Eiropas Datu aizsardzības uzraudzītāja atzinums par Komisijas Paziņojumu Eiropas Parlamentam un Padomei – "ES iekšējās drošības stratēģija darbībā – pieci soļi pretim drošākai Eiropai"

(2011/C 101/02)

EIROPAS DATU AIZSARDZĪBAS UZRAUDZĪTĀJS,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 16. pantu,

ņemot vērā Eiropas Savienības Pamattiesību hartu un jo īpaši tās 7. un 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 šādu datu brīvu apriti ([1]),

ņemot vērā lūgumu sniegt atzinumu saskaņā ar Regulu (EK) Nr. 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti ([2]), un jo īpaši tās 41. pantu,

IR PIEŅĒMIS ŠO ATZINUMU.

I. IEVADS

1. Komisija 2010. gada 22. novembrī pieņēma Paziņojumu ar nosaukumu "ES iekšējās drošības stratēģija darbībā – pieci soļi pretim drošākai Eiropai" (turpmāk tekstā – Paziņojums) ([3]). Paziņojums tika nosūtīts EDAU apspriešanai.

2. EDAU pauž gandarījumu par to, ka Komisija tam lūdz atzinumu. Jau pirms Paziņojuma pieņemšanas EDAU sniedza neoficiālas piezīmes par teksta projektu, un Paziņojuma galīgajā redakcijā dažas no tām ir ņemtas vērā.

Paziņojuma pamatojums

3. ES iekšējās drošības stratēģija (turpmāk tekstā – "IDS"), kam veltīts Paziņojums, tika pieņemta 2010. gada 23. februārī Spānijas prezidentūras laikā ([4]). Stratēģijā izklāstīts Eiropas drošības modelis, kas līdz ar citām darbībām integrē arī pasākumus tiesībaizsardzībā un tiesu sadarbībā, robežu pārvaldībā un civilajā aizsardzībā, pienācīgi ievērojot kopējās Eiropas vērtības, piemēram, pamattiesības. Tās galvenie mērķi ir šādi:

— iepazīstināt sabiedrību ar esošajiem ES instrumentiem, kas jau palīdz nodrošināt ES pilsoņu drošību un brīvību, un ar pievienoto vērtību, ko ES darbības rada šajā jomā;

— tālāk izstrādāt kopīgus rīkus un politiku, pamatojoties uz dziļāk integrētu pieeju, kas pievēršas nedrošības cēloņiem, nevis tikai sekām;

— nostiprināt tiesībaizsardzības un tiesu iestāžu sadarbību, robežu pārvaldību, civilo aizsardzību un katastrofu pārvaldību.

4. IDS mērķis ir risināt steidzamākos ES drošības apdraudējumus un problēmas, piemēram, smago noziegumu un organizētās noziedzības, terorisma un kibernoziegumu, kā arī ES ārējo robežu pārvaldības jomā, un nostiprināt pretestības spējas dabas un cilvēku izraisītām katastrofām. Stratēģija paredz vispārīgas vadlīnijas, principus un virzienus par to, kā ES vajadzētu reaģēt uz šīm problēmām, un tā aicina Komisiju piedāvāt laikus ieplānotus pasākumus šīs stratēģijas īstenošanai.

5. Turklāt šajā jautājumā ir svarīgi atsaukties uz nesenajiem Tieslietu un iekšlietu Padomes secinājumiem par ES politikas cikla izveidi un ieviešanu, lai apkarotu starptautiskos smagos noziegumus un organizēto noziedzību, kuri pieņemti 2010. gada 8.–9. novembrī ([5]) (turpmāk tekstā – "2010. gada novembra secinājumi"). Šajā dokumentā ir ņemts vērā Padomes 2006. gada secinājums par iekšējās drošības arhitektūru ([6]), un tas aicina Padomi un Komisiju definēt visaptverošu IDS, balstoties uz kopīgajām ES vērtībām un principiem, kas vēlreiz apstiprināti ES Pamattiesību hartā. ([7])

([1]) OV L 281, 23.11.1995., 31. lpp.
([2]) OV L 8, 12.1.2001., 1. lpp.
([3]) COM(2010) 673 galīgā redakcija.
([4]) Dok. 5842/2/10.
([5]) Tieslietu un iekšlietu Padomes 3043. sanāksme, 2010. gada 8.–10. novembris, Brisele.
([6]) Dok. 7039/2/06 TI 86 *CATS* 34.
([7]) ES politikas ciklu attiecībā uz smagiem starptautiskiem noziegumiem un organizēto noziedzību, kas izskatīts 2010. gada novembra secinājumos, veido četri posmi: 1) politikas izstrāde, pamatojoties uz Eiropas Savienības Smago noziegumu un organizētās noziedzības radītā apdraudējuma novērtējumu *(EU SOCTA)*, 2) politikas mehānismi un lēmumu pieņemšana, kad Padome ir apzinājusi ierobežotu skaitu prioritāšu, 3) ikgadējā Operatīvās darbības plāna *(OAP)* īstenošana un uzraudzība un 4) politikas cikla beigās – rūpīgs izvērtējums, kas vienlaikus atvieglo arī nākamā politikas cikla norisi.

6. No visiem virzieniem un mērķiem, kam jāvirza IDS īstenošana, 2010. gada novembra secinājumi pievēršas pārdomām par apsteidzošu un uz izlūkošanu balstītu pieeju, ciešākai sadarbībai starp ES aģentūrām, tostarp informācijas apmaiņas tālākai uzlabošanai starp šīm aģentūrām, kā arī mērķim attiecībā uz pilsoņu informēšanu par tā ES darba svarīgumu, kas vērsts uz viņu aizsardzību. Turklāt secinājumi aicina Komisiju kopā ar attiecīgo aģentūru speciālistiem un dalībvalstīm izstrādāt daudzgadu stratēģisko plānu (turpmāk tekstā – "MASP") attiecībā uz katru prioritāti, definējot atbilstošāko stratēģiju problēmas risināšanai. Tie arī aicina Komisiju, apspriežoties ar dalībvalstu un ES aģentūru speciālistiem, izstrādāt neatkarīgu mehānismu *MASP* īstenošanas novērtēšanai. EDAU atgriezīsies pie šiem jautājumiem vēlāk šajā atzinumā, jo tie ir cieši saistīti un tiem ir būtiska ietekme uz personas datu, privātuma un citu saistītu pamattiesību un brīvību aizsardzību.

