I

(Rezolūcijas, ieteikumi un atzinumi)

ATZINUMI

EIROPAS DATU AIZSARDZĪBAS UZRAUDZĪTĀJS

Eiropas Datu aizsardzības uzraudzītāja atzinums par ES un ASV Augsta līmeņa kontaktgrupas galīgo pārskata ziņojumu par informācijas apmaiņu un privātumu, un personas datu aizsardzību

(2009/C 128/01)

EIROPAS DATU AIZSARDZĪBAS UZRAUDZĪTĀJS,

ņemot vērā Eiropas Kopienas dibināšanas līgumu un it īpaši tā 286. pantu,

ņemot vērā Eiropas Savienības Pamattiesību hartu un it īpaši tās 8. pantu,

ņemot vērā Eiropas Parlamenta un Padomes Direktīvu 95/46/EK (1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šo datu brīvu apriti,

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

IR PIEŅĒMIS ŠO ATZINUMU.

I. IEVADS - ATZINUMA KONTEKSTS

1. Eiropas Savienības Padomes prezidentvalsts 2008. gada 28. maijā, gatavojoties ES 2008. gada 12. jūnija samitam, Pastāvīgo pārstāvju komitejai paziņoja, ka ES un ASV Augsta līmeņa kontaktgrupa (*High Level Contact Group*; še turpmāk *HLCG*) ar dalīšanos informācijā un privātuma un personas datu aizsardzību saistītu jautājumu jomā ir galīgā variantā izstrādājusi pārskata ziņojumu. Pārskatu darīja atklātībā pieejamu 2008. gada 26. jūnijā ([1]).

2. Pārskatā ir mēģināts apzināt vienotus privātuma un datu aizsardzības principus kā pirmo soli pretī tam, lai varētu dalīties informācijā ar Amerikas Savienotajām Valstīm, apkarojot terorismu un smagus pārvalstiskus noziegumus.

3. Padomes prezidentvalsts paziņojumā norāda, ka tā priecāsies par visām idejām saistībā ar minētā pārskata ziņojuma turpinājumu, un konkrēti – par reakciju uz pārskata ziņojuma ieteikumiem, kā virzīties uz priekšu. EDAU uz uzaicinājumu atbild, nākot klajā ar šo atzinumu, pamatojoties uz pašreizējo stāvokli, kas ir darīts atklātībā zināms un neskar nevienu turpmāku nostāju, ko viņš varētu ieņemt, analizējot attiecīgā jautājuma attīstību.

4. EDAU norāda, ka *HLCG* ir darbojusies apstākļos, ko, it īpaši kopš 2001. gada 11. septembra, iezīmē ASV un ES savstarpējas datu apmaiņas attīstība ar starptautisku nolīgumu vai citu tipu instrumentu starpniecību. Pie tādiem pieder Eiropola un *Eurojust* nolīgumi ar Amerikas Savienotajām Valstīm, kā arī PDR nolīgumi un *SWIFT* lieta, par ko notika ES un ASV ierēdņu vēstuļu apmaiņa, lai noteiktu obligātas datu aizsardzības garantijas ([2]).

([1]) Padomes dokuments Nr. 9831/08, pieejams vietnē – http://ec.europa.eu/justice_home/fsj/privacy/news/index_en.htm

([2]) — Amerikas Savienoto Valstu un Eiropas Policijas biroja 2001. gada 6. decembra nolīgums un Eiropola un ASV papildu nolīgums par personas datu un saistītas informācijas apmaiņu – publicēts Eiropola interneta vietnē;
— Amerikas Savienoto Valstu un *Eurojust* nolīgums par tiesu iestāžu sadarbību, 2006. gada 6. novembris, publicēts *Eurojust* interneta vietnē;
— Eiropas Savienības un Amerikas Savienoto Valstu nolīgums par aviopārvadātāju veikto pasažieru datu reģistra (PDR) datu apstrādi un pārsūtīšanu Amerikas Savienoto Valstu Iekšzemes drošības departamentam (IDD) (2007 PDR nolīgums) – Briselē parakstīts 2007. gada 23. jūlijā, un Vašingtonā 2007. gada 26. jūlijā, OV L 204, 4.8.2007., 18. lpp.;
— ASV un ES iestāžu vēstuļu apmaiņa par teroristu finansējuma izsekošanas programmu, 2007. gada 28. jūnijs.

5. Turklāt ES arī piedalās sarunās un vienojas par līdzīgiem instrumentiem, ar ko ir paredzētas personas datu apmaiņas ar citām trešām valstīm. Jaunāks piemērs ir Eiropas Savienības un Austrālijas nolīgums par aviopārvadātāju veikto Eiropas Savienības pasažieru datu reģistra (PDR) datu apstrādi un pārsūtīšanu Austrālijas muitas dienestam ([3]).

6. Šādā kontekstā rodas iespaids, ka trešo valstu tiesībaizsardzības iestāžu lūgumi piesūtīt tām personas informāciju aizvien vēršas plašumā, un turklāt tas aptver gan parastas valstu datu bāzes, gan citu tipu datnes, konkrēti – privātā sektora savāktus datus.

7. EDAU atgādina arī to, ka būtisks elements ir problēma saistībā ar personas datu pārsūtīšanu trešām valstīm, policijai un tiesu iestādēm sadarbojoties krimināllietās, kuru risina Padomes pamatlēmumā par tādu personas datu aizsardzību, ko apstrādā, policijai un tiesu iestādēm sadarbojoties krimināllietās ([4]), kuru, paredzams, pieņems līdz 2008. gada beigām.

8. Ir paredzams, ka tāda transatlantiska informācijas apmaiņa tikai pieņemsies, un skars papildu sektorus, kur apstrādā datus. Tādā kontekstā dialogs par "transatlantisku tiesībaizsardzību" reizē ir apsveicams un diskrēts. Tas ir apsveicams tādā nozīmē, ka tas varētu veidot skaidrāku sistēmu datu apmaiņām, kas notiek pašlaik vai notiks nākotnē. Tas ir arī diskrēts, jo tāda sistēma varētu padarīt likumīgu ārkārtīgi plašu datu pārsūtīšanu kādā jomā – tiesībaizsardzībā – kuras radītās sekas cilvēkiem ir īpaši smagas, un kurā stingri un uzticami drošības pasākumi un garantijas tālab ir vēl jo vajadzīgākas ([5]).

9. Šī atzinuma nākamā nodaļā uzmanība būs pievērsta pašreizējam stāvoklim un iespējamiem attīstības virzieniem. III nodaļā uzmanība būs pievērsta tāda instrumenta darbības jomai un būtībai, kurš ļautu dalīties informācijā. Atzinuma IV nodaļā no vispārējas perspektīves būs analizētas juridiskas problēmas, kas ir saistītas ar iespējama nolīguma saturu. Tajā uzmanība būs pievērsta tādām problēmām kā Amerikas Savienotajās Valstīs nodrošinātās aizsardzības izvērtējuma nosacījumi, un pārrunāts jautājums, kā izmantot ES normatīvo sistēmu par aizsardzības izvērtējuma kritēriju. Minētajā nodaļā būs uzskaitītas arī galvenās prasības, kas jāiekļauj tādā nolīgumā. Visbeidzot, atzinuma V nodaļā būs analizēti pārskata ziņojumam pievienotie privātuma principi.

([3]) OV L 213, 8.8.2008., 49. lpp.

([4]) Padomes pamatlēmums par tādu personas datu aizsardzību, ko apstrādā, policijai un tiesu iestādēm sadarbojoties krimināllietās, 2008. gada 24. jūnija variants, kas ir pieejams interneta vietnē http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=193371

([5]) Par to, ka ir vajadzīga skaidra juridiska sistēma, skat. šī atzinuma III un IV nodaļu.

II. PAŠREIZĒJAIS STĀVOKLIS UN IESPĒJAS VIRZĪTIES UZ PRIEKŠU

10. EDAU šādi vērtē pašreizējo stāvokli. Ir gūti panākumi, nosakot vienotus standartus, kā dalīties informācijā un aizsargāt privātumu un personas datus.

11. Tomēr jebkāda ES un ASV nolīguma gatavošanas darbi vēl nav galā. Ir jāpaveic vairāk. Pārskata ziņojumā *HLCG* piemin vairākas neatrisinātas problēmas, kuru vidū "kompensācijas" problēma ir visnopietnākā. Joprojām nav vienprātības, cik plaši tiesiskas kompensācijas pasākumi ir vajadzīgi ([6]). Piecas citas neatrisinātas problēmas ir apzinātas pārskata ziņojuma 3. nodaļā. Turklāt no šī atzinuma izriet, ka arī daudzi citi jautājumi vēl nav atrisināti, piemēram, jautājums par informācijas apmaiņas instrumenta darbības jomas plašumu un būtību.

