu nemaz). Priekšlikumam pievienotajā Izvērstajā efektivitātes ekspertīzē ir lēsts, ka 2007. gadā būs aptuveni 20 miljonu vīzu pieteikumu, un tas nozīmē, ka līdz 1 miljonam personu nevarēs ievērot "parastu" iekļaušanu, kam var būt nopietnas sekas attiecībā uz vīzu pieteikumiem un robežpārbaudēm.

([1]) Atzinums Nr. 7/2004 par biometrijas datu iekļaušanu uzturēšanās atļaujās un vīzās, ņemot vērā Eiropas informācijas sistēmu par vīzām (VIS) izveidošanu (Markt/11487/04/EN - WP 96) un darba dokumentu attiecībā uz biometriju (MARKT/10595/03/EN - WP 80).

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

Biometriska identifikācija pēc definīcijas ir arī statistisks process. Kļūda 0,5 % līdz 1 % apjomā ir pieļaujama ([1]), un tas nozīmē, ka pārbaudes sistēmām pie ārējām robežām būs Kļūdains atmešanas koeficients (NNR) 0,5 % un 1 % robežās. Koeficientu salīdzina ar robežvērtību, kas noteikta saskaņā ar kompetentās iestādes riska politiku (tā ir starpība starp to personu skaitu, kam ir nepamatoti atteikta vīza, un to personu skaitu, kam nematoti izsniegta vīza). Tādēļ pārspīlēts ir uzskats, ka šīs tehnoloģijas došot "precīzu datu subjekta identifikāciju", kā apgalvots regulas projekta 9. apsvērumā.

Saskaņā ar iespējamo pētījumu ([2]), ko pasūtījusi Eiropas Parlamenta *LIBE* komiteja, vajadzētu būt pieejamām *alternatīvām procedūrām* kā būtiskiem aizsardzības mehānismiem, ieviešot biometriju, jo visiem nav piekļuve šiem datiem, un tie nav pilnībā precīzi. Tādas procedūras vajadzētu ieviest un izmantot, lai respektētu cieņu pret personām, kam nav bijusi iespēja veiksmīgi piedalīties datu iekļaušanas procesā, un lai izvairītos no tā, ka tām uzveļ sistēmas nepilnību nastu ([3]).

EDAU tādēļ iesaka izstrādāt un priekšlikumā ietvert alternatīvās procedūras. Šīm procedūrām nevajadzētu mazināt nedz vīzu politikā paredzēto drošības līmeni, nedz atstumt situācijā personas ar nenolasāmiem pirkstu nospiedumiem.

3.5. **Īpašas datu kategorijas**

Uzmanība īpaši jāpievērš dažu datu kategorijām (papildu biometrijas datiem): datiem par pamatojumu vīzu noraidīšanai (3.5.1.) un datiem, kas attiecas uz citiem grupas locekļiem (3.5.2.).

3.5.1. *Pamatojums vīzu atteikumiem*

Ierosinātā dokumenta 10. panta 2. punkts paredz apstrādāt datus, kas attiecas uz atteikuma pamatojumu, pieņemot lēmumu atteikt vīzu. Atteikuma pamatojumi ir pilnībā standartizēti.

— Pirmie divi, a) un b) apakšpunktā ietvertie pamatojumi ir visnotaļ administratīvi: tas, ka nav iesniegts derīgs ceļojuma dokuments vai derīgi dokumenti, kas pierāda paredzētās uzturēšanās mērķi un nosacījumus.

— c) apakšpunktā minēts "brīdinājums pieteikuma iesniedzējam atteikt ieceļošanu", kas nozīmē, ka dati ir atrasti ŠIS datu bāzē.

— Visbeidzot, d) apakšpunktā kā iemesls atteikt vīzu ir minēts tas, ka pieteikuma iesniedzējs "apdraud kādas dalībvalsts sabiedrisko kārtību, iekšējo drošību, sabiedrības veselību vai starptautiskās attiecības".

([1])

Biometrija	Seja	Pirksts	Varavīksne
FTE % Nav iekļauts	nav datu	4	7
FNMR % noraidījuma koeficients	4	2. 5	6
FMR1 % pārbaude atbilst kļūdas koeficientam	10	<0,01	<0,001
FMR2 % identifikācijas kļūdas koeficients dB lielāks par > 1 m	40	0. 1	NAV DATU
FMR3 % pārbaude atbilst kļūdas koeficientam dB izmēram=500	12	<1	NAV DATU

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

([2]) *Biometrics at the frontiers: assessing the impact on Society*, February 2005, Institute for Prospective Technological Studies, DG Joint Research Centre, EC.

([3]) Progresa ziņojums par 108. Konvencijas principu piemērošanu biometrijas datu vākšanai un apstrādei, Eiropadome, 2005. gads., 11. lpp.

Visi atteikuma iemesli jāpiemēro ļoti piesardzīgi, jo atteikums var radīt nopietnas sekas attiecīgai personai. Turklāt daži iemesli, kas ietverti apakšpunktos c) un d), liks apstrādāt "slepenus datus" Direktīvas 95/46/EK 8. panta nozīmē.