Paziņojuma saturs un mērķis

7. Paziņojumā ir piedāvāti pieci stratēģiskie mērķi, kuriem visiem ir saistība ar privātumu un datu aizsardzību:

— sagraut starptautiskos noziedznieku tīklus;

— novērst terorismu un risināt jautājumus saistībā ar radikalizēšanos un vervēšanu;

— uzlabot pilsoņu un uzņēmumu drošību kibertelpā;

— drošības stiprināšana, izmantojot robežu pārvaldību, un

— uzlabot Eiropas izturētspēju krīzes un katastrofu gadījumos.

8. *IDS darbībā*, ko piedāvā Komisija, paredz kopīgu darba kārtību dalībvalstīm, Eiropas Parlamentam, Komisijai, Padomei, aģentūrām un citiem, tostarp pilsoniskajai sabiedrībai un vietējām pašvaldībām, un tā piedāvā veidu, kā tiem visiem būtu jāstrādā kopā nākamos četrus gadus, lai sasniegtu IDS mērķus.

9. Paziņojuma pamatā ir Lisabonas līgums, un tas atzīst Stokholmas programmas (un tās Rīcības plāna) piedāvātās vadlīnijas, kas 4.1. nodaļā uzsver nepieciešamību sagatavot visaptverošu IDS, pamatojoties uz pamattiesību ievērošanu, starptautisku aizsardzību un tiesiskumu. Turklāt saskaņā ar Stokholmas programmu iekšējās drošības stratēģijas izstrādei, uzraudzībai un īstenošanai ir jākļūst par vienu no prioritārajiem uzdevumiem Iekšējās drošības komitejai *(COSI)*, kas izveidota saskaņā ar Līguma par Eiropas Savienības darbību 71. pantu. Lai nodrošinātu efektīvu IDS īstenošanu, tai ir jāaptver arī integrētās robežu pārvaldības drošības aspekti un vajadzības gadījumā – arī tiesu sadarbība krimināllietās, kas attiecas uz operatīvo sadarbību iekšējās drošības jomā. Šajā jautājumā ir svarīgi arī norādīt, ka Stokholmas programma aicina piemērot IDS integrētu pieeju, ņemot vērā arī ES izstrādāto ārējās drošības stratēģiju, kā arī citas ES politikas, jo īpaši tās, kas attiecas uz iekšējo tirgu.

Atzinuma mērķis

10. Paziņojums attiecas uz dažādām politikas jomām, kas ietilpst plaši izprastā Eiropas Savienības "iekšējās drošības" jēdzienā vai ietekmē to.

11. Šā atzinuma mērķis nav analizēt visas politikas jomas un konkrētos tematus, kam pievēršas Paziņojums, bet gan:

— apskatīt Paziņojumā piedāvātos IDS mērķus no īpaša – privātuma un datu aizsardzības – viedokļa, un, pamatojoties uz to, uzsvērt vajadzīgās saites ar citām stratēģijām, kas pašlaik tiek apspriestas un pieņemtas ES līmenī;

— precizēt datu aizsardzības priekšstatu un jēdzienu skaitu, kas jāņem vērā, ES līmenī izstrādājot, papildinot un īstenojot IDS;

— atbilstošos vajadzības gadījumos sniegt ierosinājumus par to, kā datu aizsardzības problēmas var labāk ņemt vērā, īstenojot Paziņojumā piedāvātās darbības.

12. EDAU to darīs, jo īpaši uzsverot saistību starp IDS un Informācijas pārvaldības stratēģiju, kā arī darbu pie visaptveroša datu aizsardzības regulējuma. Turklāt EDAU izmantos tādus jēdzienus kā – labākās pieejamās metodes un "modelētais privātums", privātuma un datu aizsardzības ietekmes novērtējums un datu subjektu tiesības, kas tieši ietekmē IDS izstrādi un īstenošanu. Atzinumā būs sniegtas arī piezīmes par daudzām izvēlētām politikas jomām, piemēram, integrēto robežu pārvaldību, tostarp *EUROSUR* un personas datu apstrādi, ko veic *FRONTEX*, kā arī citām jomām, piemēram, kibertelpu un *TFTP*.

II. VISPĀRĪGAS PIEZĪMES

Vajadzība pēc vispusīgākas, ietverošākas un "stratēģiskākas" pieejas ES stratēģijām, kas attiecas uz IDS

13. Daudzas ES stratēģijas, kas balstītas uz Lisabonas līgumu un Stokholmas programmu un tieši vai netieši ietekmē datu aizsardzību, pašlaik tiek apspriestas un piedāvātas ES līmenī. IDS ir viena no tām, un tā ir cieši saistīta ar citām stratēģijām (kas ir izskatītas nesenos Komisijas paziņojumos vai ir paredzētas tuvākajā nākotnē), piemēram, ES Informācijas pārvaldības stratēģija un Eiropas Informācijas apmaiņas modelis, stratēģija ES Pamattiesību hartas īstenošanai, visaptveroša datu aizsardzības stratēģija un ES Pretterorisma politika. Šajā atzinumā EDAU jo īpaši pievēršas saistībai ar Informācijas pārvaldības stratēģiju un visaptverošo datu aizsardzības regulējumu, pamatojoties uz Līguma par Eiropas Savienības darbību 16. pantu, kam no datu aizsardzības viedokļa ir visredzamākā politiskā saistība ar IDS.

