EIROPAS DATU AIZSARDZĪBAS UZRAUDZĪTĀJS

Eiropas datu aizsardzības uzraudzītāja atzinums sakarā ar ierosināto Padomes lēmumu par to, kā par iekšējo drošību atbildīgām dalībvalstu iestādēm un Eiropolam informācijas nolūkos piekļūt Vīzu informācijas sistēmai (*Visa Information System — VIS*), lai novērstu, atklātu un izmeklētu terora aktus un citus smagus noziedzīgus nodarījumus (COM (2005) 600 galīgais variants)

(2006/C 97/03)

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 personu 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 2005. gada 29. novembrī saņemto Komisijas lūgumu dot atzinumu saskaņā ar Regulas (EK) Nr. 45/2001 28. panta 2. punktu,

IR PIEŅĒMIS ŠO ATZINUMU.

1. IEVADS

1.1. Provizoriska piezīme

Ierosināto Padomes lēmumu par to, kā par iekšējo drošību atbildīgām dalībvalstu iestādēm un Eiropolam informācijas nolūkos piekļūt Vīzu informācijas sistēmai (*Visa Information System — VIS*), lai novērstu, atklātu un izmeklētu terora aktus un citus smagus noziedzīgus nodarījumus (še turpmāk "priekšlikums") Komisija 2005. gada 24. novembra vēstulē nosūtījusi Eiropas Datu aizsardzības uzraudzītājam (EDAU). EDAU uztver šo vēstuli kā lūgumu konsultēt Kopienas iestādes un struktūras, kā paredzēts Regulas (EK) Nr 45/2001 28. panta 2. punktā. EDAU uzskata, ka šis atzinums būtu jāmin lēmuma preambulā.

EDAU uzskata, ka ir ļoti svarīgi nākt klajā ar atzinumu šajā kutelīgajā jautājumā, jo šis priekšlikums tieši izriet no tā, ka izveidota Vīzu informācijas sistēma, kas būs viņa kontrolē, un par ko viņš ir nācis klajā ar atzinumu 2005. gada 23. martā ([1]). Minētajā atzinumā jau bija paredzēta hipotētiska tiesībaizsardzības iestāžu piekļuve (skat. še turpmāk); radīt jaunas piekļuves tiesības Vīzu informācijas sistēmai no datu aizsardzības viedokļa būtiski ietekmē šo sistēmu. Tālab atzinums par šo priekšlikumu ir dabisks pirmā atzinuma izvērsums.

1.2. Priekšlikuma nozīme

a) *Konteksts:*

Šis priekšlikums ir svarīgs ne tikai tā īpašību dēļ, bet arī tāpēc, ka tas saskan ar vispārēju tendenci dot tiesībaizsardzības iestādēm piekļuvi vairākām lielām informācijas un identifikācijas sistēmām. Tas citastarp ir minēts Komisijas 2005. gada 24. novembra paziņojumā par Eiropas datu bāzu lielāku efektivitāti, mijdarbību un sinerģijām tieslietu un iekšlietu jomā ([2]), jo īpaši 4.6. punktā: "*Attiecībā uz mērķi apkarot terorismu un noziedzību, Padome kā trūkumu nu apzina to, ka iekšējās drošības iestādēm nav dota piekļuve VIS datiem. To pašu varētu teikt arī par ŠIS II imigrācijas un* EURODAC *datiem*".

Tālab šo priekšlikumu var uzskatīt par priekšteci līdzīgiem juridiskiem instrumentiem, ko attīsta citu datu bāzu sakarā, un ir būtiski svarīgi jau sākumā apzināt gadījumus, kad piekļuve var būt pieļaujama.

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

([2]) COM(2005) 597 galīgā redakcija

b) *Paplašinātas piekļuves iespaids uz VIS*

EDAU noteikti apzinās vajadzību tiesībaizsardzības iestādēm izmantot iespējami labākos instrumentus, identificējot terora aktu vai citu nopietnu noziegumu veicējus. Viņš apzinās arī to, ka dažos apstākļos VIS dati var izrādīties būtiski svarīgs informācijas avots minētajām iestādēm.

