Eiropas datu aizsardzības uzraudzītājs

Eiropas datu aizsardzības uzraudzītāja atzinums

— par priekšlikumu Padomes Lēmumam par otrās paaudzes Šengenas Informācijas sistēmas (*SIS II*) izveidi, pārvaldību un izmantošanu (COM(2005) 230 galīgā redakcija);

— priekšlikumu Eiropas Parlamenta un Padomes Regulai par otrās paaudzes Šengenas Informācijas sistēmas (*SIS II*) izveidi, darbību un izmantojumu (COM(2005) 236 galīgā redakcija) un

— priekšlikumu Eiropas Parlamenta un Padomes Regulai par dalībvalstu dienestu, kas ir atbildīgi par transportlīdzekļu reģistrācijas apliecību izdošanu, piekļuvi otrās paaudzes Šengenas informācijas sistēmai (*SIS II*) (COM(2005) 237 galīgā redakcija).

(2006/C 91/11)

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 lūgumu nākt klajā ar atzinumu saskaņā ar Regulas (EK) Nr. 45/2001 28. panta 2. punktu, kurš saņemts no Komisijas 2005. gada 26. maijā,

IR PIEŅĒMIS ŠO ATZINUMU:

1. IEVADS

1.1. Vispārēja informācija

Šengenas informācijas sistēma (*SIS*) ir ES mēroga IT sistēma, ko izveidoja, lai atsvērtu iekšējas robežkontroles atcelšanu Šengenas teritorijā. *SIS* ļauj dalībvalstu kompetentām iestādēm apmainīties ar informāciju, ko izmanto, pārbaudot personas un objektus pie ārējām robežām vai Šengenas teritorijā, kā arī, izsniedzot vīzas un uzturēšanās atļaujas.

Šengenas Konvencija stājās spēkā 1995. gadā valdību nolīguma formā. *SIS* kā daļu no Šengenas Konvencijas vēlāk iekļāva ES sistēmā, pieņemot Amsterdamas Līgumu.

Pašreizējo sistēmu aizstās ar jaunu, "otrās paaudzes" Šengenas Informācijas sistēmu II, tādējādi Šengenas teritorijā iekļaujot arī jaunās ES dalībvalstis. Jaunajai sistēmai arī būs jaunas tehniskas funkcijas. Valdību izstrādātos Šengenas noteikumus pilnībā pārstrādās parastos Eiropas tiesību instrumentos.

Eiropas Komisija 2005. gada 1. jūnijā iesniedza trīs priekšlikumus par *SIS* II izveidi. Tie ir:

— priekšlikums regulai, kas pamatojas uz EK Līguma IV sadaļu (vīzas, patvēruma, imigrācijas un citas ar cilvēku brīvu pārvietošanos saistītas politikas jomas) un ar ko reglamentēs *SIS* II pirmā pīlāra (imigrācijas) aspektus — še turpmāk "ierosinātā regula";

— priekšlikums lēmumam, kas pamatojas uz Līguma par ES VI sadaļu (policijas un tiesu iestāžu sadarbība krimināllietās) un ar ko reglamentēs *SIS* izmantošanu attiecībā uz trešo pīlāru — še turpmāk "ierosinātais lēmums";

— priekšlikums regulai, kas pamatojas uz V sadaļu (Transports) un konkrēti attiecas uz transportlīdzekļu reģistrācijas iestāžu piekļuvi *SIS* datiem; šim priekšlikumam pievērsīsies atsevišķi (skat. turpmāk, 4.6. punktā).

Šajā sakarā der piebilst, ka Komisija turpmākajos mēnešos nāks klajā ar paziņojumu par ES informācijas sistēmu (*SIS*, *VIS*, *Eurodac*) savstarpēju savietojamību un pastiprinātām sinerģijām.

SIS II ir centralizēta datubāze — saukta "Centrālā Šengenas informācijas sistēma" (*CS-SIS*) –, kuras operatīvo vadību nodrošina Komisija saistībā ar katras attiecīgas valsts noteiktiem piekļuves punktiem (*NI-SIS*). *SIRENE* iestādes nodrošina jebkādu apmainīšanos ar papildinformāciju (informāciju, kas saistīta ar *SIS* II brīdinājumiem, bet ko neglabā *SIS* II).

Dalībvalstis nodrošinās SIS II ar datiem par personām, ko meklē, lai tās apcietinātu, nodotu vai izdotu; personām, ko meklē saistībā ar tiesas procedūrām; personām, kas jāuzrauga vai īpaši jāpārbauda; personām, kam jāliedz ieceļošana pie ārējām robežām; kā arī datiem par zaudētiem vai zagtiem priekšmetiem. Datu kopums, ko sauc par "brīdinājumiem" un ko ievada *SIS*, ļauj kompetentai iestādei identificēt personu vai objektu.

SIS II ir jaunas iezīmes: paplašināta pieejamība *SIS* (Eiropolam, *Eurojust*, attiecīgu valstu prokuroriem, transportlīdzekļu reģistrācijas iestādēm), savstarpēji saistīti brīdinājumi, jaunas datu kategorijas, tostarp biometrijas dati (pirkstu nospiedumi un fotogrāfijas), kā arī tehniska platforma, ko izmanto arī Vīzu informācijas sistēma. Šie papildinājumi jau gadiem ilgi ir rosinājuši diskusijas par *SIS* pārveidošanu no kontroles instrumenta par ziņošanas un izmeklēšanas sistēmu.

1.2. **Priekšlikumu vispārējs novērtējums**

1. EDAU pauž gandarījumu par to, ka ar viņu apspriežas, kā paredzēts Regulas (EK) Nr. 45/2001 28. panta 2. punktā. Ņemot vērā to, ka 28. panta 2. punkts uzliek obligātas saistības, šis atzinums tomēr būtu jāpiemin dokumentu preambulā.

2. EDAU pauž gandarījumu par priekšlikumiem vairāku iemeslu dēļ. Valdību izveidotas struktūras pārveidei Eiropas tiesību instrumentos ir vairākas pozitīvas sekas: tādējādi precizēs juridisko vērtību noteikumiem, ar ko reglamentē *SIS* II, Tiesa būs kompetenta interpretēt pirmā pīlāra juridisko instrumentu), Eiropas Parlaments būs vismaz daļēji iesaistīts (lai gan mazliet par vēlu procesa norisē).

3. Turklāt attiecībā uz būtību — liela priekšlikumu daļa ir veltīta datu aizsardzībai un daži ierosinājumi paredz gaidītus uzlabojumus, salīdzinot ar pašreizējo stāvokli. Jo īpaši var minēt pasākumus, lai atbalstītu personas, kas cietušas identitātes nozagšanu, Regulas 45/2001 piemērošanas jomas paplašināšanu, lai iekļautu Komisijas veiktas datu apstrādes darbības IV sadaļas darbībās, labāku pamatojumu brīdinājuma izsniegšanai par fiziskām personām, liedzot tām ieceļošanu .

4. Ir acīmredzams, ka priekšlikumu sagatavošana ir veikta ļoti rūpīgi; priekšlikumi ir sarežģīti, bet tas atspoguļo to, cik sarežģīta ir sistēma, ko ar tiem reglamentē. Vairākums piebilžu, kas izteikti šajā atzinumā, ir paredzēti, lai precizētu vai papildinātu priekšlikumu noteikumus, bet nerada vajadzību priekšlikumus pilnīgi pārstrādāt.

Lai gan novērtējums ir visnotaļ pozitīvs, tomēr var izteikt dažus iebildumus, jo īpaši par šādiem jautājumiem:

1. Ir daudzkārt grūti zināt, kas ir dokumenta sastādīšanas nodoms; ir patiešām žēl, ka nav pievienots paskaidrojuma raksts. Ņemot vērā, cik ļoti sarežģīti ir šie dokumenti, būtu domājams, ka šāda paskaidrojuma pievienošana būtu bijusi pamatprasība. Paskaidrojuma trūkuma dēļ lasītājam dažkārt atliek tikai minēt.

2. Turklāt var tikai nožēlot, ka nav veikts ietekmes novērtējums. Tas, ka sistēmas pirmā versija jau darbojas, neattaisno šādu rīcību, jo priekšlikumi viens no otra ļoti atšķiras. Cita starpā būtu vajadzējis labāk izvērtēt biometrijas datu ieviešanas iespaidu.

3. Juridisko datu aizsardzības sistēma ir ļoti sarežģīta; tā pamatojas uz *lex generalis* un *lex specialis* kopīgu piemērošanu. Būtu jānodrošina, ka pat tad, kad izstrādā konkrētu tiesību aktu, Direktīvā 95/46/EK un Regulā 45/2001 noteiktā, spēkā esošā datu aizsardzības sistēma paliek pilnībā piemērojama. Dažādu juridisku instrumentu kopīgai piemērošanai nebūtu jārada valstu režīmu atšķirības būtiskos jautājumos, nedz arī jāizraisa pašreizējā datu aizsardzības līmeņa pazemināšanās.

4. Nodrošinot piekļuvi daudzām jaunām iestādēm, kas neveic darbības "personu un objektu pārbaudes nolūkos", būtu arī jāparedz stingrāki drošības mehānismi.

5. Priekšlikumi lielā mērā ir balstīti uz citiem juridiskiem instrumentiem, kas vēl nav galīgi izstrādāti (dažkārt tie pat nav vēl ierosināti). EDAU saprot, cik grūti ir izstrādāt tiesību aktus sarežģītā un pastāvīgi mainīgā vidē; ņemot vērā, kādas var būt sekas attiecīgām personām un juridisko neskaidrību, ko tas rada, viņš tomēr šādu stāvokli uzskata par nepieņemamu.

6. Dalībvalstu un Komisijas pilnvaru sadale nav visai skaidra. Skaidrība ir būtiski svarīga ne tikai, lai sistēma pareizi darbotos, bet arī, jo tā ir pamatprasība, nodrošinot sistēmas vispārēju uzraudzību.

1.3. **Atzinuma struktūra**

Atzinuma struktūra ir šāda: pirmkārt, tajā ir precizēts *SIS* II piemērojamais tiesiskais regulējums. Pēc tam tajā pievēršas *SIS* II mērķa definīcijai un aspektiem, kas būtiski atšķiras no tiem, kuri piemīt pašreizējai sistēmai. 5. punktā iekļautas piebildes par Komisijas un dalībvalstu attiecīgo vietu *SIS* II darbībā. 6. punkts attiecas uz datu subjekta tiesībām, kamēr 7. punktā pievēršas attiecīgu valstu mērogā un EDAU veiktai uzraudzībai, kā arī uzraudzītāju savstarpējai sadarbībai. 8. punktā dotas piebildes un ierosināti iespējami grozījumi attiecībā uz drošību; 9. un 10. punktā pievēršas, attiecīgi, komitoloģijai un savstarpējai savietojamībai. Visbeidzot, secinājumu kopsavilkumā uzsvērti galvenie secinājumi par katru punktu.

2. ATTIECĪGAIS TIESISKAIS REGULĒJUMS

2.1. **Attiecīgā SIS II datu aizsardzības sistēma**

Priekšlikumos izmantotais datu aizsardzības tiesiskais regulējums ir Direktīva 95/46/EK, Konvencija Nr. 108 un Regula 45/2001. Arī citi instrumenti ir būtiski.

Lai precizētu šo regulējumu un atgādinātu par galvenajiem izskatīšanā izmantojamiem atsauces punktiem, noder šāds saraksts:

— 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 noteiktas "tiesības 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 "gadījumos, kas noteikti likumā" un ir "nepieciešami demokrātiskā sabiedrībā" svarīgu interešu aizsargāšanai. Eiropas Cilvēktiesību tiesas praksē šie nosacījumi ir bijuši par pamatu papildu prasībām par iejaukšanās juridiskā pamata kvalitāti, kā arī attiecībā uz pasākumu samērīgumu un vajadzību pēc piemērotiem drošības mehānismiem pret datu ļaunprātīgu izmantošanu.

— Tiesības uz privāto dzīvi un personas datu aizsardzību ir paredzētas tuvākā pagātnē — Eiropas Savienības Pamattiesību hartas 7. un 8. pantā. Saskaņā ar Hartas 52. pantu atzīts, ka uz šīm tiesībām var attiekties ierobežojumi, ar nosacījumu, ka ievēro līdzīgus nosacījumus, ko piemēro saskaņā ar ECK 8. pantu.