12. Tā kā pārskata ziņojumā par labāko variantu ir atzīts tāds nolīgums, kas uzliek saistības – EDAU tam piekrīt – piesardzība ir vēl jo vajadzīgāka. Ir jāturpina rūpīgi un nopietni gatavoties, pirms varētu panākt nolīgumu.

13. Visbeidzot, pēc EDAU domām, nolīguma noslēgšanai vajadzētu notikt saskaņā ar Lisabonas Līgumu, protams, atkarībā no tā, kā tas stājas spēkā. Patiesi, ja tas notiktu saskaņā ar Lisabonas Līgumu, nevajadzētu rasties neskaidrībām par ES pīlāru nošķirumu. Turklāt būtu nodrošināta pilnīga Eiropas Parlamenta iesaiste līdz ar Tiesas veiktu juridisku kontroli.

14. Tādos apstākļos labākais, kā virzīties uz priekšu, būtu izstrādāt ceļvedi, lai vēlākā stadijā panāktu iespējamu nolīgumu. Tādā ceļvedī varētu būt šādi elementi –

— norādes, kā *HLCG* (vai kādai citai grupai) turpināt darbu, kā arī tā termiņi

— agrā stadijā – diskusijas un, iespējams, vienošanās par būtiskām problēmām, piem., nolīguma darbības jomu un būtību

— pamatojoties uz vienotu minēto būtisko problēmu izpratni, sīkāk izstrādāt datu aizsardzības principus

— ieinteresēto personu iesaiste dažādās procedūras stadijās

— Eiropas pusei – risināt organizatoriskus ierobežojumus.

([6]) Pārskata 5. lappuse, C punkts.

III. **INFORMĀCIJAS APMAIŅAI PIEŅEMTA INSTRUMENTA DARBĪBAS JOMA UN BŪTĪBA**

15. Pēc EDAU viedokļa ir ļoti svarīgi, lai iespējama instrumenta darbības joma un būtība, kā arī datu aizsardzības principi būtu skaidri definēti, jo tas būtu pirmais solis turpmākā tādu instrumentu izstrādē.

16. Runājot par darbības jomu, svarīgi jautājumi, kas jāatbild, ir šādi –

— kas ir iesaistītie darbību veicēji gan tiesībaizsardzības jomā, gan ārpus tās;

— kas ir domāts ar "tiesībaizsardzības vajadzībām", un kāda ir to saikne ar citām vajadzībām, piemēram, attiecīgas valsts drošību, un konkrētāk, ar robežkontroli un sabiedrības veselības aizsardzību;

— kā attiecīgais instruments iekļausies vispārējā transatlantiskas drošības teritorijas perspektīvē.

17. Būtības definīcijai vajadzētu padarīt skaidrākus šādus jautājumus –

— vajadzības gadījumā – kādā pīlārā notiks sarunas par instrumentu;

— vai instruments uzliks saistības ES un ASV;

— vai tam būs tiešas sekas – tādā nozīmē, ka tajā ir paredzētas cilvēku tiesības un pienākumi, ko tiesu iestādes var īstenot;

— vai instrumentā pašā būs paredzēta informācijas apmaiņa, vai arī būs noteikts obligāts informācijas apmaiņas standarts, ko papildinātu ar konkrētiem nolīgumiem;

— kā instruments saistīsies ar esošiem instrumentiem – vai tas tos respektēs, aizstās vai papildinās.

III. 1. **Instrumenta darbības joma**

Iesaistītie dalībnieki

18. Lai gan *HLCG* sniegtajā pārskata ziņojumā nav skaidru norāžu par precīzu nākotnē pieņemamā instrumenta darbības jomu, no tajā minētajiem principiem var secināt, ka to ir paredzēts attiecināt gan uz savstarpēju privātu un valsts mēroga darbību veicēju datu pārsūtīšanu ([7]) gan arī valsts iestāžu savstarpēju datu pārsūtīšanu.

— Privātu un valsts mēroga dalībnieki –

19. EDAU saskata loģiku izmantot nākotnē pieņemamu instrumentu, lai privāti un valstu mēroga dalībnieki savstarpēji pārsūtītu datus. Tādus instrumentus izstrādā, pamatojoties uz ASV puses pēdējo gadu lūgumiem saņemt informāciju no privātpersonām. EDAU norāda, ka patiesi – privāti darbību veicēji kļūst par regulāras informācijas avotu tiesībaizsardzības perspektīvē, vienalga, vai tas notiktu ES vai starptautiskā līmenī ([8]). *SWIFT* lieta bija nopietns precedents, kurā privātu uzņēmējsabiedrību lūdza regulāri pārsūtīt visus datus kādas trešās valsts tiesībaizsardzības iestādēm ([9]). Vācot PDR datus no aviosabiedrībām, ir izmantots tas pats domu gājiens. EDAU uzskata, ka jautājumā par iecerētu, Eiropas PDR sistēmai paredzētu pamatlēmumu, viņš jau ir apšaubījis tādas tendences likumīgumu ([10]).

20. Ir vēl divi iemesli nesteigties nākotnē pieņemama instrumenta darbības jomā iekļaut datus, ko savā starpā pārsūta privāti un valstu mēroga darbību veicēji.

21. Pirmkārt, tādu datu iekļaušana varētu radīt negribētas sekas pašā ES teritorijā. EDAU ir nopietni norūpējies, ja privātu uzņēmējsabiedrību (piem., finanšu iestāžu) datus vispār var pārsūtīt trešām valstīm, tad tas varētu radīt stipru spiedienu, lai Eiropas Savienības tiesībaizsardzības iestādēm vienu un to pašu tipu datus darītu vienādi pieejamus. PDR sistēma ir piemērs tādam nevēlamam notikumu pavērsienam, ko sākusi ASV, bez izšķirības vācot visus pasažieru datus, un kas ir transponēts arī Eiropas iekšējā kontekstā ([11]) – bez skaidriem pierādījumiem, ka tāda sistēma ir vajadzīga un samērīga.

22. Otrkārt, EDAU atzinumā par Komisijas ierosināto ES PDR arī izvirzīja jautājumu par (pirmā vai trešā pīlāra) datu aizsardzības sistēmu, ko piemērot valsts mēroga un privātiem darbību veicēju sadarbības nosacījumiem, – vai noteikumiem par pamatu būtu jāņem datu apstrādātāju kvalitāte

([7]) Skat. konkrēti pārskata ziņojuma 3. nodaļas, "Neatrisināti jautājumi, kas attiecas uz transatlantiskām attiecībām", 1. punktu – "Privātu struktūru pienākumu konsekvence, pārsūtot datus".

([8]) Šajā jautājumā skat. EDAU 2007. gada 20. decembra atzinumu par ierosināto Padomes pamatlēmumu izmantot pasažieru datu reģistra (*Passenger Name Record – PNR*) datus tiesībaizsardzības vajadzībām, OV C 110, 01.05.2008., 1. lpp. "Agrāk tiesībaizsardzības nozares un privātā sektora darbības bija skaidri nošķirtas, ja tiesībaizsardzības uzdevumus veic īpaši norīkotas iestādes, konkrēti policijas spēki, un privātu darbību veicējiem katrā konkrētā gadījumā individuāli lūdz darīt zināmus personas datus tiesībaizsardzības iestādēm. Tagad pastāv tendence tiesībaizsardzības vajadzību dēļ regulāri uzspiest sadarbību privātu darbību veicējiem".

([9]) Skat. 29. panta darba grupas atzinumu Nr. 10/2006 (2006. gada 22. novembris) par personas datu apstrādi, ko veic *Society for Worldwide Interbank Financial Telecommunication* (SWIFT), WP 128.

([10]) Atzinums sniegts 2007. gada 20. decembrī, *op. cit.*

([11]) Skat. 8. zemsvītras piezīmē minēto ierosināto Padomes pamatlēmumu izmantot pasažieru datu reģistra (*Passenger Name Record – PNR*) datus tiesībaizsardzības vajadzībām, ko pašlaik pārrunā Padomē.