Tomēr, dot tiesībaizsardzības aģentūrām piekļuvi pirmā pīlāra datu bāzēm ir ļoti nopietns pasākums, lai kā arī to attaisnotu terorisma apkarošana. Jāatceras, ka VIS ir informācijas sistēma, kas izstrādāta, lai piemērotu Eiropas vīzu politiku, nevis kā tiesībaizsardzības instruments. Neierobežota piekļuve patiesi būtu nopietns sākotnēji iecerētā lietojuma precizitātes principa pārkāpums. Tas radītu nesamērīgu iejaukšanos ceļotāju privātā dzīvē, kuri ir piekrituši, ka viņu datus apstrādā, lai saņemtu vīzu, un paredz, ka viņu datus vāks, izmantos kā informāciju un pārraidīs vienīgi tādos nolūkos.

Tā kā informācijas sistēmas veido konkrētiem mērķiem, ar tiem piemērotiem aizsardzības mehānismiem, drošības pasākumiem un piekļuves nosacījumiem, nodrošināt regulāru piekļuvi lietojumam, kas ir citāds nekā sākotnēji iecerētais, ne tikai nozīmētu pārkāpt sākotnēji iecerētā lietojuma precizitātes principu, bet varētu arī padarīt iepriekš minētos elementus par nepiemērotiem vai nepietiekamiem.

Saskaņā ar tādu pašu domu gaitu, tik nozīmīgas pārmaiņas sistēmā varētu padarīt nederīgus ekspertīzes rezultātus (kurā sistēma ir analizēta tikai no sākotnēji iecerētā lietojuma viedokļa). Tas pats attiecas uz datu aizsardzības iestāžu atzinumiem. Varētu apgalvot, ka jaunais priekšlikums maina viņu veiktās atbilsmes analīzes premises.

c) *Strikti ierobežota piekļuve*

Ņemot vērā še iepriekš izteiktās piebildes, EDAU vēlētos uzsvērt, ka tiesībaizsardzības iestādēm piekļuvi VIS var dot tikai konkrētos apstākļos, analizējot katru gadījumu atsevišķi, un tā jāpapildina ar stingriem drošības pasākumiem. Citiem vārdiem sakot, tiesībaizsardzības iestāžu piekļuve informatīvos nolūkos ir jāierobežo ar konkrētiem gadījumiem, izmantojot pietiekamus tehniskus un juridiskus līdzekļus.

EDAU to jau ir uzsvēris atzinumā par VIS: *"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 ir radīta, lai uzlabotu kopējo vīzu politiku, būtu jāņem vērā, ka regulāra tiesībaizsardzības iestāžu piekļuve VIS nesaskanētu ar šo mērķi. Kaut arī saskaņā ar Direktīvas 95/46/EK 13. pantu īpašos apstākļos un saskaņā ar attiecīgiem drošības mehānismiem varētu nodrošināt* ad hoc *piekļuvi, regulāra piekļuve VIS nav pieļaujama."*

Noslēgumā galvenās prasības varētu rezumēt šādi:

— regulāru piekļuvi nevajadzētu piešķirt; ar lēmumu ir jānodrošina, lai trešā pīlāra iestādes vienmēr katrā konkrētā gadījumā izskatītu vajadzību pēc piekļuves un tās samērību. Šādā sakarā ārkārtīgi svarīgi ir precīzi formulēt juridisko instrumentu, lai neatstātu iespēju plašai interpretācijai, kas savukārt izraisītu regulāru piekļuvi.

— Gadījumos, kad piekļuvi piešķir, ir jāparedz attiecīgi drošības mehānismi un nosacījumi, arī pilnvērtīgs datu aizsardzības režīms datu lietojumam attiecīgā valstī, ņemot vērā to, cik kutelīga ir tāda piekļuve.

1.3 **Sākuma piebildes**

EDAU atzīst, ka ierosinātajā instrumentā datu aizsardzībai ir pievērsta liela uzmanība, galvenokārt tādējādi, ka piekļuve ir ierobežota ar konkrētiem gadījumiem, un tikai sakarā ar smagu noziegumu apkarošanu ([1]).

