I

(Rezoliucijos, rekomendacijos ir nuomonės)

NUOMONĖS

EUROPOS DUOMENŲ APSAUGOS PRIEŽIŪROS PAREIGŪNAS

Europos duomenų apsaugos priežiūros pareigūno nuomonė dėl ES ir JAV aukšto lygio ryšių palaikymo grupės dėl keitimosi informacija, privatumo ir asmens duomenų apsaugos galutinės ataskaitos

(2009/C 128/01)

EUROPOS DUOMENŲ APSAUGOS PRIEŽIŪROS PAREIGŪNAS,

atsižvelgdamas į Europos bendrijos steigimo sutartį, ypač į jos 286 straipsnį,

atsižvelgdamas į Europos Sąjungos pagrindinių teisių chartiją, ypač į jos 8 straipsnį,

atsižvelgdamas į 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvą 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo,

atsižvelgdamas 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentą (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo, ypač į jo 41 straipsnį,

PRIĖMĖ ŠIĄ NUOMONĘ:

I. ĮVADAS – SU NUOMONE SUSIJUSI BENDRA INFORMACIJA

1. 2008 m. gegužės 28 d. Europos Sąjungos Tarybai pirmininkaujanti valstybė narė, atsižvelgdama į 2008 m. birželio 12 d. ES aukščiausiojo lygio susitikimą, pranešė Nuolatinių atstovų komitetui, kad ES ir JAV aukšto lygio ryšių palaikymo grupė (toliau – HLCG) dėl keitimosi informacija, privatumo ir asmens duomenų apsaugos parengė galutinę ataskaitą. Ši ataskaita paskelbta 2008 m. birželio 26 d. ([1]).

2. Ataskaita siekiama apibrėžti bendrus privatumo ir duomenų apsaugos principus, kurie yra pirmas žingsnis siekiant keistis informacija su Jungtinėmis Amerikos Valstijomis kovai su terorizmu ir sunkiais tarptautiniais nusikaltimais.

3. Pranešime Tarybai pirmininkaujanti valstybė narė nurodo, kad ji pageidautų sužinoti nuomonių dėl tolesnių veiksmų, susijusių su šia ataskaita, visų pirma gauti pastabų dėl rekomendacijų dėl ataskaitoje nurodytų tolesnių veiksmų. Europos duomenų apsaugos priežiūros pareigūnas (EDAPP) reaguodamas į šį kvietimą pateikia toliau išdėstytą nuomonę, parengtą remiantis dabartine padėtimi ir neturinčią įtakos jokiai kitai pozicijai, kurią jis galėtų pareikšti atsižvelgdamas į su šiuo klausimu susijusius pokyčius.

4. EDAPP pažymi, kad HLCG darbas buvo atliekamas tokiu metu, kai JAV ir ES pradėjo intensyviau keistis duomenims remdamosi tarptautiniais ar kitokiais susitarimais, ypač nuo 2001 m. rugsėjo 11 d. Tarp jų yra Europolo ir Eurojusto susitarimai su Jungtinėmis Amerikos Valstijomis, taip pat susitarimai dėl keleivio duomenų įrašo (PNR) bei SWIFT atvejis, dėl kurio ES ir JAV pareigūnai pasikeitė laiškais siekdamos nustatyti būtiniausias duomenų apsaugos garantijas ([2]).

([1]) Tarybos dokumentas Nr. 9831/08 pateiktas šioje tinklavietėje adresu http://ec.europa.eu/justice_home/fsj/privacy/news/index_en.htm

([2]) — 2001 m. gruodžio 6 d. Jungtinių Amerikos Valstijų ir Europos policijos biuro susitarimas bei Papildomas Europolo ir JAV susitarimas dėl keitimosi asmens duomenimis ir susijusia informacija, paskelbti Europolo tinklavietėje;
— 2006 m. lapkričio 6 d. Jungtinių Amerikos Valstijų ir Eurojusto susitarimas dėl teisminio bendradarbiavimo, paskelbtas Eurojusto tinklavietėje;
— Europos Sąjungos ir Jungtinių Amerikos Valstijų susitarimas dėl oro vežėjų atliekamo keleivio duomenų įrašo (PNR) duomenų tvarkymo ir perdavimo Jungtinių Valstijų Vidaus saugumo departamentui (DHS) (2007 PNR susitarimas), pasirašytas 2007 m. liepos 23 d. Briuselyje ir 2007 m. liepos 26 d. Vašingtone (OL L 204, 2007 8 4, p. 18);
— JAV ir ES valdžios institucijų pasikeitimas laiškais dėl Terorizmo finansavimo sekimo programos, 2007 m. birželio 28 d.