(privātais sektors) vai iecerētais mērķis (tiesībaizsardzība)? Pirmā un trešā pīlāra robežšķirtne nebūt nav skaidra gadījumos, ja privātiem darbību veicējiem ir uzticēts pienākums apstrādāt personas datus tiesībaizsardzības vajadzībām. Tādā sakarā ir svarīgi, ka ģenerāladvokāts *Bot* nesenā atzinumā par datu glabāšanas lietu ([12]) ir ierosinājis tādos gadījumos novilkt robežšķirtni, bet priekšlikumā piebilst – "robežšķirtni noteikti var kritizēt, un dažā ziņā tā var šķist mākslīga." EDAU arī norāda, ka Tiesas nolēmums PDR jautājumā ([13]) pilnībā nedod atbildi uz jautājumu, kādu tiesisko sistēmu piemērot. Piemēram, tas, ka uz dažām darbībām neattiecas Direktīva 95/46/EK, automātiski nenozīmē, ka minētās darbības var regulēt saskaņā ar trešo pīlāru. Tādējādi tas, iespējams, atstāj iespēju divdomīgi interpretēt jautājumu par to, kādas tiesības piemērot, un noteikti rada juridiskas neskaidrības par datu subjektiem pieejamām juridiskām garantijām.

23. No šādas perspektīves EDAU uzsver, ka ir jānodrošina, lai nākotnē pieņemamos instrumentos, kuros ietverti vispārēji datu aizsardzības principi, nevar leģitimizēt kuru katru transatlantisku, no privātpersonām un valsts struktūrām iegūtu personas datu savstarpēju pārsūtīšanu. Pārsūtīšanu var iekļaut kādā nākotnē paredzamā instrumentā tikai ar noteikumu, ka –

— iecerētajā instrumentā ir paredzēts, ka pārsūtīšana ir atļauta tikai tad, ja ir pierādīts, ka tā ir absolūti obligāta konkrētām vajadzībām, par katru konkrētu gadījumu pieņemot individuālu lēmumu;

— pati pārsūtīšana ir saistīta ar nopietniem datu aizsardzības drošības pasākumiem (kā aprakstīts šajā atzinumā).

Turklāt EDAU ņem vērā neskaidrības par to, kādu datu aizsardzības sistēmu piemērot, un tālab lūdz pašreizējā ES tiesību stāvoklī noteikti neietvert no privātpersonām un valsts struktūrām iegūtu personas datu savstarpēju pārsūtīšanu.

— Valstu iestāžu starpā –

24. Nav skaidrota precīza informācijas apmaiņas joma. Pirmajam solim, turpinot vienota instrumenta izstrādi, būtu jābūt – precizēt iecerētā instrumenta darbības jomu. Paliek konkrēti neatbildēti jautājumi, vai –

— Ciktāl ir runa par Eiropas Savienības datu bāzēm, vai instruments attiektos uz centralizētām datu bāzēm, ko (daļēji) apsaimnieko ES, piemēram, uz Eiropola un *Eurojust* datu bāzēm, vai uz decentralizētām datu bāzēm, ko apsaimnieko dalībvalstis – vai arī uz abējādām datu bāzēm;

— instrumenta darbības joma attiecas uz savstarpēji savienotiem tīkliem, tas ir, vai paredzētās garantijas attieksies uz datiem, ar ko savstarpēji apmainās dalībvalstis vai aģentūras gan Eiropas Savienībā, gan arī Amerikas Savienotajās Valstīs;

— instruments attiektos tikai uz savstarpējām tiesībaizsardzības (policijas, tiesu iestāžu, iespējams, muitas) jomas datu bāzu vai arī citu datu bāzu –, piemēram, nodokļu datu bāzu – apmaiņu ar informāciju;

— instruments attiektos arī uz valstu drošības aģentūru datu bāzēm, vai arī būtu paredzēta minēto aģentūru piekļuve tiesībaizsardzības datu bāzēm citu līgumslēdzēju pušu teritorijā (ES piekļuve ASV datu bāzēm un otrādi);

— instruments attiektos uz informācijas pārsūtīšanu, atsevišķi izskatot katru konkrētu gadījumu, vai arī uz pastāvīgu piekļuvi esošām datu bāzēm. Tāda hipotēze noteikti radītu samērības problēmas, kas būs sīkāk pārrunātas V nodaļas 3. punktā

Tiesībaizsardzības mērķis

25. Iespējama nolīguma mērķa definēšana arī ir iemesls neskaidrībām. Tiesībaizsardzības mērķis ir skaidri norādīts ievadā, kā arī pirmajā pārskata ziņojumam pievienotajā principā, un tas būs sīkāk analizēts atzinuma IV nodaļā. EDAU jau norādījis – minētie paziņojumi liecina, ka datu apmaiņa īpaši skartu trešā pīlāra jautājumus, un var minēt, vai tā ir tikai pirmais solis pretī plašākai informācijas apmaiņai. Šķiet skaidrs, ka pie "valsts drošības" mērķiem, kā norādīts pārskata ziņojumā, pieder terorisma, organizētas noziedzības un citu noziegumu apkarošana. Bet – vai ir paredzēts pieļaut datu apmaiņu arī citādu valsts interešu vārdā, piemēram, iespējamu sabiedrības veselības aizsardzības apdraudējumu dēļ?

26. EDAU iesaka mērķa noteikšanā aprobežoties ar precīzi apzinātu datu apstrādi, un pamatot politikas izvēli, definējot mērķus.

([12]) Ģenerāladvokāta *Bot* 2008. gada 14. oktobrī sniegts atzinums – Īrija pret Eiropas Parlamentu un Padomi, (Lieta C-301/06), 108. punkts.

([13]) Tiesas 2006. gada 30. maija nolēmums – Eiropas Parlaments pret Eiropas Savienības Padomi (C-317/04) un Eiropas Kopienu Komisiju (C-318/04), apvienotas lietas C-317/04 un C-318/04, ECR [2006] P. I-4721.

Pasaules mēroga transatlantiska aizsargāta teritorija

27. Plašā, pārskata ziņojuma aptvertā joma būtu jāaplūko pasaules mēroga transatlantiskas aizsargātas teritorijas perspektīvē, par ko diskutē tā dēvētā "Nākotnes grupa" ([14]). Grupas 2008. gada jūnija pārskata ziņojumā uzmanība ir pievērsta iekšlietu politikas ārējiem aspektiem. Tajā ir atbalstīta doma, ka *"Eiropas Savienībai līdz 2014. gadam būtu jāpieņem lēmums par politisku mērķi – brīvības, drošības un tiesiskuma jomā izveidot eiroatlantiskas sadarbības teritoriju ar Amerikas Savienotajām Valstīm"*. Sadarbība sniegtos tālāk par drošību stingrā nozīmē, un vismaz aptvertu tādus tematus, kas ir aplūkoti EK Līguma IV sadaļā, piemēram, imigrāciju, vīzas un patvēruma piešķiršanu, un civiltiesisku sadarbību. Ir jāapšauba, ciktāl nolīgums par datu aizsardzības pamatprincipiem, piemēram, par *HLCG* pārskata ziņojumā minētajiem, varētu būt par pamatu informācijas apmaiņai tik plašos mērogos.

28. Ja viss rit kā iecerēts, līdz 2014. gadam pīlāru struktūra vairs nepastāvēs, un datu aizsardzībai visā Eiropas Savienībā būs viens juridisks pamats (saskaņā ar Lisabonas Līgumu – 16. pants līgumā par Eiropas Savienības funkcionēšanu). Tomēr tas, ka no datu aizsardzības *normēšanas* viedokļa ES mērogā notiek saskaņošana, nenozīmē, ka jebkurā nolīgumā ar kādu trešo valsti varētu paredzēt personas datu *pārsūtīšanu* neatkarīgi no iecerētajiem mērķiem. Datu aizsardzības garantijas var būt jāpielāgo atkarībā no datu apstrādes konteksta un nosacījumiem konkrētās jomās, piemēram, tiesībaizsardzībā. EDAU iesaka ņemt vērā dažādo perspektīvu sekas, gatavojot turpmākos nolīgumus.

III.2. **Nolīguma būtība**

Eiropas organizatoriskā sistēma

29. Īstermiņā katrā ziņā būtiski ir noteikt, kādā pīlārā notiks sarunas par attiecīgo mehānismu. Tas jo īpaši ir vajadzīgs iekšējas normatīvas datu aizsardzības sistēmas dēļ, jo to ietekmēs tādi nolīgumi. Vai tā būs pirmā pīlāra sistēma – galvenokārt Direktīva 95/46/EK ar konkrētiem režīmiem, kā datus pārsūtīt trešām valstīm – vai arī trešā pīlāra sistēma, kurā, pārsūtot datus trešām valstīm, režīms nav tik stingrs? ([15])

30. Kaut gan tiesībaizsardzības mērķi gūst virsroku, kā jau minēts, *HLCG* pārskata ziņojumā tomēr ir minēta datu vākšana no privātiem dalībniekiem, un mērķus var arī interpretēt plaši, ievērojami pārsniedzot drošības jomu, ietverot arī, piem., imigrācijas un robežkontroles problēmas, bet arī, iespējams, sabiedrības veselības aizsardzību. Ņemot vērā tādas neskaidrības, būtu ļoti ieteicams pagaidīt pīlāru saskaņošanu saskaņā ar ES tiesībām, kā paredzēts Lisabonas Līgumā, lai izveidotu skaidru juridisko pamatu sarunām un precīzi noteiktu Eiropas iestāžu, it īpaši Eiropas Parlamenta un Komisijas uzdevumus.