— Līguma par ES 6. panta 2. punktā noteikts, ka Eiropas Savienība ievēros pamattiesības, ko garantē ECK.

Šādi trīs dokumenti attiecas tieši uz priekšlikumiem par *SIS* II:

— Eiropas Padomes 1981. gada 28. janvāra Konvencijā par personu aizsardzību attiecībā uz personas datu automātisko apstrādi (še turpmāk — "Konvencija Nr. 108") izstrādāti fizisku personu aizsardzības pamatprincipi attiecībā uz personas datu apstrādi. Visas dalībvalstis ir ratificējušas Konvenciju Nr. 108. Tā attiecas arī uz darbībām, kas veiktas policijas un tiesas iestāžu jomā. Konvencija Nr. 108 ir datu aizsardzības režīms, ko pašreiz piemēro *SIS* Konvencijai, kopā ar Eiropas Padomes Ministru komitejas 1987. gada 17. septembra Ieteikumu Nr. R (87) 15, ar ko reglamentē personas datu izmantošanu policijas nozarē.

— Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīva 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (OV L 281., 31. lpp.). Turpmāk tekstā šo direktīvu sauks "Dir*ektīva 95/46/EK*". Der norādīt, ka vairumā dalībvalstu valsts tiesību akti, ar ko īsteno direktīvu, attiecas arī uz apstrādes darbībām, ko veic policijas un tiesu iestāžu jomā.

— Eiropas Parlamenta un Padomes 2000. gada 18. decembra Regula (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.). Turpmāk tekstā šo regulu sauks "*Regula 45/2001*".

Direktīvas 95/46/EK un Regulas 45/2001 interpretācijai ir jābūt daļēji atkarīgai no attiecīgās Eiropas Cilvēktiesību tiesas prakses saskaņā ar 1950. gada Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvenciju (ECK). Citiem vārdiem sakot, direktīva un regula, ciktāl tajās risināti jautājumi par personu datu apstrādi, kas var radīt pamattiesību pārkāpumus, jo īpaši attiecībā uz tiesībām uz privāto dzīvi, ir jāinterpretē, ņemot vērā pamattiesības. Tas izriet arī no Eiropas Kopienu Tiesas judikatūras ([1]).

([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. Tiesas 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.

Komisija 2005. gada 4. oktobrī nāca klajā ar priekšlikumu Padomes pamatlēmumam par personas datu aizsardzību, ko apstrādā, sadarbojoties policijas un tiesu iestādēm kriminālietās ([1]) (še turpmāk "*ierosinātais pamatlēmums*"). Ar šo pamatlēmumu ir iecerēts aizstāt Konvenciju Nr. 108 kā atsauces tiesību aktu ierosinātajam lēmumam par *SIS* II, tādējādi, iespējams, šajā sakarā iespaidojot datu aizsardzības režīmu (skatīt zemāk minēto 2.2.5. punktu).

2.2. **SIS II datu aizsardzības juridiskais režīms**

2.2.1. *Vispārīga piebilde*

Juridiskajā pamatā, kas vajadzīgs, lai reglamentētu *SIS* II, ir vairāki atsevišķi instrumenti; tomēr, kā minēts apsvērumos, tas "neskar principu, ka *SIS* II ir viena vienota informācijas sistēma, kam attiecīgi jādarbojas. Dažiem šo instrumentu noteikumiem tādēļ būtu jābūt identiem".

Šo divu dokumentu struktūra pamatā ir viena un tā pati, un abu dokumentu I-III nodaļa ir gandrīz identa. Tas, ka *SIS* II uzskata par vienotu informācijas sistēmu ar diviem atšķirīgiem juridiskiem pamatiem, ir arī atspoguļots diezgan sarežģītajā datu aizsardzības režīmā.

Datu aizsardzības režīms ir daļēji paredzēts pašos priekšlikumos kā *lex specialis*, ko attiecībā uz katru nozari (Komisija, dalībvalstis pirmajā pīlārā, dalībvalstis trešajā pīlārā) papildina ar citu atsauces tiesību aktu (*lex generalis*).

Attiecībā uz šādu struktūru rodas jautājums — kā izturēties pret specializētiem noteikumiem, ņemot vērā to attiecības ar vispārējām tiesībām. Šajā gadījumā EDAU uzskata, ka ar konkrētu normu piemēro vispārēju normu. Tādēļ *lex specialis* ir vienmēr jābūt saskaņā ar *lex generalis*; ar to izvērš (precizē vai papildina) *lex generalis*, bet tas nav domāts kā izņēmums no *lex generalis*.

Attiecībā uz jautājumu par to, kuru normu piemērot konkrētā gadījumā — *lex specialis* piemēro prioritāri, bet, ja tā nav vai tas ir neskaidrs, būtu jāatsaucas uz *lex generalis*.

Saskaņā ar šo struktūru ir iespējamas trīs dažādas *lex generalis* un *lex specialis* kombinācijas. Struktūru varētu rezumēt šādi:

2.2.2. *Komisijai piemērojamais režīms*

Ja ir iesaistīta Komisija, piemēro Regulu 45/2001, tostarp attiecībā uz EDAU vietu, neatkarīgi no tā, vai darbības veic saskaņā ar pirmo (ierosinātās regulas gadījumā) vai trešo pīlāru (ierosinātā lēmuma gadījumā). Ierosinātā lēmuma 21. apsvērumā noteikts: "Regula (EK) Nr. 45/2001 (…) attiecas uz Komisijas veiktu personas datu apstrādi, ja to veic, izpildot darbības, uz ko pilnībā vai daļēji attiecas Kopienas tiesības. Uz daļu no personas datu apstrādes *SIS* II sistēmā attiecas Kopienas tiesības."

Šādiem noteikumiem ir praktiski iemesli: tiktāl, ciktāl tas attiecas uz Komisiju, būtu patiesi ārkārtīgi grūti uzzināt, vai attiecīgo datu apstrāde ir darbība, uz ko attiecas pirmā vai trešā pīlāra tiesību akti.

Turklāt, viena juridiska instrumenta piemērošana visām darbībām, ko *SIS* II sakarā veic Komisija, ne vien ir saprotamāka no praktiska viedokļa, bet arī veicina konsekvenci (saskaņā ar ierosinātās regulas 21. apsvērumu nodrošinot "konsekventu un vienveidīgu noteikumu piemērošanu attiecībā uz fizisku personu pamattiesību un brīvību aizsardzību saistībā ar personas datu apstrādi"). EDAU tādēļ pauž gandarījumu par to, ka Komisija ir atzinusi, ka Regula 45/2001 attiecas uz visām datu apstrādes darbībām, ko Komisija veic *SIS* II.

2.2.3. *Dalībvalstīm piemērojamais režīms*

Attiecībā uz dalībvalstīm stāvoklis ir sarežģītāks. Personas datu apstrādi, piemērojot ierosināto regulu, reglamentē ar pašu regulu, kā arī ar Direktīvu 95/46/EK. Ierosinātās regulas 14. apsvērumā skaidri norādīts, ka direktīvu jāuzskata par *lex generalis*, kamēr *SIS* II regula būs *lex specialis*. Šādam norādījumam ir vairākas sekas, kas turpmāk sīki izklāstītas.

Attiecībā uz ierosināto lēmumu datu aizsardzībā izmantojamais atsauces juridiskais instruments (*lex generalis*) ir Konvencija Nr. 108, kas attiecībā uz dažiem jautājumiem var radīt būtiski svarīgas pirmā un trešā pīlāra datu aizsardzības režīma atšķirības.

2.2.4. *Ietekme uz datu aizsardzības līmeni*

Kā vispārīgu piebildi par šādu datu aizsardzības struktūru, EDAU uzsver:

— Piemērojot ierosināto regulu kā *lex specialis* attiecībā uz Direktīvu 95/46/EK (un līdzīgā kārtā piemērojot ierosināto lēmumu kā *lex specialis* attiecībā uz Konvenciju Nr. 108), nekādā ziņā nevajadzētu pazemināt datu aizsardzības līmeni, ko nodrošina ar attiecīgo direktīvu vai konvenciju. EDAU nāks klajā ar attiecīgiem ieteikumiem (skatīt, piemēram, tiesības uz aizsardzības līdzekļiem).

([1]) (COM (2005) 475 galīgā redakcija).

— Līdzīgā kārtā juridisku instrumentu apvienota piemērošana nedrīkst pazemināt datu aizsardzības līmeni, ko nodrošina spēkā esošā Šengenas Konvencija (skatīt, piemēram, turpmākās piebildes par Direktīvas 95/46/EK 13. pantu).

— Divu dažādu instrumentu piemērošanai, vienalga, cik vajadzīga tā būtu Eiropas tiesību sistēmas dēļ, nebūtu jārada nepamatotas atšķirības attiecīgu fizisku personu datu aizsardzībā atkarīgi no tā, kāda veida ar tiem saistītus datus apstrādā. Šāds stāvoklis pēc iespējas jānovērš. Turpmākie ieteikumi tiecas cik vien iespējams panākt lielāku konsekvenci (skatīt, piemēram, valstu uzraudzības iestāžu pilnvaras).

— Tiesiskais regulējums ir tik sarežģīts, ka, to piemērojot, ļoti iespējams, radīsies pārpratumi. Dažos gadījumos ir grūti saprast *lex generalis* un *lex specialis* mijiedarbību — būtu labi to precizēt priekšlikumos. Turklāt šajā sarežģītajā juridiskā vidē ļoti lietderīgs ir ieteikums, ar ko nākusi klajā Šengenas Apvienotā uzraudzības iestāde 2005. gada 27. septembra "atzinumā par ierosināto *SIS* II juridisko pamatu": proti, izstrādāt rokasgrāmatu, kurā uzskaitītas visas spēkā esošās ar *SIS* II saistītās tiesības un izklāstīta skaidra piemērojamo tiesību aktu hierarhija.

Visbeidzot, ar šo ieteikumu tiecas nodrošināt augsta līmeņa datu aizsardzību, konsekvenci un skaidrību, lai datu subjektam sniegtu vajadzīgo juridisko skaidrību.

2.2.5. *Pamatlēmuma projekta ietekme uz datu aizsardzību trešajā pīlārā*

Konvenciju Nr. 108 kā datu aizsardzības atsauces instrumentu *SIS* II lēmuma projektam aizstās ar Pamatlēmumu par datu aizsardzību trešajā pīlārā [1]. Tas nav minēts priekšlikumā, bet izriet no ierosinātā pamatlēmuma. Tā 34. panta 2. punktā noteikts, ka "katru atsauci uz Eiropas Padomes 1981. gada 28. janvāra Konvenciju Personu aizsardzībai attiecībā uz personisko datu automātisko apstrādi (Nr. 108) uzskata par atsauci uz šo pamatlēmumu". Turpmākajās nedēļās EDAU nāks klajā ar atzinumu par ierosināto pamatlēmumu, atzinumā sīki neizpētot pamatlēmuma saturu. Tomēr, ja pamatlēmuma piemērošanai varētu būt nozīmīga ietekme uz *SIS* II datu aizsardzības režīmu, to minēs.

2.2.6. *Direktīvas 95/46/EK 13. panta un Konvencijas Nr. 108 9. panta piemērošana*

Direktīvas 95/46/EK 13. pants un Konvencijas Nr. 108 9. pants dod dalībvalstīm iespēju veikt likumdošanas pasākumus, lai ierobežotu šajos pantos noteikto saistību un tiesību darbības jomu, ja šāds ierobežojums ir pasākums, kas vajadzīgs, lai aizsargātu citas svarīgas intereses (piemēram, valsts drošības, aizsardzības, sabiedrības drošības intereses) [2].

Gan ierosinātas regulas, gan ierosinātā lēmuma apsvērumos minēts, ka dalībvalstis varētu izmantot šādu iespēju, īstenojot priekšlikumus attiecīgās valsts mērogā. Šādā gadījumā būtu jāpiemēro divkārša pārbaude: Direktīvas 95/46/EK 13. panta piemērošanai jāsaskan ar Eiropas Padomes Cilvēktiesību konvencijas 8. pantu un nevajadzētu vājināt spēkā esošo datu aizsardzības režīmu.