Eiropas datu aizsardzības uzraudzītājs konkrēti vēlas pievērst uzmanību nosacījumam, kas saistīts ar sabiedrības veselības aizsardzību, jo tas šķiet nekonkrēts, un prasa apstrādāt ļoti slepenu informāciju. Saskaņā ar ierosinātajam dokumentam pievienoto komentāru par pantiem, atsauce uz sabiedrības veselībai radītu apdraudējumu pamatojas uz priekšlikumu Padomes regulai, ar ko izveido Kopienas Kodeksu par noteikumiem, kas regulē personu pārvietošanos pāri robežām (COM (2004)391 galīgā versija).

Eiropas datu aizsardzības uzraudzītājs apzinās, ka Kopienas tiesību aktos par personu brīvu pārvietošanos ir plaši lietots kritērijs "sabiedrības veselības aizsardzība", un to piemēro ļoti stingri, kā liecina Eiropas Parlamenta un Padomes 2004. gada 29. aprīļa Direktīva 2004/38/EK par Eiropas Savienības pilsoņu un viņu ģimenes locekļu tiesībām brīvi pārvietoties un pastāvīgi dzīvot dalībvalstu teritorijā. Šīs direktīvas 29. pantā ir uzskaitīti nosacījumi, ņemot vērā sabiedrības veselības apdraudējumu: "Vienīgās slimības, kas attaisno pārvietošanās brīvības ierobežošanas pasākumus, ir slimības, kas potenciāli var izraisīt epidēmijas, kā definēts attiecīgos Pasaules veselības aizsardzības organizācijas instrumentos, un infekcijas slimības vai lipīgas parazītu slimības, ja uz tām attiecas aizsardzības noteikumi, ko piemēro uzņēmējas dalībvalsts valstspiederīgiem."

— Tomēr jāņem vērā, ka iepriekš minētais priekšlikums pašlaik ir tikai priekšlikums, un nosacījuma — neradīt apdraudējumu sabiedrības veselībai — iekļaušana regulā par vīzu informācijas sistēmu ir atkarīga no Kopienas kodeksa pieņemšanas.

— Turklāt, ja šo ieceļošanas atteikuma pamatojumu pieņems, tas būtu jāinterpretē piesardzīgi. Patiesi, ierosinātais Kopienas kodekss savukārt balstās uz nupat pieminēto Direktīvu 2004/58/EK.

Eiropas datu aizsardzības uzraudzītājs tālab iesaka ierosinātajā dokumentā iekļaut atsauci uz Direktīvas 2004/58/EK 29. pantu, lai nodrošinātos, ka "sabiedrības veselības apdraudējumu" saprot saskaņā ar šo pantu. Ņemot vērā datu slepenību, noteikti tie būtu jāapstrādā tikai tad, ja pastāv patiess, tūlītējs un pietiekami nopietns sabiedrības veselības apdraudējums.

3.5.2. *Dati par citiem grupas locekļiem*

2. panta 7. punktā "grupas dalībnieki" ir definēti kā citi "pieteikuma iesniedzēji, ar ko pieteikuma iesniedzējs ceļo kopā, arī viņa laulāto draugu un bērnus, kas pavada pieteikuma iesniedzēju". Komentārā par pantiem ir minēts, ka 2. pantā ierosinātā dokumenta dotās definīcijas attiecas uz Līgumu vai Šengenas *acquis* vīzu politikas jautājumos, izņemot dažus terminus, arī "grupas dalībnieki", kas ir definēts īpaši šajā regulā. Tātad var uzskatīt, ka šī definīcija neattiecas uz "grupas vīzu" definīciju, kas dota Kopējo konsulāro instrukciju 2. panta 1. punkta 4. apakšpunktā. Komentārā par pantiem ir minēti "pieteikuma iesniedzēji, kas grupā ceļo kopā ar citiem pieteikuma iesniedzējiem, piem., saskaņā ar nolīgumu par apstiprināta galamērķa statusu vai kopā ar ģimenes locekļiem".

Eiropas datu aizsardzības uzraudzītājs uzsver, ka regulā būtu jādod precīza un pietiekami plaša "grupas locekļu" definīcija. Tā kā šajā ierosinātajā dokumentā trūkst precīzu atsauču uz Līgumu vai Šengenas *acquis*, Eiropas datu aizsardzības uzraudzītājam jāatzīst, ka definīcija ir pārāk aptuvena. Saskaņā ar pašreizējo formulējumu pie "grupas dalībniekiem" var piederēt kolēģi, citi tās pašas ceļojumu aģentūras klienti, kas piedalās organizētā ceļojumā, utt.. Sekas, ko tas var izraisīt, tiešām ir ļoti nopietnas:

saskaņā ar regulas projekta 5. pantu pieteikuma iesniedzēja pieteikuma lietu saistīs ar citu grupas locekļu pieteikuma lietām.

3.6. **Datu glabāšana**

Regulas projekta 20. pants visām pieteikuma lietām paredz piecu gadu glabāšanas laiku. Kopienas likumdevējiem ir dota politiska izvēle — nolikt loģiski pieņemamu termiņu.

Nekas neliecina — jo īpaši, ņemot vērā komentārā par pantiem minētos iemeslus — ka šajā projektā izdarītā politiskā izvēle būtu neloģiska vai tai būtu nepieņemamas sekas — ar nosacījumu, ka darbojas visi vajadzīgie korekcijas mehānismi. Tas nozīmē, ka ir jānodrošina datu labošana vai dzēšana, ja dati vairs neatbilst patiesībai, un, jo īpaši, ja kāda persona ir ieguvusi kādas dalībvalsts valstspiederību vai statusu, kas neprasa viņu iekļaut sistēmā.