14. Visas šīs stratēģijas veido saistīto politikas vadlīniju, programmu un rīcības plānu sarežģītu "kompilāciju", kas aicina izstrādāt visaptverošu un integrētu pieeju ES līmenī.

15. Vispārīgāk runājot, šī "stratēģiju sasaistīšanas" metode, ja tā tiks ņemta vērā nākotnes darbībās, atklās, ka ES līmenī ir savs skatījums par *ES stratēģijām* un ka šīs stratēģijas un nesen pieņemtie paziņojumi, kas tos papildina, ir cieši saistīti, un šajā gadījumā Stokholmas programma ir kopīgs atskaites punkts tām visām. Tā arī veidotu pozitīvu sinerģiju starp dažādām politikām, kas attiecas uz brīvības, drošības un tiesiskuma jomu, un novērstu jebkādu iespējamu darba dublēšanos šajā jomā. Tikpat svarīgi ir tas, ka šī metode ļautu efektīvāk un saskaņotāk piemērot datu aizsardzības noteikumus attiecībā uz visām saistītajām stratēģijām.

16. EDAU uzsver, ka viens no IDS pīlāriem ir efektīva informācijas pārvaldība Eiropas Savienībā, kam jābūt balstītai uz nepieciešamības un proporcionalitātes principiem, lai pamatotu informācijas apmaiņas nepieciešamību.

17. Turklāt, kā norādīts EDAU atzinumā par Paziņojumu par informācijas pārvaldību ([8]), EDAU uzsver, ka visi jaunie likumdošanas pasākumi, kas atvieglotu personas datu uzglabāšanu un apmaiņu, ir jāpiedāvā tikai tādā gadījumā, ja tiem ir konkrēts nepieciešamības pamatojums ([9]). Īstenojot IDS, šī tiesību aktu prasība ir jāīsteno kā apsteidzošas politikas metode. Nepieciešamība pēc visaptverošas pieejas IDS neizbēgami izraisa arī vajadzību novērtēt visus instrumentus un rīkus, kas iekšējās drošības jomā jau ir pieejami, pirms tiek piedāvāti jauni.

18. Šajā jautājumā EDAU piedāvā arī biežāk izmantot klauzulas, kas paredz periodiski novērtēt esošos instrumentus, piemēram, klauzulu, kas iekļauta pašlaik izvērtējamajā Datu saglabāšanas direktīvā. ([10])

Datu aizsardzība kā IDS mērķis

19. Paziņojums pievēršas personas datu aizsardzībai nodaļā "Drošības politikas jomas, kas balstītas uz kopīgām vērtībām", kurā norādīts, ka instrumentiem un darbībām IDS īstenošanai ir jābūt balstītiem uz mūsu kopīgām vērtībām, tostarp uz tiesiskumu un pamattiesību ievērošanu, kā noteikts ES Pamattiesību hartā. Līdz ar to tas paredz, ka "efektīva tiesībaizsardzība ES tiek veicināta ar informācijas apmaiņu, un šajā sakarā mums ir arī jāaizsargā indivīdu privātums un pamattiesības uz personas datu aizsardzību".

20. Tā ir apsveicama apņemšanās. Tomēr nevar uzskatīt, ka tā pietiekami risina datu aizsardzības problēmu IDS. Paziņojums sīkāk neanalizē datu aizsardzību ([11]) un arī neizskaidro, kā privātuma respektēšana un personas datu aizsardzība tiks nodrošināta praksē – darbībās, ar ko īsteno IDS.

([8]) EDAU 2010. gada 30. septembra atzinums par Komisijas paziņojumu Eiropas Parlamentam un Padomei - "Pārskats par informācijas pārvaldību brīvības, drošības un tiesiskuma jomā".

([9]) Tā ir tiesību aktu prasība; skatīt jo īpaši Eiropas Tiesas 2010. gada 2. novembra spriedumu apvienotajās lietās C-92/09 un C-93/09. Konkrētākos jautājumos EDAU arī citos atzinumos par tiesību aktu priekšlikumiem saistībā ar brīvības, drošības un tiesiskuma jomu ir veicinājis šīs metodes piemērošanu, piemēram, 2005. gada 19. oktobra atzinumā par trim priekšlikumiem attiecībā uz Otrās paaudzes Šengenas informācijas sistēmu *(SIS II)*; 2007. gada 20. decembra atzinumā par priekšlikuma projektu Padomes Pamatlēmumam par Pasažieru datu reģistra *(PNR)* datu izmantošanu tiesībaizsardzības nolūkos; 2009. gada 18. februāra atzinumā par priekšlikumu Regulai par pirkstu nospiedumu salīdzināšanas sistēmas *EURODAC* izveidi, lai efektīvi piemērotu Regulu (EK) Nr. (…/…), (ar ko paredz kritērijus un mehānismus, lai noteiktu dalībvalsti, kura ir atbildīga par trešās valsts valstspiederīgā vai bezvalstnieka starptautiskās aizsardzības pieteikuma izskatīšanu, kas iesniegts kādā no dalībvalstīm); 2009. gada 18. februāra atzinumā par priekšlikumu Regulai, ar ko paredz kritērijus un mehānismus, lai noteiktu dalībvalsti, kura ir atbildīga par trešās valsts valstspiederīgā vai bezvalstnieka starptautiskās aizsardzības pieteikuma izskatīšanu, kas iesniegts kādā no dalībvalstīm; un 2009. gada 7. oktobra atzinumā par priekšlikumiem attiecībā uz tiesībaizsardzības iestāžu piekļuvi *EURODAC*.