Citu pozitīvu aspektu starpā EDAU arī vēlētos konkrēti pieminēt:

— aprobežošanos ar dažu formu noziegumiem, kas minēti Eiropola konvencijā;

— pienākumu dalībvalstīm sastādīt to iestāžu sarakstu, kurām ir dota piekļuve, un publiskot šos sarakstus;

— to, ka katrai dalībvalstij (un specializētai Eiropola vienībai) ir centrāls piekļuves punkts, kas ļauj labāk filtrēt piekļuves lūgumus, kā arī labāk veikt kontroli;

— stingrus noteikumus par datu tālāku pārraidi saskaņā ar priekšlikuma 8. panta 5. punktu;

— pienākumu dalībvalstīm un Eiropolam glabāt reģistra datus par personām, kas atbild par piekļuvi datiem informācijas nolūkos.

2. **PRIEKŠLIKUMA ANALĪZE**

2.1. **Provizoriska piezīme**

Lai iestādēm piešķirtu piekļuvi attiecībā uz trešā pīlāra bāzes, galvenā pirmā pīlāra VIS priekšlikumā būtu jāparedz pārejas klauzula, kas faktiski noteiktu iespējamo saturu trešā pīlāra juridiskiem instrumentiem, piemēram, šim priekšlikumam. Laikā, kad EDAU nāca klajā ar atzinumu par VIS, tāda pārejas klauzula vēl nebija ieviesta, un EDAU nevarēja izteikt piebildes par to. Tālab visas šeit izteiktās piebildes ir izteiktas ar pienācīgu atrunu par pārejas klauzulas saturu.

([1]) Tas arī saskan ar Padomes 2005. gada marta un jūlija secinājumiem, kuros lūgts, lai par iekšējo drošību atbildīgām iestādēm piešķirtu piekļuvi VIS, *"stingri ievērojot noteikumus, kas regulē personas datu aizsardzību"*.

2.2 **Piekļuves mērķis**

Lai nodrošinātu pareizus piekļuves ierobežojumus, svarīgi ir rūpīgi definēt nosacījumus, kā piekļūt VIS datiem. Ir apsveicami, ka, līdztekus pašam ierosinātajam lēmumam paskaidrojuma raksts un apsvērumi (skat. jo īpaši 7. apsvērumu) ļoti labi paskaidro, ka nodoms paredz piekļuvi vienīgi individuālos gadījumos.

Par priekšlikuma 5. pantu var izteikti vienu piebildi, lai vadītu tā interpretāciju.

5. pants ierobežo piekļuves apjomu ar būtiskiem nosacījumiem:

b) datiem informācijas nolūkos ir jāpiekļūst, lai novērstu, atklātu un izmeklētu terora aktus un citus smagus noziedzīgus nodarījumus;

c) datiem informācijas nolūkos ir jāpiekļūst, izskatot konkrētu lietu (...), un

d) ir jābūt pietiekamam, faktos apliecinātam pamatojumam, lai uzskatītu, ka piekļuve VIS datiem informācijas nolūkos palīdzēs novērst, atklāt un izmeklēt kādus no attiecīgiem noziedzīgiem nodarījumiem.

Minētie nosacījumi ir kumulatīvi, b) apakšpunktā ietvertais nosacījums vairāk ir *ratione materiae* mēroga definīcija. Praksē tas nozīmēs, ka iestādei, kas grib panākt piekļuvi, ir jāsastopas ar smagu noziegumu, ka minēts priekšlikuma b) apakšpunktā; ir jābūt konkrētai lietai, kā minēts c) apakšpunktā. Turklāt iestādei jāspēj pierādīt, ka konkrētā gadījumā piekļuve VIS datiem informācijas nolūkos palīdzēs novērst, atklāt vai izmeklēt minēto noziedzīgo nodarījumu, kā paredzēts d) apakšpunktā.

EDAU, arī šādi interpretējot 5. pantu, ir norūpējies par d) punkta brīvo izteiksmi: "palīdz" ir pārāk plašs formulējums. Ir daudzi gadījumi, kad VIS dati varētu "palīdzēt" novērst vai izmeklēt kādu smagu noziegumu. Lai pamatotu piekļuvi VIS datiem, atkāpjoties no sākotnēji iecerētā lietojuma precizitātes principa, EDAU uzskata, ka piekļuvei datiem informācijas nolūkos būtu "būtiski jāpalīdz", lai novērstu, atklātu vai izmeklētu attiecīgus smagus noziedzīgus nodarījumus, un ierosina attiecīgi grozīt 5. pantu.