Instruments, kas uzliek saistības

31. Būtu jānoskaidro, vai diskusijās gūtie secinājumi liks noslēgt saprašanās memorandu, vai kādu citu instrumentu, kas neuzliek saistības, – vai arī starptautisku nolīgumu, kas uzliek saistības.

32. EDAU atbalsta to, ka pārskata ziņojumā ir dota priekšroka nolīgumam, kas uzliek saistības. EDAU uzskata, ka oficiāls nolīgums, kas uzliek saistības, ir obligāts priekšnoteikums katrai datu pārsūtīšanai ārpus ES, neatkarīgi no datus pārsūtīšanas mērķa. Datus nevar pārsūtīt uz trešo valsti bez attiecīgiem nosacījumiem un drošības pasākumiem, kas ir paredzēti konkrētā tiesiskā sistēmā (turklāt tādā, kas uzliek saistības). Citiem vārdiem sakot, saprašanās memorands vai cits instruments, kas neuzliek saistības, var noderēt, lai dotu ievirzi sarunām par turpmākiem nolīgumiem, kas uzliek saistības, bet tas nekad nevarēs aizstāt nolīgumu, kas uzliek saistības.

Tieša iedarbība

33. Instrumentam būtu vienādi jāuzliek saistības gan ASV, gan ES un tās dalībvalstīm.

34. Turklāt būtu jānodrošina, lai cilvēki būtu tiesīgi īstenot tiesības, un it īpaši – saņemt kompensāciju – pamatojoties uz principiem, par ko ir panākta vienprātība. Pēc EDAU domām, to vislabāk var nodrošināt, ja instrumenta būtiskos noteikumus formulē tā, ka tie rada tiešas sekas Eiropas Savienības rezidentiem, un tos var izmantot tiesā. Tālab instrumentā ir skaidri jāformulē tiešas sekas, ko radīs starptautiskais nolīgums, kā arī nosacījumi tā transponēšanai Eiropas iekšējās tiesībās un attiecīgu valstu tiesībās, lai nodrošinātu pasākumu efektivitāti.

Saistība ar citiem instrumentiem

35. Svarīgs ir arī jautājums par to, ciktāl nolīgums ir savrups vai arī katrā konkrētā gadījumā tas ir jāpapildina ar turpmākiem nolīgumiem par konkrētām datu apmaiņām. Patiesi ir apšaubāmi, vai viens nolīgums, ar vienotu standartu kompleksu, varētu pienācīgi aptvert daudzas dažādas

([14]) Neoficiālās augsta līmeņa padomdevēju grupas pārskata ziņojums par Eiropas iekšlietu politikas nākotni – "Brīvība, drošība, privātums – Eiropas iekšlietas atvērtā pasaulē", 2008. gada jūnijs, pieejams tīkla vietnē register.consilium.europa.eu

([15]) Skat. 11. un 13. *DPFD* pantu, kas minēts atzinuma 7. punktā.

nianses, datus apstrādājot trešajā pīlārā. Vēl apšaubāmāk ir tas, ka ar nolīgumu – bez papildu diskusijām un drošības pasākumiem – varētu *ļaut* automātiski apstiprināt jebkādu personas datu pārsūtīšanu – neatkarīgi no pārsūtīšanas mērķa un attiecīgo datu būtības. Turklāt nolīgumi ar trešām valstīm ne vienmēr ir pastāvīgi, jo tos var saistīt ar konkrētiem apdraudējumiem, tos var pārskatīt, un tiem var būt pašizbeigšanās klauzulas (*sunset clauses*). No otras puses, vispārpieņemti obligāti standarti, kas ir atzīti kādā instrumentā, kurš uzliek saistības, varētu atvieglināt turpmākas diskusijas par tādu personas datu pārsūtīšanu, kas ir saistāmi ar konkrētām datu bāzēm vai apstrādes darbībām.

36. EDAU tālab dotu priekšroku attīstīt obligātu datu aizsardzības kritēriju kompleksu, ko katrā konkrētā gadījumā, kā minēts *HLCG* pārskata ziņojumā, papildinātu ar konkrētiem papildu noteikumiem, nevis tā alternatīvu – noslēgt savrupu nolīgumu. Tādi konkrēti papildu nosacījumi ir priekšnosacījums, lai varētu paredzēt datu pārsūtīšanu konkrētās lietās. Tas palīdzētu panākt no datu aizsardzības viedokļa saskaņotu pieeju.

Esošo instrumentu izmantojums

37. Būtu jāizskata arī tas, kā iespējamu vispārēju nolīgumu apvienot ar jau esošiem nolīgumiem, ko ES un ASV ir noslēgušas savā starpā. Būtu jāatceras, ka ar esošiem nolīgumiem nav uzliktas tādas pašas saistības – konkrēti būtu jāpiesauc PDR nolīgums (tas, kas dod lielāku juridisku skaidrību), Eiropola un *Eurojust* nolīgumi, vai *SWIFT* gadījumā notikusī vēstuļu apmaiņa ([16]). Vai jauna vispārēja sistēma papildinātu esošos instrumentus, vai arī tie paliktu neskarti, un jaunā sistēma attiektos tikai uz citām personas datu apmaiņām nākotnē? Pēc EDAU viedokļa, juridiska konsekvence prasītu saskaņotu noteikumu kompleksu, kas attiektos gan uz noslēgtiem, gan nākotnē noslēdzamiem nolīgumiem par datu pārsūtīšanu, un attiecīgi tos papildinātu.

38. Vispārēja nolīguma piemērošanai esošiem instrumentiem būtu tāda priekšrocība, ka stiprākas kļūtu ar tiem uzliktās saistības. Tas būtu īpaši apsveicami instrumentiem, ar ko neuzliek juridiskas saistības, piemēram, *SWIFT* vēstuļu apmaiņai, jo tas uzliktu pienākumu ievērot vismaz vispārēju privātuma principu kompleksu.

IV. **VISPĀRĒJS JURIDISKS IZVĒRTĒJUMS**

39. Šajā nodaļā aplūkos, kā jāizvērtē konkrētas sistēmas vai instrumenta aizsardzības līmenis, arī jautājums par piemērotiem kritērijiem un vajadzīgajām pamatprasībām.

Pietiekama līmeņa aizsardzība

40. Pēc EDAU domām, būtu jāsaprot, ka vienam no galveniem nākotnes instrumenta rezultātiem būtu jābūt tādam, ka personas datus varētu pārsūtīt uz Amerikas Savienotajām Valstīm tikai tad, ja ASV iestādes garantētu attiecīga līmeņa aizsardzību (un otrādi).

41. EDAU uzskata, ka tikai nopietna piemērotības pārbaude nodrošinās pietiekamas personas datu aizsardzības līmeņa garantijas. Viņš uzskata, ka vispārējam pamatnolīgumam, kā darbības joma būtu tik plaša kā *HLCG* pārskata ziņojuma, vispār būtu grūti izturēt nopietnu piemērotības pārbaudi. Vispārējā nolīguma piemērotību varētu atzīt tikai tad, ja nolīgumu apvienotu ar piemērotiem, īpašiem nolīgumiem, kas būtu noslēgti katrā konkrētā gadījumā atsevišķi.

42. Trešo valstu nodrošinātās aizsardzības līmeņa izvērtējums nav ārkārtas parādība, kur nu vēl Eiropas Komisijai, – piemērotība ir pirmā pīlāra prasība, lai datus varētu pārsūtīt. Vairākos gadījumos piemērotība ir mērīta saskaņā ar Direktīvas 95/46/EK 25. pantu, pamatojoties uz konkrētiem kritērijiem, un to ir apstiprinājuši Eiropas Komisijas lēmumi ([17]). Trešajā pīlārā tāda sistēma nav skaidri paredzēta – datu aizsardzības piemērotības mērīšana ir paredzēta tikai konkrētās, 11. un 13. pantā paredzētās situācijās – vēl nepieņemtajā datu aizsardzības pamatlēmumā ([18]), un ir atstāta dalībvalstu ziņā.