([10]) Eiropas Parlamenta un Padomes Direktīva 2006/24/EK (2006. gada 15. marts) par tādu datu saglabāšanu, kurus iegūst vai apstrādā saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu vai publiski pieejamu komunikāciju tīklu nodrošināšanu, un par grozījumiem Direktīvā 2002/58/EK, OV L 105, 13.4.2006., 54. lpp.

([11]) Datu aizsardzība konkrētāk ir pieminēta tikai saistībā ar jautājumu par personas datu apstrādi *FRONTEX*.

21. Pēc EDAU domām, vienam no *IDS darbībā* mērķiem ir jābūt plaši izprastai *aizsardzībai*, kas nodrošinātu *pareizu* līdzsvaru starp pilsoņu aizsardzību pret esošajiem apdraudējumiem, no vienas puses, un viņu privātuma aizsardzību un tiesībām uz personas datu aizsardzību, no otras puses. Citiem vārdiem sakot, drošības un privātuma problēmas ir jāuztver vienādi nopietni, izstrādājot IDS, un tai būtu jāsaskan ar Stokholmas programmu un Padomes secinājumiem.

22. Īsumā, drošības garantēšana un vienlaikus arī pilnīga privātuma ievērošana un datu aizsardzība ir jānorāda kā galvenie ES iekšējās drošības stratēģijas mērķi. Tas ir jāatspoguļo visās darbībās, ko dalībvalstis un ES iestādes veic šīs stratēģijas īstenošanai.

23. Šajā jautājumā EDAU atsaucas uz paziņojumu COM(2010)609 "Vispusīga pieeja personas datu aizsardzībai Eiropas Savienībai". ([12]) EDAU drīzumā sniegs atzinumu par šo paziņojumu, bet šeit tikai uzsver, ka nav iespējams izveidot efektīvu IDS bez nopietnas datu aizsardzības shēmas, kas to papildinātu un sekmētu uzticību un lielāku efektivitāti.

III. **PRIEKŠSTATI UN JĒDZIENI, KO PIEMĒRO IDS IZSTRĀDEI UN ĪSTENOŠANAI**

24. Ir skaidrs, ka dažas darbības, kas izriet no IDS mērķiem, var palielināt riskus attiecībā uz fizisko personu privātuma un datu aizsardzību. Lai šiem riskiem pretdarbotos, EDAU vēlas pievērst īpašu uzmanību tādiem jēdzieniem kā "modelētais privātums", privātuma un datu aizsardzības ietekmes novērtējums, datu subjektu tiesības un labākās pieejamās metodes *(BAT)*. Tie visi ir jāņem vērā IDS īstenošanā, un tie var arī noderēt, izstrādājot vairāk uz privātumu un datu aizsardzību orientētas politikas šajā jomā.

Modelētais privātums

25. EDAU vairākos gadījumos un dažādos atzinumos ir atbalstījis jēdzienu par "neatņemamu" privātumu ("modelētais privātums" vai "privātums pēc definīcijas"). Šis jēdziens pašlaik ir izstrādāts gan privātajam, gan sabiedriskajam sektoram, tādēļ tam ir arī jābūt svarīgai nozīmei attiecībā uz ES iekšējās drošības, kā arī policijas un tiesu jomu. ([13])

26. Paziņojumā šis jēdziens nav pieminēts. EDAU ierosina iekļaut atsauces uz šo jēdzienu mērķvirzītajās darbībās, kas jāpiedāvā un jāuzņemas, lai īstenotu IDS, jo īpaši saistībā ar 4. mērķi "Drošības stiprināšana, izmantojot robežu pārvaldību", kurā ir nepārprotama norāde par jauno tehnoloģiju padziļinātu izmantošanu robežu pārbaudēs un robežu uzraudzībā.

Privātuma un datu aizsardzības ietekmes novērtēšana

27. EDAU rosina Komisiju pārdomāt – turpmākā darba ietvaros pie IDS izstrādes un īstenošanas, pamatojoties uz Paziņojumu – kas ir jāsaprot ar reālu "privātuma un datu aizsardzības ietekmes novērtējumu" *(PIA)* brīvības, drošības un tiesiskuma jomā un jo īpaši IDS.

28. Paziņojumā ir minēti apdraudējuma un riska novērtējumi. Tas ir apsveicami. Tomēr Paziņojums nevienā punktā nepiemin privātuma un datu aizsardzības ietekmes novērtējumus. EDAU ir pārliecināts, ka darbs pie Paziņojuma izpildes IDS jomā ir lieliska iespēja izstrādāt šādus privātuma un datu aizsardzības ietekmes novērtējumus saistībā ar iekšējo drošību. EDAU norāda, ka ne Paziņojums, ne Komisijas Ietekmes novērtēšanas vadlīnijas ([14]) neprecizē šo aspektu un nenosaka to par politikas prasību.

29. Tādēļ EDAU iesaka, īstenojot turpmākos instrumentus, veikt konkrētāku un nopietnāku ietekmes novērtējumu attiecībā uz privātumu un datu aizsardzību – kā atsevišķu novērtējumu vai kā Komisijas veiktā vispārīgā pamattiesību ietekmes novērtējuma daļu. Šajā ietekmes novērtējumā ir ne vien jānorāda pamatprincipi un jāanalizē politikas izvēles, kā tas notiek pašlaik, bet arī jāsniedz ieteikumi par specifiskiem un konkrētiem aizsargpasākumiem.

30. Tādēļ ir jāizstrādā īpaši rādītāji un iezīmes, lai nodrošinātu, ka ikviens priekšlikums, kam ir ietekme uz privātumu un datu aizsardzību ES iekšējās drošības jomā, tiktu rūpīgi apsvērts, tostarp attiecībā uz tādiem aspektiem kā proporcionalitāte, nepieciešamība un mērķa ierobežojuma princips.