Turklāt, ja dati vēl ir sistēmā, tie nekādi neskar jaunu lēmumu. Dažiem atteikuma pamatojumiem (jo īpaši — brīdinājumiem, lai pieteikuma iesniedzējam atteiktu ieceļošanu sakarā ar sabiedrības veselības apdraudējumu) ir laika ziņā ierobežots darbības laiks. Tam, ka reiz tie ir bijuši pamatoti iemesli atteikt ieceļošanu, nevajadzētu ietekmēt jaunu lēmumu. Katram jaunam vīzas pieteikumam stāvoklis ir jāvērtē pilnīgi no jauna, un attiecīgās regulas vietās tas jāpasaka skaidri.

3.7. **Pieeja datiem un to izmantojums**

3.7.1. *Provizoriskas atziņas*

Eiropas datu aizsardzības uzraudzītājs atzīst, ka daudz darba noteikti ir ieguldīts vīzu informācijas sistēmas pieejas un izmantojuma sistēmā. Katrai iestādei ir pieejami citi dati citiem mērķiem. Tā ir pareiza pieeja, ko Eiropas datu aizsardzības uzraudzītājs var tikai atbalstīt. Šīs atziņas tiecas šo pieeju piemērot pēc iespējas pilnīgi.

3.7.2. *Vīzu pārbaudes ārējo robežu kontrolpunktos un dalībvalstu teritorijā*

Par vīzu pārbaudēm pie ārējām robežām regulas projekta 16. pantā ir skaidri pausti divi precīzi uzdevumi:

— "pārbaudīt personas identitāti", kas saskaņā ar definīciju nozīmē salīdzināt "viens pret vienu";

— "pārbaudīt vīzas īstumu". Kā ierosināts Starptautiskās Civilās aviācijas organizācijas (*ICAO*) standartos, vīzas mikroshēmā varētu būt iestrādāta publisku un privātu kodu sistēma (*PKI*) (*public/ private key system*), lai nodrošinātu apstiprināšanu.

Šos abus mērķus var pareizi sasniegt tikai tad, ja aizsargātai mikroshēmai var piekļūt tikai kompetentas iestādes, kas pārbauda vīzas. Tādējādi pieeja centrālai vīzu informācijas sistēmas datu bāzei šajā konkrētā gadījumā nepavisam nebūtu vajadzīga. Tāda iespēja liktu vairākām iestādēm saistīties ar vīzu informācijas sistēmu, un tas var palielināt iespējamību, ka datus lietos nepareizi. Tas arī būtu dārgāks variants, jo tādējādi droša un kontrolēta piekļuve vīzu informācijas sistēmai kļūtu plašāka, un reizē palielinātos vajadzība pēc konkrētām mācībām, kas saistītas ar piekļuvi tai.

Turklāt pastāv šaubas par to, cik pareiza ir pieeja datiem, kas paredzēta 16. panta otrā punktā. Patiesi, 2. punkta a) apakšpunktā ir teikts, ja šķiet, ka pēc pirmā prasījuma dati par pieteikuma iesniedzēju ir reģistrēti vīzu informācijas sistēmā (kā būtu jābūt), kompetenta iestāde var tos salīdzināt ar citiem datiem — arī, lai pārliecinātos par identitāti. Minētajos datos ir visa informācija, kas saistīta ar pieteikumu, fotoattēli, pirkstu nospiedumi, kā arī par visām agrāk izdotām, anulētām, atsauktām vai paildzinātām vīzām.

Ja identitātes pārbaude ir sekmīga, nepavisam nav skaidrs, kam gan vajadzīgi pārējie dati. Patiesībā tie būtu jādara pieejami — ar stingriem nosacījumiem — tikai tad, ja pārbaudes procedūras nav bijušas sekmīgas. Tādā gadījumā 16. panta 2. punktā minētos datus attiecīgi varētu izmantot alternatīvā procedūrā, lai palīdzētu pārliecināties par personas identitāti. Tātad tie nebūtu pieejami katram robežpārbaudes personāla loceklim, bet tikai izmeklētiem ierēdņiem, kas atbild par sarežģītu gadījumu risināšanu.

Visbeidzot, to iestāžu definīcijai, kurām ir dota piekļuve, būtu jābūt precīzākai. Konkrēti, nav skaidrs, kas ir "iestādes, kas kompetentas pārbaudīt vīzas dalībvalsts teritorijā". Eiropas datu aizsardzības uzraudzītājs pieņem, ka tās ir kompetentas iestādes, kas pārbauda vīzas, un 16. pants būtu jāgroza šajā ziņā.

3.7.3. *Datu izmantojums nelegālu imigrantu identifikācijai un atpakaļsūtīšanai, kā arī patvēruma procedūrās*

17., 18. un 19. pantā aprakstītajos gadījumos (nelegālu imigrantu atpakaļsūtīšana un patvēruma procedūras) vīzu informācijas sistēmu izmanto identifikācijai. Pie datiem, ko var izmantot identifikācijai, pieder fotoattēli. Tomēr, ņemot vērā pašreizējo tehnoloģiju, kas lielās informācijas tehnoloģijas sistēmās attiecas uz automatizētu seju pazīšanu, fotoattēlus identifikācijai izmantot nevar (viens fotoattēls var attiekties uz daudziem cilvēkiem); tie nevar dotu droši ticamus rezultātus. Tātad tos nevar uzskatīt par datiem, kas noder identifikācijai.