10. pantā paredzēts, ka reģistra datiem būtu jāatspoguļo piekļuves īstais mērķis. "Īstajā mērķī" būtu jāietver elementi, kāpēc bijusi vajadzīga piekļuve VIS informācijas nolūkos — 5. *sub* panta d) apakšpunkta nozīmē. Tas palīdzēs nodrošināt to, ka piekļuve VIS datiem informācijas nolūkos vienmēr būs atkarīga no pārbaudes, pārliecinoties par vajadzību to darīt, un mazināt regulāras pieejas iespējamību.

2.3. **Parametri meklējumiem VIS datu bāzē**

5. panta 2. un 3. punktā paredz divpakāpju pieeju VIS datiem, kurā datu komplekss kļūst pieejams tikai tad, ja dati ir atrasti, izmantojot pirmo datu kompleksu. Pati par sevi tā ir loģiska pieeja. Tomēr pirmais datu komplekss šķiet ļoti plašs. Konkrēti, var apšaubīt tādu datu svarīgumu, kuri ir minēti 5. panta 2. punkta e) un i) apakšpunktā pirmam datu kompleksam:

— "Brauciena iemesls" šķiet pārlieku vispārīgs parametrs, lai gūtu iespēju reāli izmantot sistēmu. Turklāt tas rada iespēju sastādīt braucēju profilu pēc minētā elementa.

— Runājot par "fotoattēliem", iespējas meklēt datus tik milzīgā datu bāzē, izmantojot fotoattēlus, ir ierobežotas; tādu meklējumu rezultāti pašreizējā tehnoloģijas attīstības stadijā rada nepieņemami lielu nepareizu sakritību procentu. Nepareizas identifikācijas sekas attiecīgai personai ir ļoti nopietnas.

Tālab EDAU lūdz datus 5. panta 2. punkta e) un i) apakšpunktā uzskatīt par papildu informāciju, kas ir pieejama, ja pirmais informācijas meklējums rāda, ka sistēmā jau ir dati, un pārcelt uz 5. panta 3. punktu.

Alternatīvi, iespēja veikt meklējumus datu bāzē, izmantojot fotoattēlus, varētu būt atkarīga no minētās tehnoloģijas izvērtējuma konsultatīvā komitejā, un īstenot vienīgi tad, kad tehnoloģija būs attīstījusies, un to varēs uzskatīt par pietiekami drošticamu.

2.4. **Iesniegumi dalībvalstīm, uz ko neattiecas VIS regula**

VIS datu bāzei informatīvos nolūkos var piekļūt iestādes, kas ir atbildīgas par iekšējo drošību dalībvalstīs, kuras nepiedalās Vīzu informācijas sistēmā. Tādiem dienestiem informācija jāiegūst ar tādas dalībvalsts starpniecību, kura piedalās sistēmā, pienācīgi ņemot vērā 5. panta 1. punkta b) līdz d) apakšpunktā ietvertos nosacījumus (piem., katrā individuālā gadījumā), un jāiesniedz pietiekami pamatots rakstisks lūgums.

EDAU vēlētos uzsvērt vajadzību uzlikt dažus nosacījumus datu apstrādei pēc informācijas ieguves. Noteikums, kas attiecas uz dalībvalstīm, kuras nepiedalās Vīzu informācijas sistēmā, ir — kad dati ir iegūti no VIS, tie jāapstrādā saskaņā ar pamatlēmumu par datu aizsardzību un datu aizsardzību trešā pīlāra jomā (skat. še turpmāk). Tam pašam nosacījumam būtu jāattiecas uz tām dalībvalstīm, uz ko neattiecas VIS regula, bet kuras izmanto tās datus. Tādai pašai domu gaitai būtu jābūt, glabājot reģistra datus kontrolei nākotnē. Tālab EDAU ierosina priekšlikuma 6. pantam pievienot punktu, lai lēmuma 8. un 10. pants attiektos arī uz tām dalībvalstīm, uz ko neattiecas VIS regula.