31. Turklāt šajā ziņā varētu būt noderīgi atsaukties uz *RFID* ieteikuma ([15]) 4. pantu, kurā Komisija aicināja dalībvalstis nodrošināt, lai nozares speciālisti sadarbībā ar attiecīgajām iesaistītajām personām pilsoniskajā sabiedrībā izstrādātu privātuma un datu aizsardzības ietekmes novērtēšanas regulējumu. Arī Madrides rezolūcija, ko 2009. gada novembrī

([12]) Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai "Vispusīga pieeja personas datu aizsardzībai Eiropas Savienībai", COM (2010) 609.

([13]) EDAU savā atzinumā par Komisijas paziņojumu par Stokholmas programmu ieteica noteikt tiesisku pienākumu informācijas sistēmu veidotājiem un lietotājiem izstrādāt un lietot tādas sistēmas, kas ievēro "modelētā privātuma" principu.

([14]) SEC(2009) 92, 15.1.2009.

([15]) C (2009) 3200 galīgā redakcija, 12.5.2009.

pieņēma Privātuma un datu aizsardzības speciālistu starptautiskā konference, rosināja īstenot *PIA* pirms jaunu informācijas sistēmu un tehnoloģiju ieviešanas personas datu apstrādē vai pirms būtiskām izmaiņām esošajā apstrādē.

Datu subjektu tiesības

32. EDAU norāda, ka Paziņojums īpaši nepievēršas jautājumam par datu subjektu tiesībām, kam ir būtiska nozīme datu aizsardzībā un ir jāietekmē IDS izstrāde. Būtiski ir nodrošināt, lai visās dažādajās sistēmās un instrumentos, kas veltīti ES iekšējai drošībai, personas, uz kurām tie attiecas, varētu izmantot līdzīgas tiesības jautājumā par personas datu apstrādes veidu.

33. Daudzas paziņojumā minētās sistēmas paredz īpašus noteikumus attiecībā uz datu subjektu tiesībām (pievēršoties arī tādām personu kategorijām kā cietušie, aizdomās turētie noziedznieki vai migranti), tomēr ir lielas atšķirības starp dažādām sistēmām un instrumentiem, un tās nav pietiekami pamatotas.

34. Tādēļ EDAU aicina Komisiju tuvākajā nākotnē rūpīgāk iedziļināties šajā jautājumā par datu subjektu tiesību saskaņošanu ES attiecībā uz IDS un Informācijas pārvaldības stratēģiju.

35. Īpašu uzmanību vajadzētu pievērst datu labošanas mehānismiem. IDS ir jāgarantē, lai visos gadījumos, kad fizisko personu tiesības nav pilnībā ievērotas, personas datu kontrolieriem būtu jānodrošina pārsūdzības procedūras, kas būtu viegli izmantojamas, efektīvas un pieejamas.

Labākās pieejamās metodes

36. IDS īstenošana neizbēgami būs balstīta uz IT infrastruktūras izmantošanu, kas nodrošinās Paziņojumā paredzētās darbības. Labākās pieejamās metodes *(BAT)* var uzskatīt par pareiza līdzsvara garantu starp IDS mērķu sasniegšanu un fizisko personu tiesību ievērošanu. Šajā kontekstā EDAU vēlas atkārtot ieteikumu, kas sniegts iepriekšējos atzinumos ([16]) jautājumā par nepieciešamību Komisijai kopā ar nozares pārstāvjiem definēt un atbalstīt konkrētus pasākumus labāko pieejamo metožu piemērošanai. Šī piemērošana nozīmē visefektīvāko un modernāko posmu darbību un to īstenošanas metožu izstrādē, un tā norāda, ka kādas konkrētas metodes ir praktiski piemērotas, lai plānotos rezultātus nodrošinātu efektīvi un saskaņā ar ES privātuma un datu aizsardzības regulējumu. Šāda pieeja pilnībā saskan ar iepriekš minēto "modelētā privātuma" metodi.

37. Attiecīgos gadījumos un iespēju robežās ir jāizstrādā atsauces dokumenti par labākajām pieejamajām metodēm, lai nodrošinātu vadlīnijas un lielāku tiesisko skaidrību attiecībā uz IDS ietvaros paredzēto pasākumu faktisko īstenošanu. Tas varētu arī sekmēt minēto pasākumu labāku saskaņotību dažādās dalībvalstīs. Visbeidzot, bet ne mazāk svarīgi – privātumam un drošībai piemērotu labāko pieejamo metožu definēšana atvieglos datu aizsardzības iestāžu uzraudzības uzdevumu veikšanu, sniedzot tām ar privātumu un datu aizsardzību samērojamas tehniskas norādes, ko pieņēmuši personas datu kontrolieri.

38. EDAU arī norāda, cik svarīgi ir pareizi saskaņot IDS ar darbībām, kas jau ir veiktas saskaņā ar Izpētes un tehnoloģiju attīstības septīto pamatprogrammu un Drošības un brīvību aizsardzības pamatprogrammu. Kopīgs skatījums uz labāko pieejamo metožu nodrošināšanu ļautu ieviest inovācijas attiecībā uz kompetenci un spējām, kas nepieciešamas pilsoņu aizsardzībai, vienlaikus ievērojot arī pamattiesības.