Tālab Eiropas datu aizsardzības uzraudzītājs sirsnīgi iesaka "fotoattēlus" šo pantu pirmajās daļās svītrot, bet paturēt otrajās daļās (fotoattēlus var izmantot kā līdzekli, lai pārbaudītu identitāti, bet ne, lai identificētu personu lielās datu bāzēs.)

Cita iespēja būtu grozīt 36. pantu tādējādi, lai tehniskos aspektus, kas saistīti ar fotoattēlu apstrādi identifikācijai, ieviestu tikai tad, kad šī tehnoloģija būtu atzīta par uzticamu (droši vien pēc tehnikas komitejas ieteikuma).

3.7.4. *To iestāžu publiskošana, kurām ir dota piekļuve*

Regulas 4. pantā ir paredzēts, ka *Eiropas Savienības Oficiālajā Vēstnesī* publicē, kādām kompetentām iestādēm katra dalībvalsts uzticējusi pieeju vīzu informācijas sistēmai. Publikācijai būtu jānotiek regulāri (ik gadu), lai informētu par to, kā mainījies stāvoklis katrā valstī. Eiropas datu aizsardzības uzraudzītājs uzsver, ka publikācija ir svarīga kā neaizstājams kontroles līdzeklis tiklab Eiropas kā valstu vai vietējā līmenī.

3.8. **Kompetence**

Te jāatceras, ka vīzu informācijas sistēma izmantos centralizētu arhitektūru ar centrālu datu bāzi, kur glabāsies visa informācija par vīzām, un saskarnēm dalībvalstīs, lai kompetentās iestādes varētu piekļūt centrālai sistēmai. Saskaņā ar regulas projekta 14. un 15. apsvērumu Direktīva 95/46/EK attieksies uz personu datu apstrādi dalībvalstīs, piemērojot regulu, un Regula 45/2001 attieksies uz Komisijas darbībām, kas saistītas ar personas datu aizsardzību. Šajā sakarā apsvērumos ir minēts, ka projektā paredzēts vairākus punktus padarīt skaidrākus, *inter alia*, par atbildību datu lietojumā un datu aizsardzības kontroli.

Patiesībā šie punkti, šķiet, attiecas uz dažiem būtiski svarīgiem sīkumiem, kurus atmetot, Direktīvā 95/46/EK un Regulā 45/2001 paredzētie drošības mehānismi nedarbotos vai nebūtu pilnībā saderīgi ar projektu. Piemērojot attiecīgu valstu tiesību aktus saskaņā ar šo direktīvu, parasti pieņem, ka konkrētā dalībvalstī darbojas datu apstrādātājs, kas reģistrēts tajā (4. pants), bet regulas piemērojamība ir atkarīga no tā, kā Kopienas iestāde vai struktūra apstrādā personas datus, veicot darbības, kas visas vai kuru daļa ietilpst Kopienas tiesību aktu jomā (3. pants).

Saskaņā ar regulas projekta 23. panta 2. punktu "vīzu informācijas sistēma apstrādā datus dalībvalstu interesēs". Saskaņā ar 23. panta 3. punktu dalībvalstis izvēlas iestādi, ko uzskata par datu apstrādātāju saskaņā ar Direktīvas 95/46/EK 2. panta d) punktu. Šķiet, tas nozīmē, ka, saskaņā ar direktīvā izmantoto sistēmu Komisija būtu jāuzskata par apstrādātāju. Tas ir apstiprināts Pantu skaidrojumā ([1]).

Tāda izteiksme nepietiekami uzsver Komisijas ļoti svarīgo, patiesībā būtisko vietu tiklab sistēmas izstrādes fāzē kā tās normālā darbībā. Ir grūti Komisijas vietu precīzi saistīt ar datu kontroliera jeb apstrādātāja jēdzienu; tā ir vai nu apstrādātāja ar neparastām pilnvarām (citastarp — sistēmas plānošanā), vai apstrādātāja ar ierobežotām pilnvarām (jo datus ievada un izmanto dalībvalstis). Vīzu informācijas sistēmā Komisijai patiesībā ir *sui generis* vieta ([2]), un tas ir jāatzīst.

Svarīgā vieta būtu jāatzīst pilnīgā Komisijas uzdevumu aprakstā, nevis izmantojot izteiksmi, kas realitātei īsti neatbilst, jo ir pārāk nepilnīga, neko nemaina vīzu informācijas sistēmas darbībā, un tikai rada sajukumu. Tas ir svarīgi, lai konsekventi un efektīvi kontrolētu vīzu informācijas sistēmu (skat. arī 3.11. punktu). Tālab Eiropas datu aizsardzības uzraudzītājs iesaka svītrot 23. panta 2. punktu.

Eiropas datu aizsardzības uzraudzītājs vēlas uzsvērt, ka pilnīgs to Komisijas uzdevumu apraksts attiecībā uz vīzu informācijas sistēmu ir vēl jo svarīgāks, ja Komisija paredz vadības uzdevumus uzticēt citai struktūrai. Projektam pievienotajā "Fiche Financière" ir minēta iespēja nodot šos uzdevumus ārējo robežu aģentūrai. Tādā sakarā ir būtiski, lai Komisija neatstāj nekādu neskaidrību tās kompetenču ziņā, lai tās pilnvaru pārņēmējs zinātu, kādās robežās viņš var darboties.