43. Aplūkojamā gadījumā darbības joma skar tiesībaizsardzības vajadzības, un Komisija vada diskusijas Padomes pārraudzībā. Konteksts atšķiras no "drošas ostas" principu vai Kanādas likumu piemērotības izvērtēšanas konteksta, un vairāk piederas nesenajām PDR sarunām ar ASV un Austrāliju, kas notika trešā pīlāra tiesiskajā sistēmā. Tomēr *HLCG* principi ir minēti arī tādā kontekstā kā programma, kas paredz atteikties no vīzām, un kura ir saistīta ar robežu un imigrācijas, un tātad pirmā pīlāra jautājumiem.

44. EDAU iesaka jebkādu piemērotības analīzi nākotnē iespējamu instrumentu sakarā pamatot ar minētajās dažādajās

([16]) Skat. 2. zemsvītras piezīmi.

([17]) Komisijas lēmumi par personas datu aizsardzības piemērotību trešās valstīs, arī Argentīnā, Kanādā, Šveicē, Amerikas Savienotajās Valstīs, Gērnsijā, Menas salā un Džersijā, ir pieejami internetā – http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

([18]) Dalībvalstīm ir ierobežota tādu datu pārsūtīšana trešām valstīm vai starptautiskām struktūrām, kuri ir saņemti no kompetentām citu dalībvalstu iestādēm.

jomās gūto pieredzi. Viņš iesaka sīkāk attīstīt jēdzienu "piemērotība" nākotnē iespējamu instrumentu kontekstā, pamatojoties uz kritērijiem, kas ir līdzīgi tiem, kuri jau ir izmantoti, nosakot piemērotību.

Savstarpēja atzīšana – savstarpējība

45. Otrs aizsardzības līmeņa elements ir saistīts ar ES un ASV sistēmu savstarpēju atzīšanu. *HLCG* pārskata ziņojumā par to ir minēts, ka mērķis būtu "panākt savstarpēju privātuma un datu aizsardzības sistēmu efektivitātes atzīšanu jomās, uz ko attiecas minētie principi" ([19]), un panākt "privātuma un personas datu aizsardzības tiesību aktu līdzvērtīgu un savstarpēju piemērojumu".

46. EDAU uzskata par pašsaprotamu, ka savstarpēja atzīšanu (jeb savstarpējība) ir iespējama tikai tad, ja ir garantēta attiecīga līmeņa aizsardzība. Citiem vārdiem sakot, nākotnē pieņemamam instrumentam būtu jāsaskaņo obligātā līmeņa aizsardzība (izmantojot piemērotības analīzi, ņemot vērā vajadzību pēc īpašiem nolīgumiem, ko atsevišķi pieņem katrā konkrētā gadījumā). Vienīgi ar tādu priekšnosacījumu varētu atzīt savstarpējību.

47. Pirmais elements, kas jāņem vērā, ir būtisku datu aizsardzības noteikumu savstarpējība. Pēc EDAU viedokļa, nolīgumā būtu jārisina jautājums par būtisku datu aizsardzības noteikumu savstarpējības jēdzienu, lai, no vienas puses, nodrošinātu datu apstrādi ES (un ASV) teritorijā, pilnībā respektējot vietējos datu aizsardzības likumus, un, no otras puses, lai, nolīguma jomā apstrādājot datus ārpus to izcelsmes valsts, būtu respektēti nolīgumā ietvertie datu aizsardzības principi.

48. Otrs elements ir kompensācijas mehānismu savstarpējība. Būtu jānodrošina, lai Eiropas pilsoņiem būtu pieejama attiecīga kompensācija, ja ar viņiem saistītus datus apstrādā Amerikas Savienotajās Valstīs (neatkarīgi no tiesībām, ko piemēro apstrādei), un lai Eiropas Savienība un tās dalībvalstis tādas pašas tiesības dotu ASV pilsoņiem.

49. Trešais elements ir savstarpēja tiesībaizsardzības iestāžu piekļuve personas datiem. Ja kāds instruments ASV iestādēm dotu piekļuvi datiem no Eiropas Savienības, savstarpējība nozīmētu, ka tāda pati piekļuve būtu jādod ES iestādēm, lai piekļūtu datiem no ASV. Savstarpējība nedrīkst kaitēt efektīvai datu subjektu aizsardzībai. Tas ir priekšnosacījums "transatlantiskai" piekļuvei, ko izmantotu tiesībaizsardzības iestādes. Tas konkrēti nozīmē, ka –

— Amerikas Savienoto Valstu iestādēm nebūtu jādod tieša piekļuve datiem ES teritorijā (un otrādi). Piekļuve būtu jādod, tikai izmantojot netiešu, lūgumu sistēmu.

— Piekļuvei būtu jānotiek tās valsts datu aizsardzības iestāžu un tiesu iestāžu kontrolē, kurā notiek datu apstrāde.

— Amerikas Savienoto Valstu iestādēm piekļūstot ES datu bāzēm būtu jārespektē svarīgākie datu aizsardzības noteikumi (skat. iepriekš) un datu subjektiem jānodrošina pilnīga kompensācija.

Instrumenta precizitāte

50. Īpaši izvērtējuma nosacījumu aspekti (piemērotība, līdzvērtība, savstarpēja atzīšana) ir būtiski, jo ar tiem nosaka aizsardzības saturu no precizitātes, juridiskas skaidrības un aizsardzības efektivitātes viedokļa. Iecerētā instrumenta saturam ir jābūt precīzam un akurātam.

51. Turklāt, būtu jābūt skaidram, ka visos īpašos nolīgumos, ko noslēgs kādā nākamā pakāpē, arī vajadzēs iekļaut sīki izstrādātus un pilnīgus datu aizsardzības drošības pasākumus, kas attieksies uz paredzēto datu apmaiņu. Vien tādu divkāršu, konkrētu datu aizsardzības principu piemērojums nodrošinās vajadzīgo vispārējā nolīguma saderību ar īpašajiem nolīgumiem, kā jau ir norādīts šī atzinuma 35. un 36. punktā.

Izstrādājot modeli citām trešām valstīm

52. Tas, ciktāl nolīgums ar ASV varētu noderēt kā paraugs citām trešām valstīm, ir pelnījis īpašu uzmanību. EDAU norāda, ka Nākotnes grupas pārskata ziņojumā arī Krievija ir minēta kā stratēģiska ES partnervalsts – līdztekus ASV. Ciktāl principi ir neitrāli, un atbilst būtiskiem ES drošības pasākumiem, tie varētu radīt derīgu precedentu. Tomēr īpašie aspekti, kas datu pārsūtīšanas gadījumos būtu saistīti, piem., ar saņēmējas valsts tiesisko sistēmu, neļautu nolīgumu transponēt tīrā formā. Tikpat svarīgs būs demokrātijas stāvoklis trešās valstis – būtu jāpārliecinās, ka principus, par ko panākta vienprātība, saņēmējā valstī efektīvi garantē un īsteno.

Kādi ir aizsardzības līmeņu vērtēšanas kritēriji

53. Tiešai vai netiešai piemērotībai jebkurā gadījumā vajadzētu atbilst starptautiskai un Eiropas tiesiskai sistēmai, un it īpaši datu aizsardzības drošības pasākumiem, par ko ir panākta

([19]) A nodaļa. Starptautisks nolīgums, kas uzliek saistības, 8. lpp.

vienprātība. Tie ir ierakstīti ANO pamatnostādnēs, Eiropas Padomes 108. konvencijā un tā papildu protokolā, EDSO pamatnostādnēs un iecerētajā datu aizsardzības pamatlēmumā, kā arī – pirmā pīlāra vajadzībām – Direktīvā 95/46/EK ([20]). Visos minētajos instrumentos ir līdzīgi principi, ko plašāk pazīst kā personas datu aizsardzības stūrakmeņus.

54. Ir vēl jo svarīgāk iepriekš minētos principus pienācīgi ņemt vērā, analizējot iespējama nolīguma sekas, piemēram, tāda, kas ir paredzēts *HLCG* pārskata ziņojumā. Instruments, kas attieksies uz visu kādas trešās valsts *tiesību īstenošanas* jomu, patiesi būtu stāvoklis, kam nav precedenta. Pirmajā pīlārā pieņemto lēmumu un ES trešajā pīlārā ar trešām valstīm noslēgto (Eiropola, *Eurojust*) nolīgumu piemērotība vienmēr ir bijusi saistīta ar konkrētu datu pārsūtīšanu, bet šajā gadījumā datu pārsūtīšana varētu kļūt iespējama daudz plašākā jomā, jo sasniedzamie mērķi būtu daudz plašāki (apkarot kriminālnoziegumus, sargāt valstu un sabiedrību drošību, kā arī robežas) un būtu aptverts nezināms skaits datu bāzu.