2.5. **Datu aizsardzības režīms**

a) *Piemērojot pamatlēmumu par datu aizsardzību un datu aizsardzību trešā pīlāra jomā*

Tā kā par iekšējo drošību atbildīgo iestāžu piekļuve ir izņēmums no sākotnēji iecerētā VIS lietojumā, uz to būtu jāattiecina konsekvents datu aizsardzības režīms, kas nodrošinātu augsta līmeņa aizsardzību no VIS iegūtiem un attiecīgu valstu iestāžu vai Eiropola apstrādātiem datiem.

Priekšlikuma 8. pantā paredzēts, ka Padomes pamatlēmums par to personas datu aizsardzību, kurus apstrādā saskaņā ar policijas un tiesu iestāžu sadarbību krimināllietās (še turpmāk: "pamatlēmums") attieksies uz datu apstrādi saskaņā ar ierosināto lēmumu. Ciktāl ir runa par datu aizsardzību, šo priekšlikumu vajadzētu uzskatīt par *lex specialis*, kas papildina vai precizē *lex generalis* (t.i., pamatlēmumu). Piemēram, šajā priekšlikumā ir stingrāki noteikumi par datu pārsūtīšanu tālāk, un tie būtu jāievēro. Tas pats attiecas uz pamatojumiem, kāpēc vajadzīga piekļuve datiem.

b) *Darbības joma*

EDAU sveic to, ka pamatlēmumā paredzētais datu aizsardzības režīms ir piemērojams visai personas datu apstrādei saskaņā ar ierosināto lēmumu. Tas nozīmē, ka datu aizsardzības līmenis ir tāds pats, lai kādas iestādes informācijas nolūkos iegūtu VIS datus.

Tā kā 2. pantā ir izmantots funkciju kritērijs, lai noteiktu tādas iestādes ("tās dalībvalstu iestādes, kas ir atbildīgas par terora aktu un citu smagu noziedzīgu nodarījumu novēršanu, atklāšanu un izmeklēšanu"), šī definīcija varētu attiekties arī uz izlūkdienestiem, ne tikai tiesībaizsardzības iestādēm. Tālab uz izlūkdienestiem, kas informācijas nolūkos izmanto VIS, principā attiecas tie paši pienākumi attiecībā uz datu aizsardzību, un tas ir klaji pozitīvs elements.

Tomēr, tā kā var rasties šaubas par tādu interpretāciju attiecībā uz pamatlēmuma piemērojamību izlūkdienestiem, kad tie gūst piekļuvi VIS datiem, EDAU ierosina citu formulējumu, piemēram:

"Gadījumos, kad pamatlēmums (...) nav piemērojams, dalībvalstis nodrošina tāda līmeņa datu aizsardzību, kas ir vismaz līdzvērtīga pamatlēmumā paredzētajai".

c) *Kontrole*

Attiecībā uz 8. panta formulējumu, būtu jāpaskaidro, ka 1. punkts attiecas uz datu apstrādi dalībvalstu teritorijā. 2. un 3. punkts izskaidro to piemērojuma jomu (datu apstrāde Eiropolā un Komisijā), un būtu jādara skaidri saprotams, ka 1. punkts attiecas uz citu hipotēzi.

Kontroles kompetenču sadale, ievērojot dažādu darbību veicēju attiecīgās darbības, ir loģiska pieeja. Viena elementa tomēr trūkst: vajadzības pēc koordinētas pieejas kontrolē. Kā jau ir norādīts EDAU atzinumā par VIS:

"Attiecībā uz VIS kontroli ir arī svarīgi uzsvērt, ka attiecīgo valstu un Eiropas datu aizsardzības uzraudzītāja veiktās kontroles darbības būtu mazliet jākoordinē. Patiesi, regula ir jāīsteno saskaņoti, un jāstrādā, lai rastu vienotu pieeju kopējām problēmām. [VIS priekšlikuma] 35. pantā būtu jāietver nosacījums par to, ka Eiropas datu aizsardzības uzraudzītājs vismaz reizi gadā sasauc sanāksmi ar visu attiecīgo valstu kontroles iestādēm."