3.9. **Drošība**

Optimālas vīzu informācijas sistēmas drošības uzturēšana un ievērošana ir priekšnoteikums, lai nodrošinātu vajadzīgo aizsardzību tās datu bāzē glabātiem personas datiem. Lai panāktu pietiekama līmeņa aizsardzību, ir jāievieš pareizi drošības mehānismi, lai novērstu iespējamus draudus, kas ir saistīti ar sistēmas infrastruktūru un iesaistītajām personām. Šo tematu tagad pārrunā dažādās projekta daļās, un tajā būtu jāveic daži uzlabojumi.

Priekšlikuma 25. un 26. pantā ir paredzēti dažādi datu drošības pasākumi un konkrēti norādīts, kāds to nepareizs lietojums būtu jānovērš. Šos noteikumus tomēr lietderīgi būtu papildināt ar pasākumiem, lai metodiski pārraudzītu jau minēto drošības pasākumu efektivitāti, un ziņotu par to. Eiropas datu aizsardzības uzraudzītājs konkrēti iesaka šiem pantiem pievienot noteikumus par metodisku drošības pasākumu (paš)auditu.

Tas ir saistīts ar projekta 40. pantu, kurā paredzēta pārraudzība un izvērtējums. Tam būtu jāattiecas gan uz tādiem aspektiem kā pakalpojumu darbības efektivitāti, izmaksu lietderīgumu un kvalitāti, gan arī uz juridisko prasību ievērošanu, jo īpaši datu aizsardzības jomā. Tāpēc Eiropas datu aizsardzības uzraudzītājs iesaka paplašināt 40. panta darbības jomu un attiecināt to arī uz apstrādes likumīguma pārraudzību un ziņojumiem par tās likumību.

Turklāt, papildinot 24. panta 4. punkta c) apakšpunktu vai 26. panta 2. punkta e) apakšpunktu, kas attiecas uz pienācīgi pilnvarotu personālu, kam ir dota pieeja datiem, būtu jāpiebilst, ka dalībvalstīm vajadzētu nodrošināt to, ka ir pieejami precīzi lietotāju profili (kas būtu jātur attiecīgu valstu kontroles iestāžu rīcībā pārbaudes vajadzībām). Dalībvalstīs līdztekus lietotāju profiliem ir jāsastāda un visu laiku jāatjaunina pilnīgs saraksts ar lietotāju identitātes datiem. Tas pats attiecas uz Komisiju: tālab 25. panta 2. punkta b) apakšpunkts būtu jāpapildina tāpat.

([1]) Skat. projekta 37. lpp. .

([2]) Kaut arī Direktīvā 95/46/EK un Regulā 45/2001 dotā definīcija paredz arī iespēju, ka ir vairāki datu apstrādātāji ar dažādiem pienākumiem.

Pēdējie drošības pasākumi ir pārraudzības un organizatoriski drošības mehānismi. Projekta 28. pants apraksta nosacījumus, kā glabāt visām datu apstrādes operāciju reģistru, un šo operāciju mērķi. Reģistra datus glabā ne tikai, lai pārraudzītu datu aizsardzību un garantētu datu drošību, bet arī regulāram VIS pašauditam. Pašaudita ziņojumi palīdzēs kontroles iestādēm efektīvi veikt pienākumus, kas spēs atklāt vājākos punktus un tiem pievērsties savā audita procedūrā.

3.10. **Datu subjektu tiesības**

3.10.1. *Datu subjektu informēšana*

Ārkārtīgi svarīgi ir informēt datu subjektu, lai nodrošinātu datu godprātīgu apstrādi. Informēšana ir neatņemams indivīda tiesību nodrošinājums. To nodrošinot, projekta 30. pantā tagad pamatvilcienos ir ievērots Direktīvas 95/46/EK 10. pants.

Šo pantu tomēr varētu uzlabot daži grozījumi, lai tas labāk iekļautos VIS sistēmā. Direktīvā patiešām ir paredzēts sniegt kādu informāciju, bet vajadzības gadījumā ļauj sniegt vairāk informācijas ([1]). Attiecīgi būtu jāgroza 30. pants, lai iekļautu šādus punktus:

— datu subjektus vajadzētu informēt arī par to, kāds glabāšanas laiks attiecas uz viņu datiem;

— 30. panta 1. punkta e) apakšpunkts attiecas uz "tiesībām piekļūt datiem [..], kā arī tiesībām šos datus labot"; precīzāk būtu minēt "tiesības piekļūt datiem, [..] kā arī tiesībām *lūgt* šos datus labot *vai dzēst*". Šajā sakarā datu subjekti būtu informēti par iespēju lūgt padomu vai palīdzību attiecīgām kontroles iestādēm.

— Visbeidzot, 30. panta 1. punkta a) apakšpunktā ir minēta informācija par datu apstrādātāja — un tā pārstāvja, ja tāds ir — identitāti. Tā kā datu apstrādātājs vienmēr darbojas Eiropas Savienības teritorijā, tāda iespēja nav jāparedz.