Tas ir vēl būtiskāk *SIS* II gadījumā, jo sistēmai ir jābūt prognozējamai. Tā kā dalībvalstis dalās datiem, jābūt iespējai zināt diezgan konkrēti, kā tos apstrādās attiecīgā valstī.

Attiecībā uz šo jautājumu ir viens aspekts, kas vieš bažas: jautājums par to, vai priekšlikumi izraisīs pašreizējā datu aizsardzības līmeņa pazemināšanos. Šengenas Konvencijas 102. pantā noteikta sistēma, kurā datu izmantošana ir stingri reglamentēta un ierobežota, tostarp valsts tiesību aktos ("Datu izmantošanu, kas neatbilst 1. — 4. punkta prasībām, uzskata par ļaunprātīgu izmantošanu atbilstīgi katras Līgumslēdzējas puses valsts tiesību aktiem" Gan Direktīvā 95/46/EK, gan Konvencijā Nr. 108 tomēr noteikts, ka cita starpā izņēmumus no mērķu ierobežojuma principa var ieviest valstu tiesību aktos. Ja to izdarītu, tas būtu pretrunā pašreizējai Šengenas Konvencijā paredzētajai sistēmai, kurā noteikts, ka valstu tiesību aktos nevar atkāpties no pamatprincipa — mērķu un izmantošanas ierobežojuma.

Ar pamatlēmuma pieņemšana šī piezīme nemainītos: galvenā problēma nav nodrošināt, ka datus apstrādātu saskaņā ar pamatlēmumu, bet gan uzturēt stingru mērķu ierobežojuma principu attiecībā uz *SIS* II datu apstrādi.

[1] Ar to arī aizstās Šengenas Konvencijā paredzēto vispārējo datu aizsardzības režīmu (Šengenas Konvencijas 126.-130. pants). Režīms neattiecas uz *SIS*.

[2] Kā iepriekš minēts, dalībvalstis var izmantot šo izvēles iespēju tikai atbilstīgi Eiropas Padomes Cilvektiesību konvencijas 8. pantam.

EDAU iesaka ar *SIS* II saistītos priekšlikumos (konkrēti — ierosinātās regulas 21. pantā un ierosinātā lēmuma 40. pantā) ieviest noteikumu, kam ir tas pats mērķis, kā Šengenas Konvencijas 102. 4. pantam — ierobežot dalībvalstu iespējas paredzēt datu izmantošanu vajadzībām, kas nav paredzētas *SIS* II dokumentos. Cita iespēja ir ierosinātajā lēmumā un ierosinātajā regulā skaidri ierobežot, kādus izņēmumus var izmantot saskaņā ar direktīvas 13. pantu vai konvencijas 9. pantu, piemēram, nosakot, ka dalībvalstis var tikai ierobežot tiesības uz piekļuvi un informāciju, bet nedrīkst ierobežot datu kvalitātes principus.

3. **MĒRĶIS**

Saskaņā ar abu dokumentu 1. pantu, ("*SIS* II izveide un vispārīgais mērķis"), *SIS* II ir izveidota, lai "lai dalībvalstu kompetentās iestādes var sadarboties, apmainoties ar informāciju personu un objektu kontroles nolūkos" un "veicina to, ka tiek uzturēta augsta līmeņa drošība telpā bez iekšējas robežkontroles starp dalībvalstīm".

SIS II mērķa formulējums ir diezgan vispārīgs; minētie noteikumi vien precīzi nenorāda, uz ko attiecas (ko nozīmē) šis mērķis.

SIS II mērķis, šķiet, ir daudz plašāks nekā spēkā esošās *SIS* mērķis, kas definēts Šengenas Konvencijas 92. pantā, kurā konkrēti atsaucas uz "(…) piekļūt ziņojumiem par personām un priekšmetiem, lai veiktu robežkontroli, pārbaudes un citas policijas un muitas īstenotās kontroles (…), kā arī — 96. pantā paredzētā ziņojuma gadījumā — lai izsniegtu vīzas, uzturēšanās atļaujas un lai veiktu ārvalstnieku uzskaiti (…)".

Mērķis ir plašāks arī tādēļ, ka *SIS* II ir paredzētas jaunas funkcijas un piekļuves, kas nav saistītas ar sākotnējā mērķa — fizisku personu un objektu kontroles — īstenošanu, bet gan drīzāk pieder izmeklēšanas instrumentam. Piekļuve ir jo īpaši paredzēta iestādēm, kas izmantos *SIS* II datu savām vajadzībām, nevis *SIS* II mērķu īstenošanai (skatīt turpmāk); brīdinājumu savstarpēju sasaisti padarīs vispārēji pieņemtu, kas ir policijas izmantota izmeklēšanas instrumenta tipiska iezīme.

Joprojām pastāv arī jautājumi par biometrijas meklētājprogrammu, ko paredzēts izstrādāt tuvākajos gados un kas ļaus veikt tādus meklējumus sistēmā, pēc kuriem nav nepieciešamības kontroles sistēmā.

Visbeidzot, minētajiem priekšlikumiem ir daudz plašāka darbības joma, nekā spēkā esošai sistēmai. Tas prasa papildu drošības pasākumus. Šajā sakarā EDAU pievērsīs uzmanību ne tik daudz plašajai 1. panta definīcijai, bet *SIS* II piedāvātām funkcijām un citām sastāvdaļām.

4. **NOZĪMĪGAS PĀRMAIŅAS, KAS ĪSTENOTAS *SIS* II**

Šajā nodaļā vispirms pievērsīsies jaunajiem *SIS* II iekļautajiem aspektiem, proti, biometrijas datu ieviešanai, jaunai piekļuves koncepcijai, pievēršot īpašu uzmanību Eiropola un *Eurojust* piekļuvei, transportlīdzekļu reģistrācijas atbildīgām iestādēm, brīdinājumu savstarpējai sasaistei un dažādu iestāžu piekļuvei imigrācijas datiem.

4.1. **Biometrijas dati**

Ar priekšlikumiem par *SIS* II paredz iespēju apstrādāt jaunas kategorijas datus, kam būtu jāpievērš īpaša uzmanība — biometrijas datus. Kā jau uzsvērts EDAU atzinumā par Vīzu informācijas sistēmu ([1]), biometrijas dati ir būtībā konfidenciāli un prasa īpašus drošības pasākumus, kas nav iekļauti ar *SIS* II saistītajos priekšlikumos.

Vispārēji ņemot, tendence izmantot biometrijas datus ES mēroga informācijas sistēmās (VIS, *EURODAC*, Vadītāju apliecību informācijas sistēmā utt.) pakāpeniski pieaug, bet vienlaicīgi netiek rūpīgi apsvērti saistītie draudi un vajadzīgie drošības pasākumi. Vajadzība pēc dziļākām pārdomām ir arī uzsvērta nesenajā rezolūcijā par biometrijas datiem, ar ko nākusi klajā Starptautiskā datu komisāru konference *Montreux* ([2])(2).

Līdz šim uzmanība ir pievērsta tikai viena tipa papildu vertībai, ko dod standartu izstrāde — arvien lielākai sistēmu savietojamībai, nevis biometrijas procesu kvalitātes uzlabošanai.

([1]) 3.4.2. punkts EDAU 2005. gada 23. marta Atzinumā par priekšlikumu Eiropas Parlamenta un Padomes regulai par Vīzu informācijas sistēmu (VIS) un datu apmaiņu starp dalībvalstīm saistībā ar īstermiņa vīzām.

([2]) Datu un privātuma aizsardzības komisāru 27. starptautiskā konference, kas notika *Montreux* 2005. gada 16. septembrī – Rezolūcija par biometrijas datu izmantošanu pasēs, personas apliecībās un ceļošanas dokumentos.

Derētu izstrādāt kopējus pienākumus vai prasības, kas saistītas ar šādu datu īpašām iezīmēm, kā arī kopēju metodiku šo pienākumu vai prasību īstenošanai. Kopējās prasībās jo īpaši varētu iekļaut šādus aspektus (uz vajadzību pēc tiem norāda ar *SIS* II saistītie priekšlikumi):

— **Konkrētas Ietekmes novērtējums:** Jāuzsver, ka attiecībā uz priekšlikumiem nav veikts biometrijas datu izmantošanas ietekmes novērtējums ([1]).

— **Uzsvars uz iekļaušanas procesu:** Ne biometrijas datu avoti, ne arī datu vākšanas metode nav norādīta. Iekļaušana ir būtiski svarīgs posms ar biometrijas datiem veiktas identifikācijas procesā, un to nevar tikai definēt pielikumos vai turpmākās apakšgrupu apspriedēs, jo no tās būs tieši atkarīgs procesa iznākums — kļūdainas atmešanas koeficients vai kļūdainas pieņemšanas koeficients.

— **Jāuzsver precizitātes pakāpe:** Biometrijas datu izmantošana identifikācijā (salīdzinot vienu ar vairākām) — priekšlikumā ir paredzēta kā "biometrijas datu meklētājprogramma" — ir vēl būtiskāka, jo šāda procesa iznākums ir mazāk precīzs nekā tas, ko gūst, izmantojot šādus datus autentiskuma pārbaudei vai kontrolei (salīdzinot vienu ar vienu). Biometrijas datiem tādēļ nevajadzētu būt vienīgam identifikācijas līdzeklim vai līdzeklim, ar ko piekļūt papildu informācijai.

— **Alternatīva procedūra:** Jāīsteno viegli pieejamas alternatīvas procedūras (fallback procedures), lai ievērotu nepareizi identificētu personu cieņu un viņiem neuzvelt sistēmas nepilnību nastu.

Biometrijas datu izmantošana bez kārtīga iepriekšēja novērtējuma liecina par pārāk augstu biometrijas datu ticamības novērtējumu. Biometrijas dati ir "dzīvi" dati, kas laika gaitā mainās; datubāzē uzglabātie dati atspoguļo dinamiska elementa stāvokli konkrētā brīdī. Tie nepastāv mūžīgi un tie ir jākontrolē. Biometrijas datu precizitāte vienmēr jāredz saistībā ar citiem aspektiem, jo tā nekad nebūs absolūta.

([1]) Novērtējums varētu balstīties uz tā sauktiem septiņiem biometrijas datu filozofijas pīlāriem, kas minēti "*Biometrics at the frontiers: Assessing the impact on Society*" IPTS, DG-JRC, EUR 21585 EN, 1.2. daļā, 32. lappusē.

SIS II datu iespējams izmantojums izmeklēšanās varētu radīt nopietnus draudus datu subjektam, ja pierādījumiem biometrijas datu formā ir piešķirta palielināta vai pārāk liela nozīme, kā rādījuši iepriekšēji gadījumi ([2]).

Tādēļ priekšlikumos būtu jāatzīst un jāveicina apziņa par to, kādas ir biometrijas datu izmantošanas reālās iespējas saistībā ar identifikāciju.

4.2. **Piekļuve SIS II datiem**

4.2.1. *Jauna piekļuves koncepcija*

Iestādes, kas var piekļūt *SIS* datiem, ir noteiktas katram brīdinājumam atsevišķi. Piešķirot piekļuvi *SIS* datiem, būtībā piemēro divkāršu pārbaudi: piekļuvi jāpiešķir iestādēm, kas pilnībā atbilst *SIS* vispārējam mērķim un katra brīdinājuma konkrētam mērķim.

Tas izriet no brīdinājuma definīcijas, kas lietota gan ierosinātajā regulā, gan ierosinātajā lēmumā (abu instrumentu 3.1.a. pantā: *"Brīdinājums" ir datu kopums, ko ievada SIS II un kas kompetentajām iestādēm ļauj identificēt personu vai objektu, lai konkrēti rīkotos*). Šāds viedoklis nostiprināts ierosinātā lēmuma 39.3. pantā, norādot, ka *"Datus, kas minēti 1. punktā, drīkst izmantot tikai personas identificēšanai, lai saskaņā ar šo lēmumu veiktu konkrētu rīcību"*. Šajā ziņā *SIS* II vēl joprojām līdzinās sistēmai, kas paziņo, vai informācija ir atrasta vai nav, un kurā brīdinājums ir iekļauts konkrētam nolūkam (izdošanai, ieteikuma atteikšanai…).