Tas pats attiecas uz konkrētu VIS sistēmas lietojumu (šajā gadījumā arī ar Eiropola apvienotās kontroles struktūras iesaisti). Kontrolei būtu pilnībā jāsaskan ar "pirmā pīlāra VIS" kontroli, jo tā ir viena un tā pati sistēma. Turklāt EDAU sasauktās koordinācijas sanāksmes, kurās piedalās visas kontrolē iesaistītās personas, ir arī modelis, kas izraudzīts sakarā ar citu liela mēroga informācijas sistēmu, piemēram *Eurodac* kontroli.

EDAU apzinās, ka priekšlikumā ir paredzēta kāda koordinācija, jo tajā pieminēts uzdevums, kas būs dots izveidojamai darbagrupai indivīdu aizsardzības jautājumos attiecībā uz personas datu aizsardzību, ko izveidos saskaņā ar ierosinātā pamatlēmuma 31. pantu. Tomēr jāuzsver, ka pie minētās konsultatīvās struktūras uzdevuma nepieder pati kontrole.

EDAU ierosina pievienot noteikumu, kas paredzētu, ka EDAU sasauktas koordinācijas sanāksmes saskaņā ar "pirmā pīlāra VIS" kontroli būtu arī kompetentas attiecībā uz datiem, kas apstrādāti saskaņā ar šo ierosināto tiesību aktu, un tātad būtu jāpārstāv Eiropola AUI.

2.6. **Pašaudits**

Priekšlikuma 12. pantā ir paredzētas VIS pārraudzības sistēmas. EDAU uzskata, ka pārraudzībai būtu jāattiecas gan uz tādiem aspektiem kā pakalpojumu darbības efektivitāti, rentabilitāti un kvalitāti, gan arī uz juridisko prasību ievērošanu, jo īpaši datu aizsardzības jomā. 12. pants būtu attiecīgi jāgroza.

Lai veiktu datu apstrādes likumīguma pašauditu, Komisijai būtu jādod iespējas izmantot reģistra datus, ko glabā saskaņā ar priekšlikuma 10. pantu. Attiecīgi 10. pantā būtu jāparedz, ka reģistra datus glabā ne tikai, lai pārraudzītu datu aizsardzību un garantētu datu drošību, bet arī regulāram VIS pašauditam. Pašaudita ziņojumi palīdzēs EDAU un citiem kontrolieriem veikt pārraudzības pienākumus, viņi varēs labāk noteikt prioritāras pārraudzības jomas.

3. **SECINĀJUMS**

Ņemot vērā iepriekš teikto, EDAU uzsver, cik būtiski ir tas, ka par iekšējo drošību atbildīgām iestādēm un Eiropolam piekļuvi piešķir vienīgi konkrētos gadījumos un ievērojot stingrus drošības pasākumus. Priekšlikumā šis mērķis ir sasniegts kopumā pietiekami, kaut gan varētu veikt dažus uzlabojumus, kā ierosināts šajā atzinumā:

— Par priekšnosacījumu piekļuvei VIS saskaņā ar 5. pantu, ka iegūtā informācija "būtiski" palīdzēs novērst, atklāt un izmeklēt smagus noziedzīgus nodarījumus, un 10. pantā prasītiem reģistra datiem būtu jāļauj katrā konkrētā gadījumā izvērtēt šo nosacījumu.

— Divi parametri meklējumiem Vīzu informācijas sistēmā, kuri minēti 5. panta 2. punktā, konkrēti "brauciena iemesls" un "fotoattēli", būtu jāpārdomā un jāizmanto kā papildinformācija gadījumā, ja informācija atrodas.

— Datu aizsardzības līmenim, kas piemērojams pēc informācijas ieguves, būtu jābūt līdzvērtīgam neatkarīgi no tā, kādas iestādes informācijai iegūst VIS datus. 8. un 10. pantam būtu jāattiecas arī uz dalībvalstīm, kas nepiemēro VIS regulu.

— Būtu jānodrošina koordinēta pieeja kontrolei, arī attiecībā uz piekļuvi VIS, kā priekšlikumā paredzēts.

— Noteikumiem par pārraudzības sistēmām arī būtu jānodrošina datu aizsardzības prasību ievērošanas pašaudits.

Briselē, 2006. gada 20. janvārī

Peter HUSTINX

Eiropas datu aizsardzības uzraudzītājs