3.10.2. *Piekļuves, labošanas un dzēšanas tiesības*

31. panta 1. punkta pēdējā teikumā ir konstatēts, ka "pieeju datiem var piešķirt tikai dalībvalsts". Var pieņemt, ka tas nozīmē: pieeju datiem (vai atļauju tos darīt zināmus) nevar piešķirt Centrālā vienība, bet tikai kāda dalībvalsts. Eiropas datu aizsardzības uzraudzītājs iesaka skaidri paredzēt, ka jebkurā dalībvalstī var lūgt atļauju darīt zināmus datus.

Turklāt šī noteikuma izstrāde šķiet paredzam, ka pieeju nevar atteikt, un ka to ļaus bez atbildīgās dalībvalsts piekrišanas. Tas varētu izskaidrot, kāpēc attiecīgu valstu iestādēm jāsadarbojas, īstenojot 31. panta 2., 3. un 4. pantā, bet ne 31. panta 1. punktā minētās tiesības ([2]).

3.10.3. *Kontroles iestāžu sniegta palīdzība*

33. panta 2. punktā ir noteikts, ka attiecīgo valstu kontroles iestāžu pienākums sniegt palīdzību un padomus paliek spēkā visu tiesvedības laiku. Šīs rindkopas doma nav skaidra. Attiecīgo valstu kontroles iestādēm ir dažāda attieksme pret to pienākumiem tiesvedības laikā. Izklausās, ka tām tiesā jādarbojas kā prasījuma iesniedzēja padomdevējām, bet daudzās valstīs tas nav iespējams.

([1]) Tajā teikts, "*papildu informācija, (…) ciktāl minētā papildu informācija ir vajadzīga, ņemot vērā īpašos apstākļus, kādos datus ievāc, lai garantētu godprātīgu apstrādi attiecībā uz datu subjektu.*"

([2]) Attiecīgi 31. panta 3. punktu, kas attiecas uz attiecīgu valstu iestāžu sadarbību, īstenojot tiesības labot vai dzēst datus, šajā ziņā varētu grozīt, lai panāktu lielāku skaidrību: ja lūgums, "*kā minēts 31. panta 2. punktā*". 31. panta 1. punktā minētie lūgumi (pieeja) neparedz iestādēm sadarboties.

3.11. **Kontrole**

Projektā attiecīgo valstu kontroles iestādes un Eiropas datu aizsardzības uzraudzītājs dala uzraudzības pienākumus. Tas sader ar projektā izmantoto pieeju spēkā esošiem tiesību aktiem un pienākumiem, kas saistīti ar vīzu informācijas sistēmas darbību un izmantojumu, un ar vajadzību pēc efektīvas kontroles. Tālab Eiropas datu aizsardzības uzraudzītājs sveic šo pieeju, kas izmantota 34. un 35. pantā.

Attiecīgu valstu kontroles iestādes pārrauga, cik likumīgi dalībvalstis apstrādā personas datus, *arī, tos pārsūtot uz VIS un saņemot no tās*. Eiropas datu aizsardzības uzraudzītājs uzrauga Komisijas darbības *(…) arī to, lai personas datus likumīgi pārraidītu starp valstu saskarnēm un Centrālo vīzu informācijas sistēmu*. Tā var notikt pārklāšanās, jo gan kontroles iestāde attiecīgā valstī, gan Eiropas datu aizsardzības uzraudzītājs reizē atbild par to, lai personas datus likumīgi pārraidītu starp valstu saskarnēm un Centrālo vīzu informācijas sistēmu.

Eiropas datu aizsardzības uzraudzītājs tāpēc ierosina grozīt 34. pantu, lai kļūtu skaidrs, ka kontroles iestādes attiecīgās valstīs uzrauga to, cik likumīgi dalībvalstis apstrādā personas datus, ietverot to pārraidi no valstu saskarnēm uz vīzu informācijas sistēmu un atpakaļ.

Attiecībā uz VIS kontroli ir svarīgi uzsvērt, ka attiecīgo valstu un Eiropas datu aizsardzības uzraudzītāja veiktās kontroles darbības būtu mazliet jākoordinē, lai nodrošinātu pietiekamu konsekvenci un vispārēju efektivitāti. Patiesi, regula ir jāīsteno saskaņoti, un jāstrādā, lai rastu vienotu pieeju kopējām problēmām. Turklāt, tā kā ir runa par drošību, var piebilst, ka VIS drošības līmeni galu galā noteiks tās vājākā posma drošības līmenis. Šajā sakarā jāstrukturē un jāstiprina arī Eiropas datu aizsardzības uzraudzītāja sadarbība ar attiecīgo valstu iestādēm. 35. pantā tālab būtu jāietver nosacījums par to, ka Eiropas datu aizsardzības uzraudzītājs vismaz reizi gadā sasauc sanāksmi ar visu attiecīgo valstu kontroles iestādēm.

3.12. **Īstenošana**

Priekšlikuma 36. panta 2. punktā ir paredzēts: *"Pasākumus, kas vajadzīgi, lai tehniski īstenotu 1. punktā minētos tehniskos aspektus, paredz saskaņā ar 39. panta 2. punktā minēto procedūru."* 39. pantā ir minēta 2001. gada decembrī izveidota komiteja ([1]), kas palīdz Komisijai un kas ir izmantota vairākos instrumentos.