5. Be to, ES veda derybas ir pritaria panašiems susitarimams, kuriuose numatytas keitimasis asmens duomenimis su kitomis trečiosiomis šalimis. Europos Sąjungos ir Australijos susitarimas dėl oro vežėjų atliekamo Europos Sąjungos pateiktų keleivio duomenų įrašo (PNR) duomenų tvarkymo ir perdavimo Australijos muitinės tarnybai ([3]) yra naujausias tokių susitarimų pavyzdys.

6. Todėl akivaizdu, kad trečiųjų šalių teisėsaugos institucijos prašo vis didesnės apimties asmens duomenų, prašydamos ne tik duomenų iš įprastų valstybės duomenų bazių, bet ir iš kitų bylų, visų pirma privačiojo sektoriaus surinktų duomenų.

7. EDAPP taip pat primena svarbų susijusį aspektą – asmens duomenų perdavimo trečiosioms šalims vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose klausimas yra aptartas Tarybos pamatiniame sprendime dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos ([4]), kuris turėtų būti priimtas iki 2008 m. pabaigos.

8. Šis transatlantinis keitimasis informacija galėtų tik suintensyvėti ir apimti papildomus sektorius, kurie susiję su asmens duomenų tvarkymu. Todėl dialogas „transatlantinės teisėsaugos klausimais“ taip pat yra pageidautinas ir labai svarbus. Jis pageidautinas ta prasme, kad jis galėtų suteikti aiškesnį pagrindą duomenų keitimuisi, kuris šiuo metu vyksta ar vyks. Jis taip pat labai svarbus, nes toks pagrindas įteisintų didelės apimties duomenų perdavimą srityje (teisėsauga), kurioje jis daro ypač didelį poveikį asmenims ir kurioje patikimos apsaugos priemonės ir garantijos yra dar labiau reikalingos ([5]).

9. Kitame šios nuomonės skyriuje bus aptarta dabartinė padėtis ir galimi tolesni veiksmai. III skyriuje bus aptarta susitarimo, kuris suteiktų galimybę keistis informacija, taikymo sritis ir pobūdis. Nuomonės IV skyriuje bus nagrinėjami su galimo susitarimo turiniu susiję teisiniai klausimai atsižvelgiant į bendrą perspektyvą. Jame bus aptarti klausimai, pavyzdžiui, Jungtinėse Amerikos Valstijose užtikrinamo apsaugos lygio vertinimo sąlygos, ir aptartas ES reglamentavimo sistemos taikymas kaip kriterijus vertinant tokios apsaugos lygį. Šiame skyriuje taip pat bus išdėstyti pagrindiniai reikalavimai, kurie turi būti įtraukti į tokį susitarimą. Galiausiai, nuomonės V skyriuje bus pateikta prie ataskaitos pridedamų privatumo principų analizė.

([3]) OL L 213, 2008 8 8, p. 49.

([4]) Tarybos pamatinis sprendimas dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos, 2008 m. birželio 24 d. redakcija; jis pateiktas tinklavietėje adresu http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=193371.

([5]) Dėl aiškaus teisinio pagrindo būtinybės žr. šios nuomonės III ir IV skyrius.

II. DABARTINĖ PADĖTIS IR GALIMI TOLESNI VEIKSMAI

10. EDAPP dabartinę padėtį vertina taip: buvo padaryta tam tikra pažanga siekiant apibrėžti bendrus keitimosi informacija, privatumo ir asmens duomenų apsaugos standartus.

11. Tačiau parengiamasis darbas, susijęs su bet kokio pobūdžio ES ir JAV susitarimu, dar nebaigtas. Reikia atlikti papildomą darbą. Pačioje HLCG ataskaitoje paminėta daug neišspręstų klausimų, iš kurių žalos atlyginimo klausimas yra pats aktualiausias. Vis dar nesutariama dėl žalos atlyginimo teismo tvarka taikymo srities ([6]). Penki kiti neišspręsti klausimai nurodyti ataskaitos 3 skyriuje. Be to, šioje nuomonėje pažymima, kad yra dar daugelis kitų neišspręstų klausimų, pavyzdžiui, dėl keitimosi informacija susitarimo taikymo srities ir pobūdžio.