Uz iestādēm, kas var piekļūt *SIS* datiem, attiecas *de facto* izmantošanas ierobežojums, jo tām ir atļauts piekļūt datiem būtībā tikai, lai veiktu konkrētu darbību.

Dažu tipu piekļuves, kas paredzētas jaunajos priekšlikumos, tomēr neatbilst šādai loģikai: patiesi, ar tām paredzēts nodrošināt attiecīgo iestādi ar informāciju, nevis ļaut tai identificēt personu un veikt brīdinājumā paredzēto darbību.

([2]) 2004. gada jūnijā juristu no Portlandes (ASV) apcietināja uz divām nedēļām, jo Federālais izmeklēšanas birojs (FBI) sekmīgi konstatēja viņa pirksta nospieduma atbilsmi nospiedumam, ko atrada, izmeklējot teroristu sarīkotos sprādzienus Madridē (uz plastmasas maisa, kurā bija ielikts detonators). Beigās pierādīja, ka atbilsmes konstatācijas process bijis kļūdains un devis nepareizu interpretāciju.

Konkrētāk, tas attiecas uz:

— patvēruma iestāžu piekļuvi imigrācijas datiem;

— bēgļa statusa piešķiršanas iestāžu piekļuvi imigrācijas datiem;

— Eiropola piekļuvi brīdinājumiem par izdošanu, diskrētu novērošanu un dokumentu aizturēšanu;

— *Eurojust* piekļuvi izdošanas un lokalizācijas datiem.

Visām šīm iestādēm ir vienas un tās pašas iezīmes attiecībā uz *SIS* II datiem:

tās nevar veikt konkrēto attiecīgā brīdinājuma definīcijā minēto darbību. Tām piešķir piekļuvi, lai tās varētu iegūt informāciju savām vajadzībām.

Pat attiecībā uz šīm iestādēm jāatšķir tās, kam ir piešķirta piekļuve savām vajadzībām, bet diezgan konkrēta mērķa sasniegšanai, no tām (proti, Eiropola un *Eurojust*), kuru piekļuves mērķis nemaz nav precizēts. Piemēram, patvēruma iestādēm ir piešķirta piekļuve konkrētam nolūkam, pat, ja tas nav brīdinājumā minētais. Šīs iestādes var piekļūt imigrācijas datiem "lai noteiktu, vai patvēruma lūdzējs ir nelegāli uzturējies citā dalībvalstī". Eiropols un *Eurojust* tomēr var piekļūt konkrētu kategoriju brīdinājumos ietvertiem datiem, "kas vajadzīgi, lai veiktu savus uzdevumus."

Rezumējot, piekļuvi *SIS* II datiem piešķir trijos gadījumos:

— lai īstenotu brīdinājumu;

— lai sasniegtu mērķi, ko neparedz *SIS* II, bet kas priekšlikumos ir precīzi aprakstīts;

— lai sasniegtu mērķi, ko neparedz *SIS* II, un kas nav precīzi aprakstīts.

EDAU uzskata, ka, jo vispārīgāks ir piekļuves mērķis, jo stingrākiem būtu jābūt īstenojamiem drošības pasākumiem. Vispārēji drošības pasākumi ir turpmāk sīki izklāstīti; pēc tam pievērsīsies konkrētiem apstākļiem, kas attiecas uz Eiropolu un *Eurojust*.

4.2.2. *Piekļuves piešķiršanas nosacījumi*

1. Piekļuvi jebkādā gadījumā var piešķirt tikai, ja tā ir saderīga ar *SIS* II vispārējo mērķi un ir saskaņā ar tās juridisko pamatu.

Tas nozīmē, ka ar piekļuvi imigrācijas datiem saskaņā ar ierosināto regulu praksē ir jāpalīdz īstenot tādu politiku, kas saistīta ar to Šengenas *acquis* daļu, kura attiecas uz personu pārvietošanos.

Līdzīgā kārtā piekļuve brīdinājumiem, kas paredzēti lēmumā, ir domāta, lai atbalstītu policijas un tiesu iestāžu sadarbību krimināllietās.

Šajā sakarā EDAU vērš uzmanību uz nodaļu par reģistrācijas apliecību izdošanas dienestu piekļuvi *SIS* II (skatīt turpmāk, 4.6. punktā).

2. Vajadzība piekļūt *SIS* II datiem, kā arī neiespējamība vai lielas grūtības iegūt datus ar citiem, mazākā līmenī ar iejaukšanos saistītiem līdzekļiem, ir jāpierāda. Tas būtu bijis jādara paskaidrojuma rakstā: kā jau iepriekš minēts, jānožēlo, ka tāds raksts nav iekļauts.

3. Datu lietojums ir jānosaka skaidri un stingri.

Piemēram, patvēruma iestādes var piekļūt imigrācijas datiem "lai noteiktu, vai patvēruma lūdzējs ir nelegāli uzturējies citā dalībvalstī". Eiropols un *Eurojust* tomēr var piekļūt konkrētu kategoriju brīdinājumos ietvertiem datiem, "kas vajadzīgi, lai veiktu savus uzdevumus": tāds formulējums nav pietiekami sīki izvērsts (skatīt turpmāk).

4. Piekļuves nosacījumiem jābūt labi definētiem un stingriem. Konkrēti — piekļuve būtu jāpiešķir tikai šo organizāciju dienestiem, kas izmanto *SIS* II datus. Pienākums, kas noteikts ierosinātā lēmuma 40. pantā un ierosinātās regulas 21.2. pantā, būtu jāpapildina ar pienākumu attiecīgu valstu iestādēm uzturēt atjauninātu tādu personu sarakstu, kam ir tiesības piekļūt *SIS* II. Tas pats būtu jāattiecas uz Eiropolu un *Eurojust*.

5. Tas, ka šīm iestādēm piešķir piekļuvi *SIS* II datiem, nevar būt pamatojums datu ievadīšanai vai uzturēšanai sistēmā, ja tie nav lietderīgi attiecībā uz konkrēto brīdinājumu. Sistēmu nedrīkst papildināt ar jaunu kategoriju datiem tikai tāpēc, ka tie būtu noderīgi citām informācijas sistēmām. Piemēram, ierosinātā lēmuma 39. pantā paredz brīdinājumos iekļaut datus par izdevēju iestādi. Šie dati nav vajadzīgi darbības (arestēšanas, uzraudzības. ..) veikšanai: vienīgais iemesls, kāpēc tos varētu iekļaut sistēmā ir, iespējams, lai veicinātu Eiropola un *Eurojust* darbību. Būtu skaidri jāpamato, kāpēc šādi dati būtu jāapstrādā.

6. Datu uzglabāšanas termiņu nevar paildzināt, ja tas nav jādara, lai sasniegtu datu ievadīšanas mērķi. Tas nozīmē, ka pat, ja Eiropolam un *Eurojust* ir piekļuve šādiem datiem, tāda piekļuve nav pietiekams pamatojums, lai šādus datus uzturētu sistēmā (piemēram, tiklīdz meklēta persona ir izdota, dati būtu jāizdzēš, pat ja tie varētu būt bijuši noderīgi Eiropolam). Arī šajā gadījumā būs vajadzīga uzmanīga uzraudzība, lai nodrošinātu, ka attiecīgu valstu iestādes šo noteikumu piemēro.

4.2.3. *Eiropola un Eurojust piekļuve*

a. *Piekļuves pamatojums*

Eiropola un *Eurojust* piekļuvi dažiem *SIS* datiem jau apsprieda, pirms to ieviesa ar Padomes 2005. gada 24. februāra lēmumu ([1]). No visām iestādēm, kam ir nodrošināta piekļuve savām vajadzībām, tām ir piešķirta piekļuve ar vislabvēlīgākiem nosacījumiem. Lai gan šo datu izmantošana ir aprakstīta lēmuma XII nodaļā, piekļuves piešķiršanas pamatojums nav pietiekami izstrādāts. Vēl jo vairāk tāpēc, ņemot vērā, ka Eiropola un *Eurojust* uzdevumi laika gaitā mainīsies.

EDAU mudina Komisiju ierobežot tādu uzdevumu skaitu, kuru veikšanai Eiropola un *Eurojust* piekļuve būtu pamatota.

b. *Ierobežota piekļuve datiem*

Lai Eiropols un Eurojust neveiktu nepamatotas darbības un lai nodrošinātu, ka tās tikai piekļūtu datiem "savu uzdevumu veikšanai", Šengenas Apvienotā uzraudzības iestāde 2005. gada 27. septembra atzinumā par priekšlikumiem, kas saistīti ar *SIS* II, ieteica ierobežot Eiropola un *Eurojust* piekļuvi datiem par fiziskām personām, kuru vārdi jau ir to rīcībā esošās lietās. Tas garantētu, ka tām būtu pieeja tikai sev būtiskiem brīdinājumiem. EDAU šādu ieteikumu atbalsta.

c. *Drošības aspekti*

EDAU atzinīgi vērtē pienākumu reģistrēt visus ar Eiropolu un *Eurojust* saistītus darījumus, kā arī aizliegumu kopēt vai lejupielādēt sistēmas daļas.

Ierosinātā lēmuma 56. pantā Eiropolam un *Eurojust* paredz "vienu vai divus" piekļuves punktus. Lai cik saprotama arī būtu dalībvalstu vajadzība pēc vairāk par vienu piekļuves punktu, kompetento iestāžu decentralizētības dēļ, Eiropola un *Eurojust* statuss un darbības neattaisno šādas prasības. Arī saistībā ar drošības apsvērumiem jāuzsver, ka piekļuves punktu daudzkāršošana palielina ļaunprātīgas izmantošanas draudus un tādēļ šāda daudzkāršošana būtu jāpamato precīzi, izmantojot konsekventākus elementus. Tādēļ, tā kā nav ticamas argumentācijas, EDAU iesaka Eiropola un Eurojust gadījumā piešķirt tikai vienu piekļuves punktu.

4.3. **Brīdinājumu savstarpēja sasaiste**

Regulas 26. pantā un lēmuma 46. pantā noteikts, ka dalībvalstis var sasaistīt brīdinājumus saskaņā ar saviem tiesību aktiem, lai izveidotu sasaisti starp diviem vai vairākiem brīdinājumiem.

Lai gan brīdinājumu savstarpēja sasaiste var būt noderīga, veicot kontroli (piemēram, orderi apcietināt automašīnu zagli var saistīt ar nozagtu transportlīdzekli), brīdinājumu savstarpēju sasaistīšana ir ļoti raksturīga policijas izmantota izmeklēšanas instrumenta iezīme.

Brīdinājumu sasaistei var būt liela ietekme uz attiecīgās personas tiesībām, jo personu vairs "nenovērtē", pamatojoties uz datiem, kas attiecīgas tikai uz viņu, bet gan uz viņas iespējamām saistībām ar citām personām. Ļoti iespējams, ka pret fiziskām personām, kuru dati ir saistīti ar noziedznieku datiem, izturēsies ar lielākām aizdomām. Brīdinājumu savstarpēja sasaiste turklāt atspoguļo *SIS* ar izmeklēšanu saistītu aspekta stiprināšanu, jo šāda sasaiste padarīs iespējamu bandu vai tīklu reģistrāciju (ja, piemēram, dati par nelikumīgiem imigrantiem ir saistīti ar datiem par pārvadātājiem). Visbeidzot, tā kā sasaisti nosaka attiecīgu valstu tiesību aktos, saites, kas ir nelikumīgas vienā dalībvalstī, var izveidot cita dalībvalsts, tādējādi sistēmā ievadot "nelikumīgus" datus.

([1]) Padomes Lēmums 2005/211/TI (2005. gada 24. februāris) par dažu jaunu Šengenas Informācijas sistēmas funkciju ieviešanu, tostarp terorisma apkarošanas jomā, OV L 68/44, 15.3.2005.

Padomes 2004. gada 14. jūnija secinājumos par *SIS* II funkcionālām prasībām minēts, ka katrai saitei jānosaka skaidras darbības prasības, ir jābūt pamatotai uz skaidri definētām attiecībām un jāatbilst proporcionalitātes principam. Turklāt tā nedrīkst skart tiesības uz piekļuvi. Katrā ziņā, tā kā brīdinājumu savstarpēja sasaiste ir apstrādes darbība, tai ir jāatbilst attiecīgas valsts tiesību aktu noteikumiem, ar ko īsteno Direktīvu 95/46/EK un/vai Konvenciju Nr. 108.