VIS tehnisko aspektu tehniska īstenošana (mijiedarbība ar kompetentām iestādēm un vienots vīzu formāts) datu aizsardzību iespaido vairākos, iespējams, būtiskos aspektos. Piemēram, izvēle — vīzā iegult mikroshēmu vai ne — ietekmēs to, kā izmantos centrālo datu bāzi, savukārt tas, kāda formāta standartu izmantos biometrijas datu apmaiņai, attīstīs vai ierobežos ar to saistīto datu aizsardzības politiku ([2]).

Tehnoloģiju izvēle pilnībā noteiks mērķtiecības un samērības principa pareizas īstenošanas nākotni, un tālab tā būtu jākontrolē. Tālab tehnoloģijas izvēlei, kas būtiski iespaido datu aizsardzību, būtu jānotiek, izmantojot regulu, un saskaņā ar koplēmumu procedūru. Tikai tad var sākt vajadzīgo politisko kontroli. Visos citos gadījumos, kas iespaido datu aizsardzību, Eiropas datu aizsardzības uzraudzītājam būtu jādod iespēja dot padomus šai komitejai, izdarot izvēli.

3.13. **Savstarpēja savietojamība**

Savstarpēja savietojamība ir būtiski svarīgs lielu informācijas tehnoloģijas sistēmu efektivitātes priekšnoteikums. Tas ļauj konsekventi mazināt kopējās izmaksas un izvairīties no dabiskas nesaskanīgu elementu redudances. Savstarpēja savietojamība var palīdzēt sasniegt kopīgu mērķi — kopēju vīzu politiku — īstenojot vienus un tos pašus procedūras standartus visiem elementiem, kas veido politiku. Turklāt būtiski svarīgi ir nošķirt divu līmeņu savstarpēju savietojamību:

— savstarpēja ES dalībvalstu savietojamība visnotaļ vēlama; patiesi, vīzu pieteikumiem, ko sūta vienas dalībvalsts iestādes, jābūt savietojamiem ar vīzu pieteikumiem, ko sūta visu citu dalībvalstu iestādes.

([1]) Padomes 2001. gada 6. decembra Regula Nr. 2424/2001 par otrās paaudzes Šengenas Informācijas sistēmas (ŠIS II) izveidošanu.

([2]) 2003. gada septembra priekšlikumā, ar ko groza Padomes regulu (EK)1683/95 (vienota vīzu forma) bija iekļauts līdzīgs pants.

— Savstarpēja tādu sistēmu savietojamība, kas izveidotas dažādiem mērķiem, vai ar trešo valstu sistēmām, ir krietni apšaubāmāka.

Viens no drošības mehānismiem, ko varētu izmantot, lai ierobežotu sistēmas izmantojuma mērķus un novērstu "funkciju izplūšanu", var būt dažādu tehnoloģijas standartu izmantojums. Turklāt būtu rūpīgi jādokumentē divu dažādu sistēmu mijiedarbība jebkādā formā. Savstarpējai savietojamībai nevajadzētu radīt tādu stāvokli, ka iestāde, kas nav tiesīga piekļūt konkrētiem datiem vai tos lietot, varētu iegūt tādu pieeju, izmantojot citu informācijas sistēmu.

Tādā sakarā Eiropas datu aizsardzības uzraudzītājs vēlētos atsaukties uz Padomes 2004. gada marta deklarāciju par terorisma apkarošanu, kurā Komisija ir aicināta nākt klajā ar priekšlikumiem par to, kā stiprināt informācijas sistēmu (ŠIS, VIS un *Eurodac*) savstarpēju savietojamību un sinerģijas.

Eiropas datu aizsardzības uzraudzītājs arī gribētu piesaukt pašreizējo diskusiju par to, kurai struktūrai nākotnē varētu uzticēt dažādu lielu sistēmu vadību (skat. arī šā atzinuma 3.8. punktu).

Eiropas datu aizsardzības uzraudzītājs grib atkārtoti uzsvērt, ka sistēmu savstarpēju savietojamību nevar īstenot, pārkāpjot mērķa precizitātes principu, un visi priekšlikumi šajā jomā būtu jāiesniedz viņam.

4. **SECINĀJUMI**

4.1. **Vispārēji jautājumi**

1. Eiropas datu aizsardzības uzraudzītājs atzīst, ka, lai turpinātu attīstīt kopēju vīzu politiku, ir vajadzīga efektīva apmaiņa ar attiecīgiem datiem. Viens mehānisms, kas var nodrošināt netraucētu informācijas plūsmu, ir vīzu informācijas sistēma. Eiropas datu aizsardzības uzraudzītājs ir rūpīgi ņēmis vērā izvērstajā efektivitātes novērtējumā ietvertos pierādījumus. Kaut arī pierādījumi nav gluži neapstrīdami, šķiet, ir pietiekami iemesli attaisnot vīzu informācijas sistēmas izveidi, lai uzlabotu kopējo vīzu politiku.

   Jaunajam instrumentam tomēr vajadzētu aprobežoties ar datu vākšanu un apmaiņu, ciktāl vākšana un apmaiņa ir vajadzīga, lai attīstītu kopējo vīzu politiku un ir samērīga ar šo mērķi.