12. Kadangi ataskaitoje nurodyta, kad pageidautina galimybė yra privalomas susitarimas, ir EDAPP pritaria tokiai nuomonei, atsargumas yra dar reikalingesnis. Reikia tęsti nuodugnų ir išsamų pasirengimą, kad būtų galima pasiekti susitarimą.

13. Galiausiai, pasak EDAPP, būtų geriausia, jei susitarimas būtų sudarytas pagal Lisabonos sutartį, žinoma, jei ji įsigalios. Iš tiesų pagal Lisabonos sutartį nebūtų teisinio netikrumo dėl ES ramsčių skiriamosios ribos. Be to, būtų užtikrintas visiškas Europos Parlamento dalyvavimas bei teisminė kontrolė, kurią vykdytų Teisingumo Teismas.

14. Tokiomis aplinkybėmis geriausias būdas būtų parengti veiksmų planą galimam susitarimui pasiekti vėlesniame etape. Tokiame veiksmų plane būtų pateikti šie elementai:

— HLCG (ar kurios nors kitos grupės) tolesnio darbo gairės bei tvarkaraštis;

— pradiniame etape – esminių klausimų, pavyzdžiui, dėl susitarimo taikymo srities ir pobūdžio, aptarimas ir galimas susitarimas dėl jų;

— remiantis bendru šių esminių klausimų supratimu, tolesnis duomenų apsaugos principų rengimas;

— suinteresuotųjų subjektų dalyvavimas įvairiuose procedūros etapuose;

— Europos atveju – su instituciniais apribojimais susijusių klausimų sprendimas.

([6]) Ataskaitos 5 puslapis, C dalis.

III. **SUSITARIMO DĖL KEITIMOSI INFORMACIJA TAIKYMO SRITIS IR POBŪDIS**

15. EDAPP nuomone, itin svarbu, kad galimo susitarimo, kuriame būtų numatyti duomenų apsaugos principai, taikymo sritis ir pobūdis būtų aiškiai apibrėžti, ir tai būtų pirmas žingsnis toliau rengiant tokį susitarimą.

16. Taikymo srities klausimu reikia atsakyti į šiuos svarbius klausimus:

— kas yra susiję subjektai teisėsaugos ir kitos srityse;

— ką reiškia „teisėsaugos tikslas“ ir kokia jo sąsaja su kitais tikslais, pavyzdžiui, nacionaliniu saugumu, o konkrečiau su sienų kontrole bei visuomenės sveikata;

— kaip susitarimas būtų suderinamas su visuotinės transatlantinės saugumo erdvės perspektyva.

17. Pobūdžio sąvokos apibrėžtis padėtų paaiškinti šiuos klausimus:

— jei būtina, pagal kurį ramstį bus vedamos derybos dėl susitarimo;

— ar susitarimas bus privalomas ES ir JAV;

— ar jis turės tiesioginį poveikį ta prasme, kad jame bus apibrėžtos asmenų teisės ir pareigos, kurios gali būti vykdomos teisminėje institucijoje;

— ar pats susitarimas numatys galimybę keistis informacija ar nustatys būtiniausią keitimosi informacija standartą, kurį papildytų konkretūs susitarimai;

— kaip susitarimas bus siejamas su galiojančiais susitarimais: ar jis atitiks, pakeis ar papildys juos?

III.1. **Susitarimo taikymo sritis**

Susiję subjektai

18. Nors HLCG ataskaitoje nėra aiškiai nurodyta, kokia turėtų būti tiksli būsimo susitarimo taikymo sritis, remiantis joje paminėtais principais galima daryti išvadą, kad susitarimas turėtų būti taikomas duomenų perdavimui tiek tarp privačiojo ir valstybės sektorių subjektų ([7]), tiek tarp valstybės institucijų.

— Privačiojo ir valstybės sektorių subjektų atveju:

19. EDAPP supranta, kodėl pagal kokį principą būsimas susitarimas turėtų būti taikomas duomenų perdavimui tarp privačiojo ir valstybės sektorių subjektų. Toks susitarimas rengiamas atsižvelgiant į pastaraisiais metais JAV teikiamus prašymus privačiojo sektoriaus subjektams teikti informaciją. EDAPP iš tiesų pažymi, kad privačiojo sektoriaus subjektai tampa sistemingu informacijos šaltiniu teisėsaugos srityje tiek ES, tiek tarptautiniu lygiu ([8]). SWIFT atvejis buvo svarbus precedentas, kai privačios bendrovės buvo prašoma sistemingai perduoti didelės apimties duomenis trečiosios valstybės teisėsaugos institucijoms ([9]). PNR duomenys iš aviakompanijų renkami pagal tokį pat principą. EADDP nuomonėje dėl pamatinio sprendimo projekto dėl europinės PNR sistemos jau pareiškė abejonę dėl tokios tendencijos teisėtumo ([10]).