Priekšlikumos atkārtoti apliecināts, ka saišu pastāvēšana nevar mainīt tiesības uz piekļuvi (patiesi, saite citādāk dotu piekļuvi datiem, kuru apstrāde būtu nelikumīga saskaņā ar attiecīgas valsts tiesību aktiem, tādējādi pārkāpjot direktīvas 6. pantu).

EDAU uzsver, cik svarīgi ir šauri interpretēt ierosinātās regulas 26. pantu un ierosinātā lēmuma 46. pantu: viens paņēmiens, kā šo var nodrošināt, ir skaidri paziņot, ka iestādes, kam nav tiesību piekļūt konkrētu kategoriju datiem, ne vien nevar piekļūt saitēm uz šādām kategorijām, bet tām pat nevajadzētu zināt, ka šādas saites pastāv. Ja nav tiesību piekļūt saistītajiem datiem, saišu vizualizācijai jābūt neiespējamai.

Turklāt EDAU vēlētos, lai ar viņu apspriestos par tehniskiem pasākumiem, lai šo nodrošinātu.

4.4. **Brīdinājumi ar mērķi liegt ieceļošanu**

4.4.1. *Pamats iekļaušanai*

"Brīdinājumu attiecībā uz trešo valstu valstspiederīgajiem nolūkā atteikt ieceļošanu" izmantošanai (regulas 15. pants) ir ievērojama ietekme uz privātpersonas brīvībām: personai, par kuru ir ziņots saskaņā ar šo noteikumu, uz vairākiem gadiem ir liegta piekļuve Šengenas telpai. Līdz šim tas bijis visbiežāk lietotais brīdinājums, vērtējot pēc to personu skaita, par kurām ziņots. Redzot šā brīdinājuma sekas, kā arī ietekmēto personu skaitu, ir jārīkojas ļoti uzmanīgi, izstrādājot tā koncepciju, kā arī īstenojot to. Kaut gan tas attiecas arī uz citiem brīdinājumiem, EDAU veltīs atsevišķu nodaļu šim brīdinājumam, jo tas izraisa īpašas problēmas attiecībā uz iekļaušanas pamatojumu.

Jaunais brīdinājums ieceļošanas aizliegumam nozīmē uzlabojumu salīdzinājumā ar pašreizējo stāvokli, tomēr arī tas nav pilnībā apmierinošs, jo lielā mērā ir balstīts uz instrumentiem, kuri vēl nav pieņemti vai pat ierosināti.

Uzlabojumi izpaužas kā precīzāks pamatojumu apraksts datu iekļaušanai. Pašreizējā Šengenas konvencijas formulējuma rezultātā ir radies tāds stāvoklis, ka pastāvēja ievērojamas atšķirības dalībvalstu starpā attiecībā uz personu skaitu, par kurām ziņoja saskaņā ar konvencijas 96. pantu. Šengenas apvienotā uzraudzības iestāde ir veikusi visaptverošu pētījumu [1] par šo jautājumu un nāca klajā ar ierosinājumiem, ka "politikas veidotājiem būtu jāapsver iemeslu saskaņošana brīdinājumu izveidei dažādās Šengenas valstīs".

Ierosinātā 15. panta formulējums ir sīkāk izstrādāts, kas ir apsveicami.

Turklāt 15. panta 2. punktā ir sniegts arī gadījumu saraksts, kad, piemērojot dažādus statusus, par personām nedrīkst izdot brīdinājumus, jo viņi likumīgi dzīvo kādas dalībvalsts teritorijā. Kaut gan tas izrietēja no pašreizējās Šengenas konvencijas, prakse parādījusi, ka arī šo mehānismu dažādās dalībvalstīs piemēroja dažādi. Tādēļ skaidrības ieviešana ir pozitīvs aspekts.

Tomēr šis noteikums ir arī nopietni kritizēts, jo tas ievērojamā mērā balstīts uz dokumentu, kurš vēl nav pieņemts, proti uz direktīvu "par nogādi atpakaļ".

Kopš *SIS* II priekšlikumu pieņemšanas Komisija (2005. gada 1. septembrī) ierosinājusi direktīvu par dalībvalstu kopīgiem standartiem un procedūrām, pēc kuriem nogādā atpakaļ trešo valstu valstspiederīgos, kuri nelegāli uzturas teritorijā, taču, tā kā šī nav galīgā dokumenta versija, to nevar uzskatīt par likumīgu pamatu datu ievadīšanai sistēmā. Tas jo īpaši nozīmē Eiropas Padomes Cilvēktiesību konvencijas 8. panta pārkāpumu, jo iejaukšanos personu privātajā dzīvē būtu jāpamato ar — *inter alia* — skaidriem un pieejamiem tiesību aktiem.

Tādēļ EDAU mudina Komisiju vai nu atcelt šo noteikumu, vai izstrādāt jaunu formulējumu, balstoties uz esošajiem tiesību aktiem, kas ļautu personām zināt, tieši kādus pasākumus iestādes var pieņemt attiecībā uz tām.

4.4.2. *Piekļuve 15. panta brīdinājumiem*

18. pantā ir noteikts, kurām iestādēm šie brīdinājumi ir pieejami un — kādiem mērķiem. 18. panta 1. un 2. punktā ir noteikts, kurām iestādēm ir pieejami brīdinājumi, kuri ievadīti, balstoties uz direktīvu par nogādi atpakaļ. Arī uz šo gadījumu attiecas iepriekš minētais komentārs.

[1] Šengenas kopīgās uzraudzības iestādes ziņojums par 96. panta brīdinājumu izmantošanu Šengenas Informācijas sistēmā, Brisele, 2005. gada 20. jūnijs

Regulas priekšlikuma 18. panta 3. punktā ir dota piekļuve iestādēm, kuras atbildīgas par bēgļa statusa piešķiršanu, saskaņā ar direktīvu, kura vēl nav pat ierosināta. Tā kā dokuments nav pieejams, EDAU jāatkārto iepriekš minētie komentāri.

4.4.3. *15. panta brīdinājumu uzglabāšanas ilgums*

Atbilstīgi 20. pantam brīdinājumus nedrīkst glabāt ilgāk par ieceļošanas atteikuma termiņu, kurš noteikts lēmumā (par izraidīšanu vai nosūtīšanu atpakaļ). Tas ir atbilstīgi datu aizsardzības noteikumiem. Turklāt pēc pieciem gadiem tos izdzēsīs automātiski, ja vien dalībvalsts, kura ievadījusi datus *SIS* II, nepieņems citādu lēmumu.

Pienācīgai uzraudzībai valstu mērogā būtu jānodrošina, ka nenotiek automātiska nepamatota uzglabāšanas termiņa pagarināšana un ka dalībvalstis izdzēš datus pirms piecu gadu termiņa gadījumos, kad ieceļošanas atteikuma termiņš ir īsāks.

4.5. **Uzglabāšanas laikposmi**

Kaut gan uzglabāšanas princips saglabājas nemainīgs (parasti brīdinājums būtu jāizdzēš no *SIS* II, tiklīdz paveikta brīdinājumā prasītā darbība), priekšlikumu rezultātā brīdinājumu uzglabāšanas termiņš kopumā pagarināsies.

Šengenas konvencijā bija noteikts, ka ne vēlāk kā trīs gadus pēc datu ievades (vai vienu gadu — ja dati ievadīti diskrētai novērošanai) jāpārskata pastāvīgas uzglabāšanas vajadzība. Jaunajos priekšlikumos paredzēta automātiska dzēšana (paredzot izdevējai dalībvalstij iespēju iebilst) pēc 5 gadiem — imigrācijas datiem, pēc 10 gadiem — datiem par arestu, pazudušām personām un personām, kuras meklē saistībā ar tiesas procedūrām, un pēc 3 gadiem — personām, kurām jāpiemēro diskrēta novērošana.

Kaut gan principā dalībvalstīm būs jādzēš dati pēc tam, kad brīdinājuma mērķis būs panākts, tas izraisa ievērojamu maksimālā uzglabāšanas laikposma pieaugumu (vairumā gadījumu — trīskārtīgu) bez jebkāda pamatojuma no Komisijas puses. Imigrācijas datu gadījumā var tikai izteikt minējumu, ka 5 gadu termiņš ir saistīts ar ieceļošanas aizlieguma ilgumu, kas ierosināts projektā direktīvai par nosūtīšanu atpakaļ. Visos pārējos gadījumos nav loģiska pamatojuma, kas EDAU būtu zināms.

Iespējamā ietekme uz datu subjektiem, par kuriem ziņo SIS, var radīt ievērojamas sekas attiecīgo personu dzīvē. Tas ir īpaši uztraucoši saistībā ar brīdinājumiem par personām, kuras pakļauj diskrētai novērošanai vai konkrētām pārbaudēm, jo šos brīdinājumus var izdot, balstoties uz aizdomām.

EDAU gribētu redzēt nopietnu pamatojumu šim datu uzglabāšanas laikposma pagarinājumam. Ja nav pārliecinoša pamatojuma, viņš ierosina samazināt tos līdz to pašreizējam ilgumam, jo īpaši attiecībā uz brīdinājumiem, lai veiktu diskrētus novērojumus vai konkrētas pārbaudes.

4.6. **Par transportlīdzekļu reģistrācijas apliecību izdošanu atbildīgo iestāžu piekļuve**

Galvenais jautājums ir par vairāk kā apšaubāma juridiskā pamata izvēli. Komisijai nav izdevies pārliecinoši pamatot, kādēļ jāizmanto pirmā pīlāra "transporta" juridiskā bāze pasākumam, kurš administratīvajām iestādēm dotu iespēju piekļūt *SIS* noziedzības (zagtu automašīnu tirdzniecības) novēršanas un apkarošanas nolūkā. Vajadzība pēc stingra pamatojuma un stabilas juridiskās bāzes, lai piešķirtu piekļuvi *SIS* II, tika detalizēti izklāstīta šā atzinuma 4.2.2. punktā.

EDAU atsaucas uz komentāriem par šo tēmu, ko sniedza Šengenas apvienotā uzraudzības iestāde savā atzinumā par ierosināto juridisko bāzi *SIS* II. Jo īpaši jāievēro Šengenas apvienotās uzraudzības iestādes ierosinājums grozīt ierosināto lēmumu, iekļaujot tajā šo piekļuvi.

5. KOMISIJAS UN DALĪBVALSTU FUNKCIJAS

Saistībā ar *SIS* II sevišķi svarīgs ir precīzs pienākumu apraksts un sadalījums — ne vien sistēmas veiksmīgai darbībai, bet arī no uzraudzības viedokļa. Uzraudzības pienākumu sadale izrietēs no pienākumu apraksta, tādēļ vajadzīga pilnīga skaidrība.

5.1. **Komisijas funkcijas**

EDAU pauž gandarījumu par abu priekšlikumu III nodaļu, kurā aprakstītas Komisijas funkcijas un pienākumi saistībā ar *SIS* II ("operatīvās vadības" funkcijas). Vīzu informācijas sistēmas (VIS) priekšlikumā šādas precizitātes nebija. Tomēr tikai ar šo nodaļu vien Komisijas funkcijas nav visaptveroši noteiktas. Patiesi, kā iztirzāts šā atzinuma 9. nodaļā, Komisija ir iesaistīta arī sistēmas īstenošanas un vadības procesā ar komitoloģijas procedūras starpniecību.

Datu aizsardzības ziņā Komisijai ir funkcijas, kas minētas jau VIS un *Eurodac* sistēmās, proti, atbildība par operatīvo vadību. Ņemot vērā arī tās lielo nozīmi sistēmas izstrādē un uzturēšanā, to būtu jāuzskata par *sui generis* kontrolieri. Kā minēts jau EDAU atzinumā par VIS, Komisija ir daudz vairāk nekā datu apstrādātājs, bet tās uzdevumi ir ierobežotāki par parastā kontroliera uzdevumiem, jo Komisija nevar piekļūt *SIS* II apstrādātiem datiem.

Tā kā *SIS* II izveidos, pamatojoties uz sarežģītām sistēmām, no kurām dažas balstās uz topošām tehnoloģijām, EDAU uzstāj, ka jānostiprina Komisijas atbildība par sistēmu atjaunināšanu, īstenojot vislabākās pieejamās tehnoloģijas drošības un datu aizsardzības jomā.