39. Visbeidzot, EDAU uzsver lielo nozīmi, kāda var būt Eiropas Tīklu un informācijas drošības aģentūrai *(ENISA)*, izstrādājot vadlīnijas un novērtējot drošības spējas, kas nepieciešamas IT sistēmu integritātes un pieejamības nodrošināšanai, kā arī šo labāko pieejamo metožu veicināšanai. Ņemot to vērā, EDAU atzinīgi novērtē aģentūras iesaistīšanu, atvēlot tai svarīgāko uzdevumu spēju uzlabošanā cīņā pret kiberuzbrukumiem un kibernoziegumu apkarošanā. ([17])

Dalībnieku un viņu uzdevumu noskaidrošana

40. Šādos apstākļos ir nepieciešami arī plašāki paskaidrojumi par iesaistītajām personām, kas ietilpst IDS sistēmā vai to atbalsta. Paziņojums pievēršas dažādiem dalībniekiem un iesaistītajām personām, piemēram, pilsoņiem, tiesu

([16]) EDAU 2009. gada jūlija atzinums par inteliģentajām (automatizētajām) transporta sistēmām un EDAU 2007. gada decembra atzinums par radiofrekvenču identifikāciju *(RFID)* sakaru jomā; skatīt arī EDAU gada pārskata ziņojumu par 2006. gadu, 48.–49. lpp.

([17]) EDAU paredz, ka atzinums par *ENISA* tiesisko regulējumu tiks pieņemts vēl 2010. gada decembrī.

iestādēm, ES aģentūrām, valstu iestādēm, policijai un uzņēmumiem. Šo dalībnieku konkrētie uzdevumi un kompetence ir plašāk jāiekļauj konkrētās darbībās, kas tiks piedāvātas IDS īstenošanai.

IV. ĪPAŠAS PIEZĪMES PAR POLITIKAS JOMĀM SAISTĪBĀ AR IDS

Integrētā robežu pārvaldība (IRP)

41. Paziņojumā ir norāde par faktu, ka Lisabonas līgums ļauj ES labāk izmantot sinerģiju starp robežu pārvaldības politikām attiecībā uz personām un precēm. Attiecībā uz personu pārvietošanos Paziņojumā teikts, ka "ES migrācijas pārvaldību un cīņu pret noziedzību var uzskatīt par integrētās robežu pārvaldības stratēģijas dubultmērķi". Šis dokuments atzīst robežu pārvaldību par potenciāli spēcīgu līdzekli smago noziegumu un organizētās noziedzības sagraušanā. ([18])

42. EDAU arī norāda, ka Paziņojums definē trīs stratēģiskos virzienus: 1) jaunās tehnoloģijas pastiprināta izmantošana robežpārbaudēm (otrās paaudzes Šengenas informācijas sistēma *(SIS II)*, Vīzu informācijas sistēma *(VIS)*, ieceļošanas/izceļošanas sistēma un reģistrēto ceļotāju programma); 2) jaunās tehnoloģijas pastiprināta izmantošana robežu uzraudzībā (Eiropas Robežu uzraudzības sistēma, *EUROSUR*) un 3) dalībvalstu uzlabota koordinācija ar *FRONTEX* starpniecību.

43. EDAU vēlas izmantot iespēju šajā atzinumā atgādināt savus daudzos iepriekšējos atzinumos izteiktos lūgumus izstrādāt ES līmenī skaidru robežu pārvaldības politiku, kas pilnībā ievērotu datu aizsardzības noteikumus. EDAU uzskata, ka pašreizējais darbs pie IDS un informācijas pārvaldības sniedz ļoti labu iespēju veikt konkrētākus pasākumus, lai izstrādātu saskaņotu politiku šajās jomās.

44. EDAU norāda, ka Paziņojums attiecas ne tikai uz esošajām lielapjoma sistēmām un tām, kuru ekspluatācija var sākties tuvākajā nākotnē (piemēram, *SIS*, *SIS II* un *VIS*), bet arī – savā ziņā – uz sistēmām, kuras Komisija varētu piedāvāt nākotnē, lai gan lēmums par tām vēl nav pieņemts (t. i., reģistrēto ceļotāju programma un ieceļošanas/izceļošanas sistēma). Jāatgādina šajā jautājumā, ka minēto sistēmu ieviešanas mērķi un leģitimitāte joprojām nav izskaidrota un pierādīta, arī ņemot vērā rezultātus, ko sniedz īpaši Komisijas veikti ietekmes novērtējumi. Ja tas nenotiks, Paziņojumu var izprast kā tādu, kas aizsteidzies priekšā lēmumu pieņemšanas procesam un tādēļ neņem vērā faktu, ka vēl nav pieņemts galīgais lēmums par to, vai reģistrēto ceļotāju programma un ieceļošanas/izceļošanas sistēma Eiropas Savienībā ir jāievieš.

45. Tādēļ EDAU ierosina turpmākajā darbā pie IDS ieviešanas izvairīties no šādām apsteidzošām prognozēm. Kā iepriekš teikts, jebkuru lēmumu par jaunu lielapjoma sistēmu ieviešanu, kas var aizskart privātumu, drīkst pieņemt tikai pēc visu esošo sistēmu atbilstīgas novērtēšanas, pienācīgi ņemot vērā nepieciešamību un proporcionalitāti.

EUROSUR

46. Paziņojumā teikts, ka Komisija iesniegs tiesību aktu priekšlikumu par *EUROSUR* izveidi 2011. gadā, lai sekmētu iekšējo drošību un cīņu pret noziedzību. Tajā arī norādīts, ka *EUROSUR* izmantos jaunās tehnoloģijas, kas izstrādātas ES finansētos izpētes projektos un pasākumos, piemēram, fotogrāfisko satelītdatu bāzi, lai atklātu un izsekotu objektus uz jūras robežām, piemēram, izsekotu ātrgaitas kuģus, kas pārvadā narkotikas uz ES.

47. Šajā jautājumā EDAU norāda, ka nav saprotams, vai – un ja tā, tad kādā mērā – tiesību aktu priekšlikums par *EUROSUR*, kuru Komisija iesniegs 2011. gadā, paredzēs arī personas datu apstrādi saistībā ar *EUROSUR*. Paziņojumā Komisija nav paudusi skaidru nostāju šajā jautājumā. Šī problēma ir jo īpaši aktuāla tādēļ, ka Paziņojums nepārprotami sasaista *EUROSUR* un *FRONTEX* taktiskā, operatīvā un stratēģiskā līmenī (skatīt turpmākās piezīmes par *FRONTEX*) un aicina veidot ciešu sadarbību starp šīm divām sistēmām.