20. Yra dar dvi priežastys, dėl kurių duomenų perdavimo tarp privačiojo ir valstybės sektorių subjektų nereikėtų įtraukti į būsimo susitarimo taikymo sritį.

21. Pirma, tokių subjektų įtraukimas galėtų padaryti nepageidaujamą poveikį pačios ES teritorijoje. EADDP yra labai susirūpinęs dėl to, kad tuo atveju, jeigu privačių bendrovių (pvz., finansų įstaigų) duomenys iš esmės būtų perduodami trečiosioms šalims, atsirastų didelis spaudimas tokius ES turimus duomenis taip pat teikti teisėsaugos institucijoms. PNR sistema – tokios nepageidautinos tendencijos, kuri atsirado JAV pradėjus dideliais kiekiais rinkti keleivių duomenis ir kuri tokiu būdu atsirastų ir Europoje ([11]), pavyzdys, nors sistemos būtinumas ir proporcingumas nėra aiškiai pagrįsti.

22. Antra, savo nuomonėje dėl Komisijos pasiūlymo dėl ES PNR EADDP taip pat iškėlė duomenų apsaugos sistemos (pirmojo ar antrojo ramsčio), taikytinos valstybės ir privačiojo sektorių subjektų bendradarbiavimo sąlygoms, klausimą: ar taisyklės turėtų būti grindžiamos duomenų valdytojo (privačiojo sektoriaus) kokybe ar siektinu tikslu (teisėsauga)? Pirmojo ir trečiojo ramsčių skiriamoji linija yra labai neaiški tais atvejais, kai įpareigojimai tvarkyti asmens duomenis teisėsaugos tikslais nustatomi privačiojo sektoriaus subjektams. Todėl šiuo atžvilgiu palankiai vertinama tai, kad Generalinis advokatas Bot neseniai pateiktoje

([7]) Visų pirma žr. ataskaitos 3 skyriaus „Su transatlantiniais santykiais susiję neišspręsti klausimai“ 1 punktą: „Privačiojo sektoriaus subjektų įpareigojimų suderinamumas vykdant duomenų perdavimą“.

([8]) Šiuo klausimu žr. 2007 m. gruodžio 20 d. EADDP nuomonę dėl pasiūlymo dėl Tarybos pamatinio sprendimo dėl keleivio duomenų įrašo (PNR) duomenų naudojimo teisėsaugoje, OL C 110, 2008 5 1, p. 1. „Tradiciškai teisėsaugos ir privačiojo sektoriaus veikla yra aiškiai atskirta: su teisėsauga susijusį darbą atlieka specialiai tam paskirtos institucijos, būtent policijos pajėgos, o privačių subjektų kiekvienu konkrečiu atveju prašoma perduoti asmens duomenis šioms teisėsaugos institucijoms. Šiuo metu esama tendencijos privatiems subjektams primesti sistemingą bendradarbiavimą teisėsaugos tikslais“.

([9]) Žr. pagal 29 straipsnio darbo grupės 2006 m. lapkričio 22 d. Nuomonę 10/2006 dėl Pasaulinės tarpbankinių finansinių telekomunikacijų organizacijos (SWIFT) atliekamo asmens duomenų tvarkymo, DG 128.

([10]) 2007 m. gruodžio 20 d. nuomonė, op. cit.

([11]) Žr. 8 išnašoje paminėtą pasiūlymą dėl Tarybos pamatinio sprendimo dėl keleivio duomenų įrašo (PNR) duomenų naudojimo teisėsaugoje, kuris šiuo metu svarstomas Taryboje.

nuomonėje byloje dėl duomenų saugojimo ([12]) pasiūlė tokiems atvejams skiriamosios linijos apibrėžimą, tačiau EDAPP taip pat teigia, kad: „šią skiriamąją liniją tikrai galima įvertinti kritiškai ir kai kuriais aspektais ji gali atrodyti dirbtinai apibrėžta“. EDAPP taip pat pažymi, kad Teismo sprendime dėl PNR ([13]) nėra visiškai atsakyta į klausimą dėl taikytino teisinio pagrindo. Pavyzdžiui, tai, kad Direktyva 95/46/EB netaikoma tam tikroms veiklos rūšims automatiškai nereiškia, kad šios veiklos rūšys gali būti reglamentuojamos pagal trečiąjį ramstį. Todėl taikytinos teisės požiūriu gali būti palikta spraga ir kiekvienu atveju atsiranda teisinis netikrumas dėl duomenų subjektams užtikrinamų teisinių garantijų.