Galvenās prasības

55. Nosacījumi, kas jāievēro, pārsūtot personas datus trešām valstīm, ir izstrādāti 29. panta darba grupas darba dokumentā ([21]). Kuram katram nolīgumam par obligātiem privātuma principiem būtu jāiztur atbilsmes pārbaude, nodrošinot datu aizsardzības drošības pasākumu efektivitāti.

— Runājot par būtību – datu aizsardzības principiem būtu jānodrošina augsta līmeņa aizsardzība, un tiem būtu jāatbilst tādiem standartiem, kas saskan ar ES principiem. *HLCG* pārskata ziņojumā ietvertie 12 principi šī atzinuma V nodaļā no šāda viedokļa būs analizēti sīkāk.

— Par īpašiem aspektiem – atkarībā no nolīguma būtības, un it īpaši, ja tas ir oficiāls starptautisks nolīgums – likumiem un procedūrām ir jābūt izstrādātām pietiekami sīki, lai tos varētu efektīvi īstenot.

— Par pārraudzību – lai nodrošinātu tādu likumu ievērošanu, par kuriem ir panākta vienprātība, būtu jāievieš konkrēti, gan iekšēji (revīzijas), gan ārēji (pārskatīšana) kontroles mehānismi. Tādiem mehānismiem ir jābūt vienādi pieejamiem abām nolīguma pusēm. Pārraudzībā izmanto mehānismus, ar ko nodrošina ievērošanu makrolīmenī, piemēram, kopīgus pārskatīšanas mehānismus, kā arī ievērošanu mikrolīmenī, piemēram, individuālu kompensāciju.

56. Līdztekus trijām minētajām galvenajām prasībām īpaša uzmanība būtu jāpievērš konkrētiem aspektiem, kas ir saistīti ar personas datu apstrādi tiesībaizsardzības sakarā. Tā tiešām ir joma, kurā pamattiesības var mazliet ciest – ierobežojumu dēļ. Tālab būtu jāpieņem drošības pasākumi, lai kompensētu cilvēku tiesību ierobežojumus, it īpaši šādos aspektos, ņemot vērā sekas, ko tie rada cilvēkiem, –

— Pārskatāmība – informāciju un piekļuvi personas datiem var ierobežot tiesībaizsardzības sakarā, piemēram, ņemot vērā diskrētas izmeklēšanas vajadzības. Lai gan Eiropas Savienībā parasti ievieš papildu mehānismus, lai kompensētu būtiskus tiesību ierobežojumus (kuros bieži vien ir iesaistītas neatkarīgas datu aizsardzības iestādes), ir jānodrošina, lai būtu pieejami līdzīgi kompensācijas mehānismi, pārsūtot informāciju uz kādu trešo valsti.

— Kompensācija – iepriekš minētu iemeslu dēļ cilvēkiem vajadzētu izmantot alternatīvas tiesību aizsardzības iespējas, konkrēti – izmantojot neatkarīgas pārraudzības iestādes, kā arī tiesas (tribunālus).

— Datu glabāšana – datu glabāšanas ilguma pamatojums var nebūt pārskatāms. Ir jāparedz tādi pasākumi, kas datu subjektiem vai pārraudzības iestādēm neliegtu efektīvi īstenot tiesības.

([20]) — ANO pamatnostādnes datorizētu personas datņu jautājumos, kuras Ģenerālā Asambleja ir pieņēmusi 1990. gada 14. decembrī, ir pieejamas internetā – www.unhchr.ch/html/menu3/b/71.htm
— Eiropas Padomes personas datu automātiskas apstrādes jomā pieņemtā indivīdu aizsardzības konvencija, 1981. gada 28. janvāris, pieejama internetā – www.conventions.coe.int/treaty/en/Treaties/html/108.htm
— EDSO pamatnostādnes privātuma un personas datu pārrobežu plūsmu aizsardzībai, pieņemta 1980. gada 23. septembrī, pieejama internetā –www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html
— Projekts Padomes pamatlēmumam par tādu personas datu aizsardzību, ko apstrādā, policijai un tiesu iestādēm sadarbojoties krimināllietās, pieejams internetā http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=193371
— Eiropas Parlamenta un Padomes Direktīva 95/46/EK (1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti, OV L 281, 23.11.1995., 31. lpp.

([21]) Darba dokuments (1998. gada 24. jūlijs) par personas datu pārsūtīšanu trešām valstīm – kā piemērot ES datu aizsardzības direktīvas 25. un 26. pantu; WP12.

— Tiesībaizsardzības iestāžu atbildība – ja nav efektīvas pārskatāmības, kontroles mehānismi, ko izmanto ieinteresētas personas vai struktūras, nekādi nevar būt plaši. Būtiski tomēr ir izveidot stabilus kontroles mehānismus, ņemot vērā datu diskrētumu un to, ka apstrādāto datu dēļ pret cilvēkiem var vērst piespiedu pasākumus. Atbildība ir nopietna problēma no saņēmējas valsts kontroles mehānismu viedokļa, bet arī, atkarībā no tā, kādas ir pārskatīšanas iespējas datu izcelsmes valstī vai reģionā. Pārskatīšanas mehānismi ir paredzēti konkrētos nolīgumos, piem., PDR nolīgumā, un EDAU sirsnīgi iesaka tos iekļaut arī vispārējā instrumentā.

V. **PRINCIPU ANALĪZE**

Ievads

57. *HLCG* dokumentā iekļautos 12 principus šajā nodaļā analizēs no šādas perspektīves –

— šie principi liecina par to, ka gan ASV, gan ES ir kopīgi uzskati par principu piemērošanas līmeni, jo ir saskatāma līdzība ar 108. konvencijas principiem.

— Tomēr nepietiek noslēgt nolīgumu par principu piemērošanas līmeni. Juridiskajam instrumentam būtu jābūt pietiekami stipram, lai nodrošinātu tā ievērošanu.

— EDAU nožēlo, ka principiem nav pievienots paskaidrojuma raksts.

— Būtu jāsaprot, ka, pirms sākt principu aprakstīšanu, abām pusēm ir vienādi jāsaprot izmantotais formulējums, piemēram, saistībā ar jēdzienu par personas informāciju vai par cilvēkiem, ko aizsargā. Tādā ziņā ļoti noderētu definīcijas.

1. Konkrēti izstrādāti mērķi

58. Pirmais *HLCG* pārskata ziņojuma minētais princips paredz, ka personas informāciju apstrādā likumīgām tiesībaizsardzības vajadzībām. Kā iepriekš minēts, tas nodod Eiropas Savienībai kriminālnoziegumu novēršanu, konstatāciju, izmeklēšanu vai ar tiem saistītu tiesvedību. Amerikas Savienotajās Valstīs tomēr tiesībaizsardzības interpretācija sniedzas tālāk par kriminālnoziegumiem, un pie tās pieder "robežu apsardzības, sabiedrības drošības un valsts drošības vajadzības". Nav skaidrs, kādas sekas būs tādām ES un ASV definēto mērķu nesaskaņām. Lai gan pārskata ziņojumā ir minēts, ka praksē mērķi visnotaļ var saskanēt, ir svarīgi precīzi zināt, ciktāl tie *nesaskan*. Tiesībaizsardzības jomā, ņemot vērā veikto pasākumu sekas cilvēkiem, mērķu aprobežošanas princips ir stingri jāievēro, un definētajam mērķim ir jābūt skaidram un paredzētam. Ņemot vērā pārskata ziņojumā minēto savstarpējību, arī šķiet būtiski tuvināt minētos mērķus. Īsumā – ir vajadzīgs skaidrojums, kā jāsaprot minētais princips.

2. Integritāte/datu kvalitāte

59. EDAU ir gandarīts par to, ka ir paredzēts noteikums, kas prasa akurātu, atbilstīgu, savlaicīgu un pilnīgu personas informāciju, kura ir vajadzīga likumīgai apstrādei. Tāds princips ir pamatnosacījums efektīvai datu apstrādei.