2. Vīzu informācijas sistēmas izveidošana var pozitīvi ietekmēt citas likumīgas valsts intereses, bet tas nemaina VIS mērķi. Tādēļ visiem VIS elementiem ir jābūt vajadzīgiem un samērīgiem instrumentiem, ar ko sasniegt iepriekš minēto politikas mērķi. Turklāt:

   — regulāra tiesībaizsardzības iestāžu pieeja VIS nesaskanēs ar šo mērķi;

   — Eiropas datu aizsardzības uzraudzītājs iesaka 1. panta 2. punktā skaidrāk nošķirt "mērķi" no "ieguvumiem";

   — savstarpēju savietojamību ar citām sistēmām nevar īstenot, pārkāpjot mērķa precizitātes principu.

3. Eiropas datu aizsardzības uzraudzītājs atzīst biometrijas datu izmantojuma priekšrocības, bet uzsver, ka tādu datu izmantošana atstāj ārkārtīgi lielu ietekmi, un ierosina ieviest stingrākus aizsardzības mehānismus biometrijas datu izmantošanai. Turklāt pirkstu nospiedumu tehniskās nepilnības prasa, lai izstrādātu un priekšlikumā ietvertu alternatīvas procedūras.

4. Šis atzinums būtu jāmin regulas preambulā pirms apsvērumiem ("ņemot vērā … atzinumu").

4.2. **Citi jautājumi**

5. Par vīzas atteikuma iemesliem: dokumenta projektā būtu jāiekļauj atsauce uz Direktīvas 2004/58/EK 29. pantu, lai nodrošinātos, ka "sabiedrības veselības apdraudējumu" saprot saskaņā ar šo pantu.

6. Dokumenta projektā "datiem par citiem grupas locekļiem" ir īpaša nozīme: tālab būtu jādod precīza un pietiekami plaša "grupas locekļu" definīcija.

7. Nekas neliecina, ka šajā projektā izdarītā politiskā izvēle par datu glabāšanu būtu neloģiska vai tai būtu nepieņemamas sekas — ar nosacījumu, ka darbojas visi vajadzīgie korekcijas mehānismi.

   Turklāt dokumenta projektā skaidri jānorāda, ka ikkatram jaunam vīzas pieteikumam personas dati ir jāvērtē pilnīgi no jauna.

8. Par vīzu pārbaudēm pie ārējām robežām: dokumenta projekta 16. pants būtu jāgroza, jo pieeja centrālai vīzu informācijas sistēmas datu bāzei tādos gadījumos nepavisam nav vajadzīga. Pietiek ar to, ka aizsargātai mikroshēmai var piekļūt tikai kompetentas iestādes, kas pārbauda vīzas.

   Turklāt, ja identitātes pārbaude ir sekmīga, nepavisam nav skaidrs, kam gan vajadzīgi pārējie dati.

9. Par datu izmantojumu nelegālu imigrantu identifikācijai un atpakaļsūtīšanai, kā arī patvēruma procedūrās: "fotoattēlus" 17., 18. un 19. panta pirmajā daļā svītrot, bet paturēt otrajās daļās.

10. Par Komisijas un dalībvalstu atbildību: 23. panta 2. punkts būtu jāsvītro.

11. Projektam būtu jāpievieno noteikumi par metodisku drošības pasākumu (paš)auditu. Projekta 40. panta darbības joma ir jāpaplašina un jāattiecina arī uz apstrādes likumīguma pārraudzību un ziņojumiem par tās likumību. Turklāt:

   — dalībvalstīs ir jāsastāda pilnīgs saraksts un visu laiku jāatjaunina ar lietotāju identitātes datiem. Tas pats attiecas uz Komisiju: Tālab 25. panta 2. punkta b) apakšpunkts būtu jāpapildina tāpat.

   — Projekta 28. pants apraksta nosacījumus, kā glabāt visu datu apstrādes operāciju reģistru, un šo operāciju mērķi. Reģistra datus glabā ne tikai, lai pārraudzītu datu aizsardzību un garantētu datu drošību, bet arī regulāram VIS pašauditam.

12. Par datu subjektu tiesībām:

   — 30. pants būtu jāgroza, lai nodrošinātu, ka datu subjektus vajadzētu informēt arī par to, kāds glabāšanas laiks attiecas uz viņu datiem;

   — 30. panta 1. punkta e) apakšpunktā precīzāk būtu minēt "tiesības piekļūt datiem, kā arī tiesībām lūgt šos datus labot vai dzēst".

   — 30. panta 1. punktā skaidri jāparedz, ka jebkurā dalībvalstī var lūgt atļauju darīt zināmus datus.

13. Par kontroli:

— dokumenta projekta 34. panta būtu jāgroza, lai kļūtu skaidrs, ka kontroles iestādes attiecīgās valstīs uzrauga to, cik likumīgi dalībvalstis apstrādā personas datus, ietverot to pārraidi no valstu saskarnēm uz vīzu informācijas sistēmu un atpakaļ.

— 35. pantā tālab būtu jāietver nosacījums par to, ka Eiropas datu aizsardzības uzraudzītājs vismaz reizi gadā sasauc sanāksmi ar visu attiecīgo valstu kontroles iestādēm.

14. Par īstenošanu:

— tehnoloģijas izvēlei, kas būtiski iespaido datu aizsardzību, būtu jānotiek, izmantojot regulu, un saskaņā ar koplēmumu procedūru.

— citos gadījumos Eiropas datu aizsardzības uzraudzītājam būtu jādod iespēja dot padomus dokumenta projektā paredzētajai komitejai, izdarot izvēli.

Briselē, 2005. gada 23. martā

Peter HUSTINX

Eiropas Datu aizsardzības uzraudzītājs