Tādēļ abu priekšlikumu 12. pantā būtu jāparedz, ka Komisijai būtu regulāri jāierosina tādu jaunu tehnoloģiju īstenošana, kas atspoguļo tehnisko sasniegumu līmeni attiecīgajā jomā un kas uzlabos datu aizsardzību un drošību, kā arī atvieglos to valstu iestāžu uzdevumus, kurām ir piekļuve šiem datiem.

5.2. **Dalībvalstu funkcijas**

Dalībvalstu stāvoklis faktiski nav skaidrs, jo ir diezgan grūti noteikt, kura(s) iestāde(s) būs datu kontrolieri(s).

Priekšlikumos ir aprakstītas *SIS* II valsts biroja funkcijas (nodrošināt kompetento iestāžu piekļuvi *SIS* II), kā arī *SIRENE* iestāžu funkcijas (nodrošināt apmaiņu ar visu papildu informāciju). Dalībvalstīm ir arī jānodrošina savu "VS" ("valstu sistēmu") darbība un drošība. Nav skaidrs, vai par šo pēdējo pienākumu atbildība jāuzņemas kādai no iepriekš minētajām iestādēm. Jebkurā gadījumā šajā jautājumā jāievieš skaidrība.

Runājot par datu aizsardzību, Komisiju un dalībvalstis būtu jāuzskata par saistītiem kontrolieriem, kuriem katram ir sava konkrēta atbildības joma. Šo papildinošo misiju atzīšana ir vienīgais veids, kā panākt, lai neviena no *SIS* II darbības jomām nepaliktu neuzraudzīta.

6. **DATU SUBJEKTU TIESĪBAS**

6.1. **Informācija**

6.1.1. *Ierosinātā regula*

Ierosinātās regulas 28. pantā noteiktas datu subjektu tiesības uz informāciju, galvenokārt ņemot vērā Direktīvas 95/46 10. pantu. Tās ir ļoti patīkamas izmaiņas salīdzinājumā ar pašreizējo situāciju, kad Konvencijā nav skaidri noteiktas tiesības uz informāciju. Taču vēl aizvien ir iespējami uzlabojumi šādos jautājumos.

Sarakstam būtu jāpievieno informācija, jo tas palīdzētu nodrošināt taisnīgu attieksmi pret datu subjektu ([1]). Minētajai informācijai būtu jāattiecas uz datu glabāšanas laiku; to, vai subjektam ir tiesības lūgt pārskatīt vai iesniegt apelāciju pret lēmumu izdarīt brīdinājumu (dažos gadījumos skatīt ierosinātās regulas 15. panta 3. punktu); to, vai var saņemt palīdzību no datu aizsardzības iestādes, un to, vai ir aizsardzības līdzekļi.

Ierosinātajā regulā nav nekādu norāžu uz brīdi, kad informācija būtu jāsniedz. Tas varētu radīt šķēršļus datu subjekta tiesību realizēšanai. Lai iedzīvinātu minētās tiesības, Regulā ir jānosaka precīzs brīdis, kad informācija būtu jāsniedz, atkarībā no iestādes, kas izsniedz brīdinājumu.

Praktisks risinājums būtu pievienot informāciju par brīdinājumu lēmumam, kas ir brīdinājuma pamatā: tiesas vai administratīvs lēmums, kas balstās uz sabiedriskās kārtības apdraudējumu (…) vai lēmumu par nosūtīšanu atpakaļ, vai izraidīšanas rīkojumu, kas papildināts ar atgriešanās aizliegumu. Tas būtu jāpievieno Regulas 28. pantam.

6.1.2. *Ierosinātais lēmums*

Lēmuma 50. pantā noteikts, ka informāciju sniedz pēc datu subjekta pieprasījuma, un norādīti iespējamie iemesli minētās informācijas nesniegšanai. Ierobežojumi šajā sakarā ir skaidri saprotami, ņemot vērā to, kādi ir šie dati un kā tos apstrādā.

Tomēr tiesībām uz informāciju nevajadzētu kā nosacījumu izvirzīt datu subjekta pieprasījumu (tā drīzāk būtu definīcija par piekļuves lūgumu). Var pieņemt, ka vajadzība "pieprasīt" informāciju ir attaisnojama tajos gadījumos, kad datu subjektu nevar informēt, jo viņu nevar atrast.

Šo problēmu varētu veiksmīgāk risināt tiesībām uz informāciju pievienojot izņēmumu gadījumos, kad nav iespējams sniegt informāciju vai tas ir saistīts ar nesamērīgi lielām pūlēm. Lēmuma 50. pants būtu atbilstīgi jāgroza.

([1]) Tāpat skatīt EDAU atzinuma par Vīzu informācijas sistēmas izveidi 3.10.1. punktu.

Šāds risinājums atbilstu arī pamatlēmuma par datu aizsardzību trešajā pīlārā piemērošanai.

6.2. **Piekļuve**

Pozitīvas izmaiņas ir tās, ka gan ierosinātajā regulā, gan ierosinātajā lēmumā ir noteikti termiņi, kuros atbildēt uz piekļuves lūgumiem. Ņemot vērā, ka procedūra piekļuves tiesību izmantošanai ir noteikta valsts līmenī, var rasties jautājums, kā priekšlikumos noteiktie termiņi varēs mijiedarboties ar pastāvošajām procedūrām, jo īpaši ja dalībvalstīm ir daudz īsāki termiņi, kuros atbildēt uz piekļuves lūgumiem. Būtu skaidri jānosaka, ka jāizmanto tie termiņi, kas ir vislabvēlīgākie datu subjektam.

6.2.1. *Ierosinātā regula*

Ir vērts pieminēt, ka ierosinātajā regulā neparādās pašlaik Šengenas konvencijā esošie ierobežojumi piekļuves tiesībām ("atsaka, ja tas ir pilnīgi nepieciešams likumīga uzdevuma izpildē saistībā ar brīdinājumu vai konkrētās personas vai trešo personu tiesību un brīvību aizsardzību").

Tas visticamāk ir saistīts ar Direktīvas 95/46/EK piemērošanu, kurā noteikta (13. pantā) iespēja valstu tiesību aktos īstenot izņēmumus. Jebkurā gadījumā būtu jānorāda, ka 13. panta izmantošana valstu tiesību aktos, lai ierobežotu piekļuves tiesības, vienmēr būtu jāsaskaņo ar ECK 8. pantu, un tā pieļaujama tikai atsevišķos gadījumos.

6.2.2. *Ierosinātais lēmums*

Ierosinātajā lēmumā izmantoti Šengenas konvencijā noteiktie piekļuves tiesību ierobežojumi. Ierosinātajā pamatlēmumā pēc būtības iekļauti tādi paši piekļuves tiesību ierobežojumi, tādēļ attiecībā uz šo jautājumu minētā instrumenta pieņemšanai nebūtu būtiskas nozīmes.

Tā kā vairākās dalībvalstīs pieeja tiesību īstenošanas datiem ir "netieša" (tas nozīmē, ka to īsteno ar valsts datu aizsardzības iestādes palīdzību), būtu lietderīgi padarīt par datu aizsardzības iestāžu pienākumu aktīvi sadarboties piekļuves tiesību īstenošanā.

6.3. **Tiesības pārskatīt vai iesniegt apelāciju pret lēmumu izdarīt brīdinājumu**

Regulas 15. panta 3. punktā noteiktas tiesības pārskatīt vai iesniegt apelāciju tiesu iestādē attiecībā uz lēmumu izdarīt brīdinājumu gadījumā, ja šo lēmumu pieņēmusi administratīva iestāde. Salīdzinājumā ar Šengenas konvenciju tas ir patīkams papildinājums.

Tas uzsver vajadzību pilnībā un laicīgi informēt datu subjektu, kā tas minēts 6.1 punktā: bez šīs informācijas jaunās tiesības paliktu tikai teorētiskā līmenī.

6.4. **Tiesiskās aizsardzības līdzekļi**

Ierosinātās regulas 30. pantā un ierosinātā lēmuma 52. pantā noteiktas tiesības iesniegt prasību vai apelāciju attiecīgās dalībvalsts tiesās, ja datu subjektam ir atteiktas tiesības piekļūt datiem, tos labot vai dzēst, vai tiesības iegūt informāciju vai saņemt kompensāciju.

Formulējums ("jebkurai personai dalībvalstu teritorijā") liek domāt, ka sūdzības iesniedzējam fiziski jāatrodas attiecīgajā teritorijā, lai iesniegtu savu prasību tiesā. Šāds teritoriālais ierobežojums nav attaisnojams un varētu padarīt tiesības uz tiesiskās aizsardzības līdzekļiem par nefunkcionējošām, jo vairumā gadījumu sūdzības iesniedzējs iesniegs savu lietu tieši tāpēc, ka viņam nav ļauta pieeja Šengena teritorijai. Turklāt tā kā Direktīva ir *lex generalis*, tās 22. pants jāņem vērā attiecībā uz ierosināto regulu; tajā noteikts, ka "ikvienam" ir tiesības uz tiesiskās aizsardzības līdzekļiem, neatkarīgi no viņa dzīvesvietas. Arī ierosinātajā pamatlēmumā nav tāda teritoriāla ierobežojuma. EDAU ierosina svītrot teritoriālos ierobežojumus 30. un 52. pantā.

7. PĀRRAUDZĪBA

7.1. **Ievada piezīmes: pienākumu sadalījums**

Priekšlikumos pienākumi saistībā ar uzraudzību ir sadalīti starp valsts uzraudzības iestādēm [1] un EDAU, katram savā jomā. Tas sader ar priekšlikumos izmantoto pieeju spēkā esošiem tiesību aktiem un pienākumiem, kas saistīti ar *SIS* II darbību un izmantojumu, un ar vajadzību pēc efektīvas uzraudzības.

Tādēļ EDAU pauž gandarījumu par šo pieeju, kas izmantota ierosinātās regulas 31. pantā un ierosinātā lēmuma 53. pantā. Taču labākas izpratnes un attiecīgo uzdevumu precizēšanas labad EDAU ierosina sadalīt katru pantu vairākos noteikumos, katru veltot konkrētam uzraudzības līmenim, kā tas bija pareizi izdarīts Vīzu informācijas sistēmas projektā.

[1] Eiropola un *Eurojust* pārbaudes iestādes arī ir iesaistītas, tikai mazākā mērā.

7.2. **Valstu datu aizsardzības iestāžu veiktā uzraudzība**

Saskaņā ar ierosinātās regulas 31. pantu un ierosinātā lēmuma 53. pantu katrai dalībvalstij jāgarantē, ka neatkarīga iestāde uzrauga *SIS* II personas datu apstrādes likumību.

Ierosinātā lēmuma 53. pantā papildus paredzētas indivīda tiesības prasīt uzraudzības iestādei pārbaudīt to datu apstrādes likumību, kuri uz to attiecas. Tā kā Direktīvu piemēro kā *lex generalis*, tad līdzīgs noteikums ierosinātajā regulā nav iekļauts. Tādēļ jāuzskata, ka attiecībā uz *SIS* II valstu datu aizsardzības iestādes var īstenot visas pilnvaras, kas tām piešķirtas saskaņā ar Direktīvas 95/46/EK 28. pantu, tostarp pārbaudīt datu apstrādes likumību. Regulas 31.1 pantā ir precizēts to uzdevums, bet tas nevar būt šo pilnvaru ierobežojums. Minētās pilnvaru robežas būtu jāprecizē ierosinātajā regulā.

Runājot par ierosināto lēmumu, tajā atzīti vairāk pienākumu valsts uzraudzības iestādēm, jo tā *lex generalis* ir savādāks. Taču situācija, kad atkarībā no apstrādāto datu kategorijas uzraudzības iestādēm būtu citādāks uzdevums un pilnvaras, nav saprātīga un praksē ļoti grūti pārvaldāma. Tādēļ no tā būtu jāizvairās, vai nu piešķirot iestādēm vienādas pilnvaras pašā ierosinātā lēmuma tekstā, vai arī atsaucoties uz citu *lex generalis* (proti, uz pamatlēmumu par datu aizsardzību trešajā pīlārā), paplašinot datu aizsardzības iestāžu pilnvaras.