3. Vajadzība un samērība

60. Ar minēto principu kļūst skaidra savstarpēja savāktās informācijas saistība ar vajadzību pēc tādas informācijas, lai sasniegtu tiesību aktos fiksēto tiesībaizsardzības mērķi. Tāda prasība pēc tiesiskas bāzes ir pozitīvs elements, kas apliecina datu apstrādes likumīgumu. EDAU norāda, ka, lai gan tas stiprina juridisku skaidrību par datu apstrādi, tomēr apstrādes juridiskais pamats ir kādas trešās valsts tiesības. Kādas trešās valsts tiesību akti vien nevar būt likumīgs pamats personas datu pārsūtīšanai ([22]). *HLCG* pārskata ziņojuma kontekstā šķiet pieņemts, ka trešās valsts, t. i., Amerikas Savienoto Valstu tiesību likumīgums ir būtībā atzīts. Būtu jātur prātā, ja tāda domu gaita šajā gadījumā var būt pamatota, ņemot vērā, ka ASV ir demokrātiska valsts, tāds pats modelis nedarbotos attiecībās ar kuru katru citu trešo valsti, un to nevarētu transponēt.

61. Saskaņā ar *HLCG* pārskata ziņojuma pielikumu personas datu pārsūtīšanai ir jābūt būtiskai, vajadzīgai un pareizai. EDAU uzsver, ka, lai apstrāde būtu samērīga, tā nedrīkst nevajadzīgi jaukties privātā dzīvē, un apstrādes mehānismiem ir jābūt līdzsvarotiem, ņemot vērā datu subjektu tiesības un intereses.

62. Minētā iemesla dēļ piekļuvei to informācijai būtu jānotiek, katru konkrētu gadījumu izskatot atsevišķi, atkarībā no praktiskām konkrētas izmeklēšanas vajadzībām. Trešās valsts tiesībaizsardzības iestādēm dota pastāvīga piekļuve ES datu bāzēm būtu jāuzskata par nesamērīgu un nepietiekami pamatotu. EDAU atgādina, ka pat noslēgto datu

([22]) Konkrēti skat. Direktīvas 95/46/EK 7. panta c) un e) punktu. 29. panta darba grupa 2002. gada 24. oktobra atzinumā Nr. 6/2002 par pasažieru sniegtās informācijas (*Passenger Manifest Information*) un citu no aviosabiedrībām saņemtu datu pārsūtīšanu Savienotajām Valstīm, konstatēja, ka "nešķiet pieņemams, ka trešās valsts vienpusējam, savās interesēs pieņemtam lēmumam vajadzētu likt regulāri pārsūtīt visus datus, ko aizsargā ar minēto direktīvu".

apmaiņas nolīgumu kontekstā, piem., PDR nolīguma gadījumā, datu apmaiņa balstās uz konkrētiem apstākļiem un to noslēdz uz konkrētu laiku ([23]).

63. Pēc tās pašas loģikas būtu jāregulē datu glabāšanas laiks – dati būtu jāglabā tikai tik ilgi, cik vajadzīgs, ņemot vērā konkrētus mērķus, kas jāsasniedz. Ja tie vairs nav svarīgi saistībā ar apzināto mērķi, tie būtu jādzēš. EDAU nopietni iebilst pret tādu datu noliktavu izveidi, kurās glabātos informācija par cilvēkiem, ko netur aizdomās, – gaidot, kad to ievajadzēsies.

4. Informācijas aizsardzība

64. Pasākumi un procedūras, sargājot datus pret neatļautu lietojumu, grozīšanu un citiem apdraudējumiem, ir izstrādāti minētajos principos, kā arī noteikums, ar ko piekļuve ir dota tikai īpaši pilnvarotiem cilvēkiem. EDAU uzskata, ka ar to pietiek.

65. Turklāt principu varētu papildināt ar noteikumu, kurā būtu minēts, ka ir jāveic to personu uzskaite, kuras piekļūst datiem. Tas stiprinās drošības pasākumu efektivitāti, lai ierobežotu piekļuvi datiem un novērstu to nelikumīgu lietojumu.

66. Turklāt būtu jāparedz savstarpēja informēšana drošības pārkāpumu gadījumos – datu saņēmēji ASV, kā arī Eiropas Savienībā būtu atbildīgi par partneru informēšanu, ja viņu saņemtie dati ir nelikumīgi darīti atklātībā pieejami. Tas palīdzēs stiprināt atbildību par datu apstrādes drošību.

5. Īpašu kategoriju personas informācija

67. Princips, kas aizliedz konfidenciālu datu apstrādi, pēc EDAU uzskatiem ir jūtami vājināts ar izņēmumu, ar ko vispār ir pieļauta tādu konfidenciālu datu apstrāde, kuriem attiecīgas valsts tiesības paredz "pienācīgus drošības pasākumus". Tieši tāpēc, ka dati ir konfidenciāli, jebkāda atkāpe no aizlieguma principa ir attiecīgi un precīzi jāpamato, uzskaitot vajadzības, un apstākļus, kādos apzinātu tipu konfidenciālus datus var apstrādāt, kā arī – norādot, kādai ir jābūt datu apstrādātāju kvalifikācijai, lai viņi būtu tiesīgi apstrādāt tāda veida datus. EDAU uzskata, ka, lai arī būtu jāparedz dažādi drošības pasākumi, konfidenciāliem datiem nevajadzētu būt elementam, kas varētu ierosināt izmeklēšanu. Tie varētu būt pieejami konkrētos apstākļos, bet tikai kā papildu informācija par datu subjektiem, kuru lietas jau izmeklē. Principa formulējumā tādi drošības pasākumi un nosacījumi ir jānumurē tā, lai to skaitu nevarētu patvarīgi palielināt.

6. Atbildība

68. Kā izvērsti skaidrots šī atzinuma 55. un 56. punktā, faktiski jānodrošina to attiecīgo valstu iestāžu struktūru atbildība, kuras apstrādā personas datus, un nolīgumā jādod garantijas par to, kā šādu atbildību nodrošinās. Tas ir vēl jo svarīgāk, ņemot vērā to, ka trūkst pārskatāmības, ko ierasti saista ar personas datu apstrādi tiesībaizsardzības kontekstā. Tādējādi, ja to, ka valsts struktūras ir atbildīgas, piemin, sīkāk neskaidrojot atbildības mehānismus un sekas, – kā tagad ir darīts pielikumā – tā nav pietiekama garantija. EDAU iesaka skaidrojumu dot pašā instrumentā.

7. Neatkarīga un efektīva pārraudzība

69. EDAU pilnībā atbalsta, ka tiktu iekļauts noteikums, kurā būtu paredzēta neatkarīga un efektīva pārraudzība, ko veic viena vai vairākas atklātas pārraudzības iestādes. Viņš uzskata, ka būtu skaidri jānosaka, kā interpretēt neatkarību, it īpaši to, no kā minētās iestādes ir neatkarīgas, un kam tās ir pakļautas. Ir vajadzīgi attiecīgi kritēriji, kuros būtu ņemta vērā organizatoriska un funkcionāla neatkarība no izpildvaras un likumdošanas struktūrām. EDAU atgādina, ka būtisks ir elements – nodrošināt efektīvu to principu ievērošanu, par ko ir panākta vienprātība. Šo iestāžu iejaukšanās un to pilnvaru īstenošana arī ir būtiski svarīga, ņemot vērā jautājumu par valstu iestāžu atbildību par personas datu apstrādi, kā minēts iepriekš. Datu subjektiem datu pastāvēšana un to kompetences būtu jādara skaidri redzamas, lai tie varētu īstenot tiesības, it īpaši, ja vairākas iestādes ir kompetentas atkarībā no apstrādes konteksta.

70. Turklāt EDAU iesaka nākotnē iespējamā nolīgumā paredzēt arī pārraudzības iestāžu savstarpējas sadarbības mehānismus.

8. Individuāla piekļuve un tiesiskas aizsardzības līdzekļi

71. Konkrētas garantijas ir vajadzīgas, tiesībaizsardzības kontekstā runājot par piekļuvi un tiesiskas aizsardzības līdzekļiem. Tādā sakarā EDAU ir gandarīts par principu, kas paredz, ka cilvēkiem ir nodrošināta/vajadzētu nodrošināt piekļuvi un līdzekļus, lai "labotu un/vai svītrotu savu personas informāciju". Tomēr ir palikušas dažas neskaidrības par indivīdu definīciju (būtu jāaizsargā visi datu subjekti, un ne tikai attiecīgas valsts pilsoņi), un apstākļi, kādos indivīdi varētu iebilst pret viņu informācijas apstrādi. Ir jāprecizē, kādos "attiecīgos gadījumos" iebildumus var

([23]) Minētais nolīgums un ar to saistītās saistības beigsies un pārstās būt spēkā septiņus gadus pēc parakstīšanas dienas, ja vien Puses savstarpēji nevienojas to aizstāt.

celt, un kādos ne. Datu subjektiem būtu jābūt skaidram, kādos apstākļos, – atkarībā piem., no iestādes tipa, izmeklēšanas tipa vai citiem kritērijiem – viņi varēs īstenot savas tiesības.