Personas datu apstrāde *FRONTEX*

48. EDAU 2010. gada 17. maijā sniedza atzinumu par grozījumiem *FRONTEX* regulā ([19]), un tajā tas aicināja uzsākt patiesas diskusijas un padziļinātas pārdomas par datu aizsardzības jautājumu saistībā ar *FRONTEX* esošo uzdevumu nostiprināšanu un jaunu pienākumu uzdošanu.

49. Paziņojums uzsver nepieciešamību pastiprināt *FRONTEX* darbību uz ārējām robežām saskaņā ar 4. mērķi "Drošības stiprināšana, izmantojot robežu pārvaldību". Saistībā ar to Paziņojums norāda, ka, pamatojoties uz pieredzi un ņemot vērā ES vispārējo pieeju informācijas pārvaldībai, Komisija uzskata, ka *FRONTEX* pilnvarošana apstrādāt un izmantot

([18]) Informācija presei par "ES iekšējās drošības stratēģiju darbībā – pieci soļi pretim drošākai Eiropai", *Memo* 10/598.

([19]) EDAU 2010. gada 17. maija atzinums par priekšlikumu Eiropas Parlamenta un Padomes regulai, ar ko groza Padomes Regulu (EK) Nr. 2007/2004 (2004. gada 26. oktobris), ar ko izveido Eiropas Aģentūru operatīvās sadarbības vadībai pie Eiropas Savienības dalībvalstu ārējām robežām *(FRONTEX)*.

šo informāciju – ierobežotā daudzumā un ievērojot skaidri definētus personas datu pārvaldības noteikumus – ievērojami atvieglos kriminālu organizāciju sagraušanu. Tā ir jauna pieeja, salīdzinot ar Komisijas priekšlikumu par grozījumiem *FRONTEX* regulā, kas pašlaik tiek apspriesti Eiropas Parlamentā un Padomē un neminēja ne vārda par personas datu apstrādi.

50. Saistībā ar visu minēto EDAU atzinīgi novērtē faktu, ka Paziņojums sniedz noteiktu norādi par apstākļiem, kādos šāda apstrāde var izrādīties nepieciešama (piemēram, riska analīzē, darbības uzlabošanā kopīgajās informācijas apmaiņas operācijās ar Eiropolu). Konkrētāk, Paziņojums izskaidro, ka pašlaik informācija par noziedzniekiem, kas iesaistīti kontrabandas tīklos – ar tiem *FRONTEX* nonāk saskarē, nav tālāk izmantojama riska analīzē vai labākā turpmāko operāciju plānošanā. Turklāt attiecīgie dati par aizdomās turētajiem noziedzniekiem nenonāk kompetento valsts iestāžu vai Eiropola rīcībā turpmākai izmeklēšanai.

51. Tomēr EDAU norāda, ka Paziņojums nepievēršas iesāktajai diskusijai par izmaiņām *FRONTEX* tiesiskajā regulējumā, kas – kā jau minēts – attiecas uz šo problēmu, lai piedāvātu tiesiskus risinājumus. Turklāt Paziņojuma tekstu, kurā uzsvērti *FRONTEX* uzdevumi saistībā ar mērķi sagraut kriminālās organizācijas, var izprast kā *FRONTEX* pilnvaru paplašināšanu. EDAU uzskata, ka šis jautājums ir ņemts vērā gan *FRONTEX* regulas grozījumos, gan IDS īstenošanā.

52. EDAU arī vērš uzmanību uz nepieciešamību nodrošināt, lai neveidotos uzdevumu dublēšanās starp Eiropolu un *FRONTEX*. Tādēļ EDAU atzinīgi novērtē to, ka Paziņojums norāda – ir jāizvairās no uzdevumu dublēšanās starp *FRONTEX* un Eiropolu. Tomēr šis jautājums ir arī daudz skaidrāk jārisina gan grozītajā *FRONTEX* regulā, gan IDS īstenošanas darbībās, kas paredz ciešu sadarbību starp *FRONTEX* un Eiropolu. Tas ir jo īpaši svarīgi saistībā ar mērķa ierobežojuma un datu kvalitātes principiem. Šī piezīme attiecas arī uz nākotnes sadarbību ar tādām aģentūrām kā Eiropas Tīklu un informācijas drošības aģentūra *(ENISA)* vai Eiropas Patvēruma atbalsta birojs.

Biometrisko datu izmantošana

53. Paziņojums īpaši nepievēršas tādai pašlaik aktuālai parādībai kā paplašināta biometrisko datu izmantošana brīvības, drošības un tiesiskuma jomā, tostarp attiecībā uz ES lielapjoma IT sistēmām un citiem robežu pārvaldības rīkiem.

54. Tādēļ EDAU izmanto iespēju atgādināt par savu ierosinājumu ([20]), ka šis no datu aizsardzības viedokļa ļoti sensitīvais jautājums ir nopietni jāņem vērā, īstenojot IDS, jo īpaši saistībā ar robežu pārvaldību.

55. EDAU arī iesaka izstrādāt skaidru un stingru politiku attiecībā uz biometrisko datu izmantošanu brīvības, drošības un tiesiskuma jomā, pamatojoties uz nopietnu novērtējumu un katra gadījuma atsevišķu izvērtējumu jautājumā par nepieciešamību izmantot biometriskos datus saistībā ar IDS, pilnībā ievērojot tādus datu aizsardzības pamatprincipus kā proporcionalitāte, nepieciešamība un mērķa ierobežojums.