7.3. **EDAU veiktā uzraudzība**

EDAU uzrauga to, vai datu apstrāde Komisijā notiek saskaņā ar priekšlikumiem. Līdzīgi EDAU vajadzētu būt iespējai īstenot visas saskaņā ar Regulu 45/2001 piešķirtās pilnvaras, tomēr ņemot vērā, cik ierobežotas ir Komisijas pilnvaras attiecībā uz pašiem datiem.

Ir vērts piebilst, ka saskaņā ar Regulas 45/2001 46. panta f) punktu EDAU "sadarbojas ar valsts uzraudzības iestādēm, ciktāl tas nepieciešams to attiecīgo pienākumu izpildei". Sadarbība ar dalībvalstīm, uzraugot *SIS* II, neizriet tikai no priekšlikumiem, bet arī no Regulas 45/2001.

7.4. **Kopēja uzraudzība**

Priekšlikumos arī atzīta vajadzība koordinēt dažādo iesaistīto iestāžu uzraudzības darbības. Ierosinātās regulas 31. pantā un ierosinātā lēmuma 53. pantā noteikts, ka "valstu uzraudzības iestādes un Eiropas Datu aizsardzības uzraudzītājs savstarpēji aktīvi sadarbojas. Šajā nolūkā Eiropas Datu aizsardzības uzraudzītājs vismaz vienu reizi gadā sasauc sanāksmi."

EDAU pauž gandarījumu par to, ka priekšlikumos būtībā ir ietverti visi aspekti, kas vajadzīgi, lai izveidotu attiecīgu valstu un Eiropas līmeņa uzraudzības iestāžu sadarbību, kas ir patiesi svarīgi. Būtu jāuzsver, ka priekšlikumos ir noteikta vismaz viena sanāksme gadā, bet tas būtu uzskatāms par obligātu prasību.

Šajos pantos (ierosinātās regulas 31. pantā un ierosinātā lēmuma 53. pantā) tomēr vajadzētu precizēt minētās koordinācijas saturu. Esošās Apvienotā uzraudzības iestādes pilnvarās ietilpst izpētīt grūtības saistībā ar Konvencijas piemērošanu vai interpretēšanu, pētīt problēmas, kas varētu rasties veicot neatkarīgu uzraudzību vai saistībā ar piekļuves tiesībām, kā arī izstrādāt saskaņotus priekšlikumus kopīgiem esošo problēmu risinājumiem.

Jaunajiem priekšlikumiem nevajadzētu sajaukt esošo kopējās kontroles sfēru. Ja ir skaidrs, ka datu aizsardzības iestādes attiecībā uz *SIS* II var izmantot visas savas uzraudzītāja pilnvaras, kas tām ir piešķirtas Direktīvā, tad sadarbība šo iestāžu starpā var attiekties uz plašāku sfēru saistībā *SIS* II uzraudzību, tostarp uz esošās Apvienotās uzraudzības iestādes uzdevumiem, kas noteikti Šengenas konvencijas 115. pantā.

Tomēr, lai tas būtu pilnīgi skaidrs, būtu lietderīgi to vēlreiz nepārprotami uzsvērt priekšlikumos.

8. **DROŠĪBA**

SIS II pārvaldība un optimāla aizsardzības līmeņa ievērošana ir pamatprasība, lai nodrošinātu datubāzē uzglabāto personas datu piemērotu aizsardzību. Lai panāktu pietiekama līmeņa aizsardzību, ir jāievieš pareizi aizsardzības pasākumi, lai novērstu iespējamus draudus, kas ir saistīti ar sistēmas infrastruktūru un iesaistītajām personām. Šis temats ir iztirzāts dažādās priekšlikuma daļās, un tajā būtu jāveic daži uzlabojumi.

Priekšlikuma 10. un 13. pantā ir noteikti dažādi datu drošības pasākumi un konkrēti norādīts, kāds to nepareizs lietojums būtu jānovērš. EDAU atzinīgi vērtē šajos pantos iekļautos noteikumus par drošības pasākumu metodisku (paš)revīziju.

Ierosinātā lēmuma 59. pantam un ierosinātas regulas 34. pantam, kurā ir noteikta uzraudzība un izvērtēšana, tomēr nevajadzētu attiekties tikai uz ražīgumu, rentabilitāti un pakalpojumu kvalitāti, bet arī uz atbilstību juridiskām prasībām, jo īpaši datu aizsardzības jomā. Tādēļ EDAU iesaka paplašināt šo pantu darbības jomu un attiecināt to arī uz apstrādes likumīguma uzraudzību un ziņojumiem par tās likumību.

Turklāt, papildinot ierosinātā lēmuma 10. panta 1. punkta c) apakšpunktu vai 18. panta 17. punkta e) apakšpunktu un ierosinātās regulas 17. pantu, kas attiecas uz atbilstīgi pilnvarotu personālu, kam ir dota pieeja datiem, būtu jāpiebilst, ka dalībvalstīm (kā arī Eiropolam un *Eurojust*) vajadzētu nodrošināt to, ka ir pieejami precīzi lietotāju profili (kas būtu jātur attiecīgu valstu kontroles iestāžu rīcībā pārbaudes vajadzībām). Dalībvalstīm līdztekus lietotāju profiliem ir jāsastāda un visu laiku jāatjaunina pilnīgs saraksts ar lietotāju identitātes datiem. Tas pats attiecas *mutatis mutandis* uz Komisiju.

Šos drošības pasākumus papildina ar pārraudzības un organizatoriskiem drošības pasākumiem. Priekšlikumu 14. pantā ir aprakstīti nosacījumi, un mērķi visu datu apstrādes operāciju reģistra uzturēšanai. Reģistra datus glabā ne tikai, lai pārraudzītu datu aizsardzību un garantētu datu drošību, bet arī, lai veicinātu regulāru *SIS* II pašrevīziju, ko prasa 10. pantā. Pašrevīzijas ziņojumi palīdzēs uzraudzības iestādēm efektīvi veikt savus uzdevumus, kas spēs atklāt vājākos punktus un tiem pievērsties savā revīzijas procedūrā.

Kā jau tas iepriekš minēts šajā atzinumā, sistēmu piekļuves punktu daudzkāršošana būtu pienācīgi jāpamato, jo tā automātiski palielina ļaunprātīgas izmantošanas draudus. Tādēļ priekšlikumu 4. panta 1. punkta b) apakšpunktā būtu konkrēti jāpieprasa demonstrēt vajadzību pēc otra piekļuves punkta.

Priekšlikumos nav skaidri paskaidrota vajadzība pēc centrālās sistēmas valstu eksemplāriem un tas rada nopietnas bažas par vispārējo riska un drošības līmeni sistēmā, piemēram:

— eksemplāru daudzkāršošana palielina ļaunprātīgas izmantošanas risku (jo īpaši ņemot vērā jaunu datu veidu esamību, piemēram biometrijas datu esamību);

— ar šiem eksemplāriem saistītie dati nav precīzi definēti;

— 9. pantā norādītās precizitātes, kvalitātes un pieejamības prasības izraisa lielas tehniskas problēmas un tādējādi palielina izmaksas, ņemot vērā jaunākos sasniegumus pieejamajā tehnoloģijā;

— lai minēto eksemplāru uzraudzību veiktu valstu iestādes, tām būs vajadzīgi papildu cilvēku un finansiālie resursi, kas nevienmēr var būt pieejami.

Saistībā ar iespējamajiem riskiem, EDAU nav pārliecināts ne par to, ka valstu eksemplāri ir jāizmanto (ņemot vērā pieejamās tehnoloģijas), ne arī par šo eksemplāru izmantošanas sniegto papildu vērtību. Viņš iesaka atcelt iespēju dalībvalstīm izmantot valstu eksemplārus.

Ja valstu eksemplārus tomēr izstrādā, EDAU atgādina, ka jāpiemēro strikts izmantošanas mērķu ierobežojuma princips attiecībā uz to izmantošanu attiecīgās valstīs. Līdzīgi būtu nosaka, ka var veikt meklējumus attiecīgas valsts eksemplārā, tikai izmantojot centralizēto datubāzi.

Personas datu apstrādes darbības likumība pamatojas uz striktu datu drošības un integritātes ievērošanu. EDAU efektīvi uzraudzīs šos procesus, ja viņš varēs ne tikai uzraudzīt datu drošību, bet arī integritāti, pārbaudot pieejamos reģistrus. Tādēļ ir jāpievieno vārdi "datu integritāte" 14. panta 6. punktā.

9. **KOMITOLOĢIJA**

Priekšlikumos vairākkārt paredzētas komitoloģijas procedūras, ja ir jāpieņem ar tehnoloģiju saistīti lēmumi, īstenojot vai pārvaldot *SIS* II. Kā līdzīgu iemeslu dēļ minēts atzinumā par VIS, šādiem lēmumiem būs liela ietekme uz mērķa un proporcionalitātes principa pareizu īstenošanu.

EDAU iesaka, lai lēmumi, kas būtiski ietekmē datu aizsardzību, piemēram, lēmumi par piekļuvi datiem un datu ievadīšanai, apmainīšanos ar papildinformāciju, datu kvalitāti un brīdinājumu savstarpēju saderību, valstu eksemplāru tehnisko atbilstību utt., būtu jāpieņem, pieņemot regulu vai direktīvu, ieteicams — īstenojot koplēmuma procedūru ([1]).

([1]) Tajā pašā sakarā skatīt EDAU Atzinuma par Vīzu informācijas sistēmu 3.12. punktu un 60. punktu EDAU 2005. gada 26. septembra Atzinumā par priekšlikumu direktīvai par datu saglabāšanu, kuri apstrādāti saistībā ar publisko elektronisko sakaru pakalpojumu sniegšanu.

Visos citos gadījumos, kas iespaido datu aizsardzību, EDAU būtu jādod iespēja dot padomus šīm komitejām, izdarot izvēli.

EDAU padomdevēja uzdevumi būtu jāparedz lēmuma 60. un 61. pantā un regulas 35. pantā.

Attiecībā uz konkrētāku gadījumu — tehniskiem noteikumiem par brīdinājumu sasaisti (regulas 26. pants un lēmuma 46. pants) — jāizskaidro vajadzība paredzēt atšķirīgus komitoloģijas režīmus (lēmumā — padomdevēja režīms, bet regulā — regulatīvais režīms).

10. **SAVSTARPĒJA SAVIETOJAMĪBA**

Tā kā Komisijas paziņojuma par topošu ES sistēmu savstarpēju savietojamību joprojām trūkst, ir grūti pareizi izvērtēt paredzēto, bet vēl nedefinēto sinerģiju papildu vērtību.

Tādā sakarā EDAU 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 (*SIS*, 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 pārvaldību (skat. arī šā atzinuma 3.8. punktu).

EDAU atzinumā par Vīzu informācijas sistēmu jau ir minējis, ka savstarpēja savietojamība ir ārkārtīgi svarīga un būtiska prasība, lai nodrošinātu tādu liela apjoma IT sistēmu efektivitāti, kāds ir *SIS* II. Tas ļauj konsekventi mazināt kopējās izmaksas un izvairīties no dabiskas nesaskanīgu elementu redudances.

— Savstarpēja savietojamība var arī palīdzēt sasniegt mērķi uzturēt augsta līmeņa aizsardzību teritorijā, kurā neveic robežkontroli uz dalībvalstu iekšējām robežām, piemērojot vienu un to pašu procesuālo standartu visiem šīs politikas elementiem. Turklāt būtiski svarīgi ir nošķirt divu līmeņu savstarpēju savietojamību:

  — Savstarpēja ES dalībvalstu savietojamība ir visnotaļ vēlama; patiesi, brīdinājumam, ko sūta vienas dalībvalsts iestādes, jābūt savietojamiem ar brīdinājumiem, ko sūta visu citu dalībvalstu iestādes.

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

Viens no drošības pasākumiem, 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. Ciktāl iespējams noskaidrot, lasot priekšlikumus, šķiet, piemēram, Automātiska pirkstu nospiedumu identifikācijas sistēma (*AFIS*) nedarbosies pirmajos *SIS* II darbības gados; ir tikai minēta paredzēta biometrijas datu meklētājprogramma. Ja paredz izmantot *AFIS*, kas pieder citai ES sistēmai, tas būtu skaidri jānorāda dokumentā, paredzot arī šādām sinerģijām vajadzīgos drošības pasākumus.