72. Turklāt, ja nav tiešas iespējas pamatoti iebilst pret apstrādi, būtu jābūt iespējai veikt netiešu pārbaudi, ar tādas neatkarīgas iestādes starpniecību, kura ir atbildīga par apstrādes pārraudzību.

9. Pārskatāmība un paziņojumi

73. EDAU atkārtoti uzsver to, cik svarīga ir efektīva pārskatāmība, lai indivīdi varētu īstenot tiesības, un vairotu vispārēju attiecīgas valsts iestāžu atbildību par personas datu apstrādi. Viņš atbalsta izstrādātos principus, un īpaši izceļ to, ka ir vajadzīga *gan* vispārēja paziņošana, *gan* individuāla paziņošana attiecīgam indivīdam. Tas atspoguļojas pielikuma 9. punktā ietvertajā principā.

74. Tomēr pārskata ziņojuma 2, A. B nodaļā ("principi, par ko ir panākta vienprātība") ir minēts, ka Amerikas Savienotajās Valstīs pārskatāmība var ietvert "individuālu vai kompleksu publikāciju Federālajā reģistrā, individuālu paziņošanu, un darīšanu atklātībā pieejamu tiesas prāvā". Ir jābūt skaidram, ka ar publikāciju oficiālā vēstnesī vien nepietiek, lai garantētu pietiekamu datu subjekta informētību. Līdztekus vajadzībai pēc individuāla paziņojuma, EDAU atgādina, ka informācija ir jānodrošina tādā formā un valodā, kas datu subjektam ir viegli saprotama.

10. Kompensācija

75. Lai garantētu tiesību efektīvu īstenošanu, cilvēkiem ir jāvar celt sūdzības neatkarīgās datu aizsardzības iestādēs, un viņiem ir jābūt pieejamiem tiesiskas aizsardzības līdzekļiem neatkarīgā un objektīvā tiesā (tribunālā). Abiem kompensācijas līdzekļiem būtu jābūt vienādi pieejamiem.

76. Piekļuve neatkarīgai datu aizsardzības iestādei ir vajadzīga, jo tā nodrošina elastīgu un lētāku palīdzību kontekstā – tiesībaizsardzībā –, kas cilvēkiem var būt samērā neizprotams. Datu aizsardzības iestādes var arī nodrošināt palīdzību, īstenojot piekļuvi tiesībām datu subjektu vārdā, ja izņēmumi viņiem liedz tiešu piekļuvi saviem personas datiem.

77. Piekļuve tiesu sistēmai ir papildu un obligāta garantija tam, ka datu subjekti var censties panākt kompensāciju iestādē, kas pieder pie tāda demokrātiskas sistēmas atzara, kurš ir nošķirts no tām valsts iestādēm, kuras reāli apstrādā viņu datus. Tādi efektīvi tiesiskas aizsardzības līdzekļi ir Eiropas Tiesā ([24]) atzīti par "būtiskiem, lai indivīdiem nodrošinātu efektīvu tiesību aizsardzību. (...) (Tie) atspoguļo vispārēju Kopienas tiesību principu, kas ir dalībvalstu vispārpieņemto konstitucionālo tradīciju pamatā un ir ierakstīts Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijas 6. un 13. pantā." Tas, ka pastāv tiesiskas aizsardzības līdzekļi, ir arī skaidri paredzēts Eiropas Savienības Pamattiesību hartas 47. pantā un EK Direktīvas 95/46/EK 22. pantā, neskarot nekādus administratīvus aizsardzības līdzekļus.

11. Automatizēti individuāli lēmumi

78. EDAU ir gandarīts par noteikumu, ar ko ir paredzēti attiecīgi drošības pasākumi personas informācijas automatizētas apstrādes gadījumā. Viņš norāda, ka vienota izpratne par to, ko uzskatīt par "nopietnu nelabvēlīgu darbību pret būtiskām indivīda interesēm" palīdzētu noskaidrot minētā principa piemērojuma apstākļus.

12. Pārsūtīšana tālāk

79. Daži nosacījumi, kas ir izvirzīti datu tālākai pārsūtīšanai, nav skaidri. Konkrēti, ja pārsūtīšanai tālāk ir jāatbilst starptautiskiem mehānismiem un nolīgumiem, ko savā starpā ir noslēgušas valstis, kas sūta un saņem datus, būtu jāprecizē, vai tas attiecas uz to abu valstu savstarpējiem nolīgumiem, kas ir sākušas pārsūtīt datus, vai divām valstīm, kas ir iesaistītas tālākā pārsūtīšanā. Pēc EDAU domām, to divu valstu savstarpējiem nolīgumiem, kuras ir sākušas pārsūtīšanu, noteikti ir jābūt noslēgtiem.

80. EDAU arī norāda, ka "likumīgas valsts intereses", ar ko pieļauj datu tālāku pārsūtīšanu, ir definētas ļoti plaši. Valsts drošības joma paliek neskaidra, un datu pārsūtīšanas attiecināšana uz gadījumiem, kad ir pārkāptas ētikas normas vai noteikumi par regulētām profesijām šķiet nepamatota un tiesībaizsardzības kontekstā pārmērīga.

VI. **SECINĀJUMI**

81. EDAU ir gandarīts par ES un ASV iestāžu kopīgo veikumu tiesībaizsardzības jomā, kur datu aizsardzība ir būtiski svarīga. Viņš tomēr grib uzsvērt, ka problēma ir sarežģīta, konkrēti no precīzas darbības jomas un būtības viedokļa, un tālab tā ir pelnījusi rūpīgu un nopietnu analīzi. Transatlantiska instrumenta iespaids uz datu aizsardzību būtu

([24]) Lieta 222/84 *Johnston* [1986] *ECR* 1651; lieta 222/86 *Heylens* [1987] *ECR* 4097; lieta C-97/91 *Borelli* [1992] *ECR* I-6313).

rūpīgi jāapsver saistībā ar esošo tiesisko sistēmu un sekām, ko tas rada pilsoņiem.

82. EDAU aicina panākt lielāku skaidrību un konkrētus noteikumus, it īpaši šādos aspektos –

— noskaidrot instrumenta būtību, kuram būtu jāuzliek juridiskas saistības, lai nodrošinātu pietiekamu juridisku skaidrību;

— būtu jāveic rūpīga piemērotības analīze, balstoties uz nopietnām prasībām pret projekta būtību, īpašiem aspektiem un pārraudzību. EDAU uzskata, ka vispārēja instrumenta piemērotību varētu atzīt tikai apvienojumā ar attiecīgiem konkrētiem nolīgumiem katrā konkrētā gadījumā.

— Aprakstīt piemērojuma jomu, dot skaidru un vienotu definīciju, kādas tiesībaizsardzības vajadzības ir liktas uz spēles;

— precizēt, kādi ir mehānismi, ar ko varētu privātas struktūras iesaistīt datu pārsūtīšanas shēmās;

— ievērot samērības principu, datu apmaiņu paredzot, katru konkrētu gadījumu izskatot atsevišķi, ja ir konkrēta vajadzība;

— stipri pārraudzības mehānismi, kā arī datu subjektiem pieejami kompensāciju mehānismi, un administratīvi un tiesiskas aizsardzības līdzekļi;

— efektīvi pasākumi, kas visiem datu subjektiem garantētu tiesību īstenošanu neatkarīgi no pilsonības;

— neatkarīgu datu aizsardzības iestāžu iesaiste, it īpaši saistībā ar pārraudzību un palīdzību datu subjektiem.

83. EDAU uzsver, ka būtu jāvairās no steigas principu izstrādē, jo tā liktu pieņemt nepietiekamus risinājumus, kuru sekas būtu pretējas tām, kas ir iecerētas no datu aizsardzības viedokļa. Tālab labākais, ko tagad darīt, lai virzītos uz priekšu, būtu izstrādāt ceļvedi, lai vēlākā stadijā, iespējams, noslēgtu nolīgumu.

84. EDAU arī aicina panākt lielāku pārskatāmību datu aizsardzības principu izstrādē. Tikai ar visu ieinteresēto personu, arī Eiropas Parlamenta, iesaisti par instrumentu varētu notikt demokrātiskas debates, un tas varētu gūt vajadzīgo atbalstu un atzīšanu.

Briselē, 2008. gada 11. novembrī

Peter HUSTINX

Eiropas datu aizsardzības uzraudzītājs