Teroristu finansēšanas izsekošanas programma (*TFTP*)

56. Paziņojums informē, ka Komisija 2011. gadā izstrādās ES līmeņa politiku, kā iegūt un analizēt finanšu ziņojumapmaiņas datus, kas glabājas ES teritorijā. Saistībā ar to EDAU atgādina savu 2010. gada 22. jūnija atzinumu par finanšu ziņojumapmaiņas datu apstrādi un nodošanu no ES uz ASV, lai īstenotu Teroristu finansēšanas izsekošanas programmu *(TFTP II)* ([21]). Visas kritiskās piezīmes, kas izteiktas šajā atzinumā, tikpat lielā mērā attiecas uz un ir piemērojamas saistībā ar paredzamo darbu pie ES regulējuma izstrādes jautājumā par finanšu ziņojumapmaiņas datiem. Tādēļ tās ir jāņem vērā diskusijās par šo jautājumu. Īpaša uzmanība jāpievērš lielu datu apjomu iegūšanas un apstrādes proporcionalitātei attiecībā uz cilvēkiem, kas netiek turēti aizdomās, kā arī efektīvai pārraudzībai, ko veic neatkarīgas iestādes un tiesas.

Pilsoņu un uzņēmumu drošība kibertelpā

57. EDAU atzinīgi vērtē lielo uzmanību, kas Paziņojumā veltīta profilakses pasākumiem ES līmenī, un uzskata, ka drošības pastiprināšana IT tīklos ir būtisks faktors, kas sekmē labi attīstītu informācijas sabiedrību. EDAU arī atbalsta konkrētus pasākumus, kas uzlabo rīcības spējas kiberuzbrukumu gadījumos, spēju attīstīšanu tiesībaizsardzības un tiesu iestādēs un partnerattiecību veidošanu ar nozares uzņēmumiem, lai atbalstītu pilsoņus un uzņēmumus. Atzinīgi vērtējama ir arī *ENISA* kā daudzu šim mērķim paredzētu darbību koordinatora darbība.

([20]) Skatīt jo īpaši EDAU atzinumu par Komisijas paziņojumu "Pārskats par informācijas pārvaldību brīvības, drošības un tiesiskuma jomā", kas minēts 8. zemsvītras piezīmē.

([21]) EDAU 2010. gada 22. jūnija atzinums par Priekšlikumu Padomes lēmumam par nolīguma noslēgšanu starp Eiropas Savienību un Amerikas Savienotajām Valstīm par tādu finanšu ziņojumapmaiņas datu apstrādi un nodošanu, kurus Eiropas Savienība dara pieejamus Amerikas Savienotajām Valstīm, lai īstenotu Teroristu finansēšanas izsekošanas programmu *(TFTP II)*.

58. Tomēr *IDS darbībā* sīkāk neizskaidro tiesībaizsardzības pasākumus, kas paredzēti kibertelpā, un to, kā šie pasākumi varētu apdraudēt fizisko personu tiesības un kādi aizsargpasākumi būtu nepieciešami. EDAU aicina izlēmīgāk sniegt atbilstīgas garantijas; šāda pieeja ir atbalstāma, lai aizsargātu visu fizisko personu pamattiesības, tostarp attiecībā uz tiem, kurus varētu ietekmēt pasākumi, kas paredzēti jebkādu iespējamu kriminālu darbību apkarošanai šajā jomā.

V. **SECINĀJUMI UN IETEIKUMI**

59. EDAU aicina IDS īstenošanas procesa gaitā sasaistīt dažādas ES stratēģijas un paziņojumus. Šāda pieeja būtu jāpapildina ar konkrētu rīcības plānu, ko atvieglotu reālistisks vajadzību novērtējums, un tā rezultātā ir jāizstrādā visaptveroša, integrēta un pareizi strukturēta ES politika IDS jautājumos.

60. EDAU arī izmanto iespēju uzsvērt, cik svarīga ir tiesību aktu prasība par visu to esošo instrumentu reālistisku novērtēšanu, kuri tiks izmantoti saistībā ar IDS, un informācijas apmaiņa, pirms tiek piedāvāti jauni instrumenti. Saistībā ar to īpaši ieteicama ir tādu noteikumu iekļaušana, kas paredz attiecīgo instrumentu efektivitātes regulāru novērtēšanu.

61. EDAU ierosina, lai, gatavojot daudzgadu stratēģisko plānu, ko paredz Padomes 2010. gada novembra secinājumi, tiktu ņemts vērā iesāktais darbs pie visaptveroša datu aizsardzības regulējuma, pamatojoties uz Līguma par Eiropas Savienības darbību 16. pantu un jo īpaši uz paziņojumu COM(2009)609.

62. EDAU sniedz daudzus ierosinājumus attiecībā uz priekšstatiem un jēdzieniem, kas ir atbilstīgi no datu aizsardzības viedokļa un ir jāņem vērā IDS jomā, piemēram, attiecībā uz modelēto privātumu, privātuma un datu aizsardzības ietekmes novērtējumu un labākajām pieejamām metodēm.

63. EDAU iesaka, īstenojot turpmākos instrumentus, veikt ietekmes novērtējumu attiecībā uz privātumu un datu aizsardzību – kā atsevišķu novērtējumu vai kā Komisijas veiktā vispārīgā pamattiesību ietekmes novērtējuma daļu.

64. Tas arī aicina Komisiju izstrādāt saskanīgāku un konsekventāku politiku attiecībā uz biometrisko datu izmantošanas priekšnosacījumiem IDS jomā, kā arī vairāk saskaņot ES līmenī datu subjektu tiesības.

65. Visbeidzot, EDAU iesniedz daudzas piezīmes par personas datu apstrādi saistībā ar robežu pārvaldību un jo īpaši *FRONTEX*, kā arī – iespējams – saistībā ar *EUROSUR*.

Briselē, 2010. gada 17. decembrī

Eiropas datu aizsardzības uzraudzītājs

Peter HUSTINX