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

11. **SECINĀJUMU KOPSAVILKUMS**

11.1. **Vispārēji jautājumi**

1. EDAU atzinīgi vērtē vairākus šo priekšlikumu pozitīvos aspektus, kas attiecībā uz dažiem jautājumiem un salīdzinājumā ar pašreizējo stāvokli ir uzlabojums. Viņš ņem vēra, ka noteikumi par datu aizsardzību ir visnotaļ ļoti rūpīgi izstrādāti.

2. EDAU uzsver, ka jaunajam juridiskajam režīmam, cik sarežģīts tas arī būtu, būtu

   — jānodrošina augsta līmeņa datu aizsardzība,

   — jābūt prognozējamam pilsoņiem, kā arī iestādēm, kas dalās datiem,

   — jābūt konsekventi piemērotam dažādos (pirmā vai trešā pīlāra) kontekstos.

3. Turklāt, ar *SIS* II ieviešot jaunus elementus, kas palielinātu tās iespējamo ietekmi uz fizisku personu dzīvi, būtu jāparedz stingrāki drošības mehānismi, kas aprakstīti atzinumā. Konkrēti:

— Piekļuvi *SIS* II datiem nevar piešķirt jaunām iestādēm bez stingrākā pamatojuma. Tā arī būtu cik vien iespējams jāierobežo, gan attiecībā uz pieejamiem datiem, gan uz pilnvarotām personām.

— Ar brīdinājumu savstarpēju sasaisti nedrīkst izraisīt — pat netieši — pārmaiņas piekļuves tiesībās.

— Tiesību aktu, kas nav pieņemts, nevar uzskatīt par likumīgu pamatu, lai ievadītu datus *SIS* II (brīdinājumi, lai atteiktu ieceļošanu).

— Transportlīdzekļu reģistrācijas iestāžu piekļuves juridiskais pamats būtu jāpārskata, jo piekļuve ir paredzēta galvenokārt, lai apkarotu noziedzību.

— EDAU atzīst, ka biometrijas datu izmantošana var uzlabot sistēmas darbību un palīdzēt identitātes zādzību cietušām personām. Tomēr, šādas iekļaušanas iespaids nav pietiekami pārdomāts un šo datu ticamība šķiet pārāk augstu novērtēta.

3. Piešķirot jebkurai iestādei piekļuvi *SIS* II datiem, būtu jāpiemēro stingri nosacījumi:

— Piekļuvei jāsaskan ar *SIS* II vispārējo mērķi un juridisko pamatu.

— Jāpierāda vajadzība piekļūt *SIS* II datiem.

— Datu lietojums ir jānosaka skaidri un stingri.

— Piekļuves nosacījumiem jābūt skaidri definētiem un stingriem. Jo īpaši būtu jābūt atjauninātam sarakstam, kurā norādītas personas, kam ir tiesības piekļūt *SIS* II Eiropola un *Eurojust* vajadzībām.

— Tas, ka šīm iestādēm piešķir piekļuvi *SIS* II datiem, nevar būt pamatojums datu ievadīšanai vai uzturēšanai sistēmā, ja tie nav derīgi attiecībā uz konkrēto brīdinājumu.

— Datu glabāšanas termiņu nevar paildzināt, ja tas nav jādara saistībā ar iemeslu, kādēļ dati bija jāievada.

4. Konkrēti attiecībā uz Eiropolu un *Eurojust* EDAU mudina Komisiju ierobežot tādu uzdevumu skaitu, kuru veikšanai piekļuve būtu pamatota. Eiropola un *Eurojust* piekļuvei jāaprobežojas ar datiem par fiziskām personām, kuru vārdi jau atrodami tā rīcībā esošās lietās. Ir arī ieteikts piešķirt Eiropolam un *Eurojust* tikai vienu piekļuves punktu.

11.2. **Īpašas piebildes**

1. EDAU atzinīgi vērtē Komisijas atzinumu, ka Regula 45/2001 attiecas uz visām datu apstrādes darbībām, ko Komisija veic *SIS* II, jo ar šādu atzinumu palīdzēs nodrošināt, ka noteikumus par fiziskas personas pamattiesību un pamatbrīvību aizsargāšanu attiecībā uz personas datu apstrādi piemēros konsekventi un vienveidīgi.

2. Lai attiecīgas valsts mērogā nodrošinātu mērķu stingru ierobežojumu, EDAU iesaka priekšlikumos, kas saistīti ar *SIS* II (konkrēti — ierosinātās regulas 21. pantā un ierosinātā lēmuma 40. pantā) ieviest noteikumu, kam ir viens un tas pats mērķis kā Šengenas Konvencijas 102.4 pantam — ierobežot dalībvalstu iespējas paredzēt datu izmantošanu vajadzībām, kas nav paredzētas *SIS* II dokumentos.

5. Attiecībā uz brīdinājumiem, lai atteiktu ieceļošanu, noteikumi, kas pamatojas uz vēl nepieņemtiem tiesību aktiem, būtu vai nu jāatceļ, vai jāpārstrādā, pamatojoties uz spēkā esošiem tiesību aktiem, lai fiziskas personas varētu uzzināt, tieši kādus pasākumus iestādes var veikt attiecībā uz viņiem.

6. Datu uzglabāšanas laiki ir paildzināti bez jebkāda nopietna pamatojuma. Ja nav ticama pamatojuma, būtu no jauna jāpiemēro pašreizējie termiņi, jo īpaši attiecībā uz brīdinājumiem, lai veiktu diskrētus novērojumus vai konkrētas pārbaudes.

7. Komisijas uzdevums ir atbildēt par operatīvo pārvaldību. Ņemot vērā arī Komisijas lielo nozīmi sistēmas izstrādē un uzturēšanā, Komisija būtu jāuzskata par *sui generis* kontrolieri. Komisija ir daudz vairāk nekā datu apstrādātājs, bet tās uzdevumi ir daudz ierobežotāki par parastā kontroliera uzdevumiem, jo Komisija nevar piekļūt *SIS* II apstrādātiem datiem.

   Abu priekšlikumu 12. pantā būtu jānosaka, ka Komisijai būtu regulāri jāierosina tādu jaunu tehnoloģiju īstenošana, kas atspoguļo tehnisko un organizatorisko pasākumu līmeni attiecīgajā jomā un uzlabos datu aizsardzību un drošību.

8. Attiecībā uz dalībvalstu uzdevumu ir jāsniedz precīzāka informācija par iestādēm, kas veic kontroliera funkcijas.

9. Attiecībā uz informāciju par datu subjektu:

   — Ierosinātās regulas sarakstā būtu jāiekļauj papildu informācija: datu uzglabāšanas laiks; tas, vai subjektam ir tiesības lūgt pārskatīt vai iesniegt apelāciju pret lēmumu dot brīdinājumu; tas, vai var saņemt palīdzību no datu aizsardzības iestādes, un tas, vai ir aizsardzības līdzekļi.

     Attiecībā uz informācijas sniegšanas laiku turklāt būtu jāiekļauj informācija par to, vai lēmumā, uz ko brīdinājums pamatojas, ir paredzēts pienākums sniegt informāciju par brīdinājumu.

   — Ierosinātā lēmuma 50. pants būtu jāgroza, datu subjekta tiesībām saņemt informāciju neizvirzītu par nosacījumu datu subjekta iesniegumu.

10. Doma priekšlikumos paredzēt termiņus, kādos jāatbild uz lūgumu pēc piekļuves, ir sveicama. Ja attiecīgo valstu tiesību aktos arī noteikti termiņi, būtu skaidri jāparedz, ka piemēro datu subjektam vislabvēlīgākos termiņus.

    Turklāt būtu lietderīgi paredzēt pienākumu datu aizsardzības iestādēm aktīvi sadarboties, īstenojot piekļuves tiesības.

11. Attiecībā uz tiesībām uz aizsardzības līdzekļiem — EDAU iesaka atcelt 30. un 52. pantā noteikto teritoriālo ierobežojumu.

12. Attiecībā uz valstu datu aizsardzības iestāžu pilnvarām:

    — regulā: jāuzskata, ka attiecībā uz *SIS* II šīs iestādes var īstenot visas pilnvaras, kas tām piešķirtas saskaņā ar Direktīvas 95/46/EK 28. pantu; tas būtu jāprecizē ierosinātajā regulā.

    — ierosinātajā lēmumā: būtu jāparedz uzraudzības iestādēm tās pašas pilnvaras kā attiecīgajā regulā/direktīvā.

13. Attiecībā uz EDAU pilnvarām: EDAU vajadzētu būt iespējai īstenot visas saskaņā ar Regulu 45/2001 piešķirtās pilnvaras, tomēr ņemot vērā, cik ierobežotas ir Komisijas pilnvaras attiecībā uz pašiem datiem.

14. Attiecībā uz koordinētu uzraudzību: priekšlikumos arī atzīta vajadzība koordinēt dažādo iesaistīto iestāžu uzraudzības darbības. EDAU pauž gandarījumu par to, ka priekšlikumos būtībā ir ietverti visi aspekti, kas vajadzīgi, lai izveidotu attiecīgu valstu un Eiropas mēroga uzraudzības iestāžu sadarbību. Šajos pantos (ierosinātās regulas 31. pantā un ierosinātā lēmuma 53. pantā) tomēr derētu precizēt šādas koordinācijas saturu.

15. Priekšlikuma 10. un 13. pantā paredzēti dažādi datu aizsardzības pasākumi; ir sveicami, ka ir paredzēts iekļaut noteikumus par metodisku drošības pasākumu (paš)revīziju.

    — Ierosinātā lēmuma 59. pantam un ierosinātas regulas 34. pantam, kurā noteikta pārraudzība un izvērtēšana, tomēr nevajadzētu attiekties tikai uz ražīgumu, rentabilitāti un pakalpojumu kvalitāti, bet arī uz atbilstību juridiskām prasībām, jo īpaši datu aizsardzības jomā. Šie noteikumi būtu atbilstīgi jāgroza.

    — Turklāt, papildinot ierosinātā lēmuma 10. panta 1. punkta f) apakšpunktu vai 18. pantu un ierosinātās regulas 17. pantu, būtu jāpiebilst, ka dalībvalstīm, Eiropolam un *Eurojust* vajadzētu nodrošināt to, ka ir pieejami precīzi lietotāju profili (kas būtu jāuzglabā 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.

    — Personas datu apstrādes darbības likumība pamatojas uz datu drošības un integritātes stingru ievērošanu. Būtu jāļauj EDAU pārraudzīt ne tikai datu drošību, bet arī integritāti, pārbaudot pieejamos reģistrus. Tādēļ ir jāpievieno formulējums "datu integritāte" 14. panta 6. punktam.

16. Izmantojot valstu eksemplārus, var radīt daudz papildu apdraudējumu. EDAU nav pārliecināts ne par to, ka valstu eksemplāri ir jāizmanto (ņemot vērā pieejamās tehnoloģijas), ne arī par to, ka šiem eksemplāriem dod papildu vērtību. Viņš iesaka novērst vai vismaz ļoti ierobežot dalībvalstu iespējas izmantot savus eksemplārus. Ja valstu eksemplārus tomēr izstrādā, būtu jāievēro stingrs mērķu ierobežojuma princips attiecībā uz to izmantošanu attiecīgās valstīs. Līdzīgi būtu jāparedz, ka var veikt meklējumus attiecīgas valsts eksemplārā, tikai izmantojot centralizēto datubāzi.

17. Attiecībā uz komitoloģiju: lēmumi, kas būtiski iespaido datu aizsardzību, būtu jāpieņem, pieņemot regulu vai lēmumu, vēlams, saskaņā ar koplēmuma procedūru. Ja komitoloģijas procedūru faktiski izmanto, EDAU padomdevēja uzdevums būtu jāparedz lēmuma 60. un 61. pantā un regulas 35. pantā.

18. Sistēmu savstarpēju savietojamību nevar īstenot, pārkāpjot vajadzības ierobežojuma principu, un šajā jautājumā jebkāds priekšlikums būtu jāiesniedz EDAU.

Briselē, 2005. gada 19. oktobrī

Peter HUSTINX

Eiropas datu aizsardzības uzraudzītājs