23. Atsižvelgdamas į tai, EDAPP pabrėžia, kad būtina užtikrinti, jog galimas būsimas susitarimas, kuriame būtų išdėstyti bendri duomenų apsaugos principai, negali automatiškai įteisinti transatlantinio asmens duomenų perdavimo tarp privačiojo ir valstybės sektorių subjektų. Toks perdavimas būsimame susitarime gali būti numatytas tik tuo atveju, jeigu:

— būsimame susitarime būtų numatyta, kad perduoti duomenis leidžiama tik tuo atveju, jeigu įrodyta, kad tai visiškai būtina konkrečiam tikslui, o sprendžiama kiekvienu konkrečiu atveju;

— pats perdavimas atliekamas taikant aukšto lygio duomenų apsaugos priemones (kaip nurodyta šioje nuomonėje).

Be to, EDAPP pažymi, kad yra netikrumas dėl taikytino teisinio duomenų apsaugos pagrindo, ir todėl prašo bet kokiu atveju nenumatyti asmens duomenų perdavimo tarp privačiojo ir valstybės sektorių subjektų pagal galiojančią ES teisę.

— Valstybės institucijų atveju:

24. Tiksli keitimosi informacijos taikymo sritis nėra aiški. Tolesniame darbe rengiant bendrą susitarimą pirmiausia reikėtų tiksliai apibrėžti numatomą tokio susitarimo taikymo sritį. Visų pirma reikia išspręsti šiuos klausimus:

— ar dėl ES veikiančių duomenų bazių – susitarimas apimtų centralizuotas duomenų bazes, kurias (iš dalies) tvarko ES, pavyzdžiui, Europolo ir Eurojusto duomenų bazes arba valstybių narių tvarkomas decentralizuotas duomenų bazes, arba abiejų rūšių duomenų bazes;

— ar susitarimo taikymo sritis apimtų tarpusavyje sujungtus tinklus, t. y. ar numatytos garantijos būtų taikomos duomenims, kuriais keičiasi valstybės narės ar agentūros ES bei JAV;

— ar susitarimas būtų taikomas keičiantis tik duomenų bazių duomenimis teisėsaugos (policijos, teisingumo, galbūt muitinės) srityse ir kitų duomenų bazių, pavyzdžiui, mokesčių, duomenimis;

— ar susitarimas taip pat apimtų nacionalinių saugumo agentūrų duomenų bazes ar sudarytų galimybę toms agentūroms turėti prieigą prie teisėsaugos duomenų bazių kitos susitariančiosios šalies teritorijoje (Europos Sąjungai – Jungtinėse Amerikos Valstijose ir atvirkščiai);

— ar susitarimas kiekvienu konkrečiu atveju apimtų informacijos perdavimą ar nuolatinę prieigą prie veikiančių duomenų bazių. Dėl pastarosios prielaidos tikrai kils su proporcingumu susijusių klausimų, kaip toliau aptariama V skyriaus 3 punkte.

Teisėsaugos tikslas

25. Dėl galimo susitarimo tikslo apibrėžimo taip pat yra netikrumo. Teisėsaugos tikslai yra aiškiai nurodyti įvade bei ataskaitos dalyje, kur išdėstytas pridedamas pirmasis principas, ir bus toliau nagrinėjami šios nuomonės IV skyriuje. EDAPP pažymi, kad remiantis šia informacija galima manyti, jog keitimasis duomenimis daugiausia būtų vykdomas trečiojo ramsčio klausimais, tačiau gali kilti klausimas, ar tai yra tik pirmas žingsnis siekiant suintensyvinti keitimąsi duomenimis. Atrodo aišku, kad ataskaitoje nurodyti „visuomenės saugumo“ tikslai apima kovą su terorizmu, organizuotu nusikalstamumu ir kitais nusikaltimais. Tačiau ar tai irgi reiškia, kad gali būti leidžiama keistis duomenimis kitų viešų interesų labui, pavyzdžiui, galbūt siekiant išvengti rizikos visuomenės sveikatai?

26. EDAPP rekomenduoja numatyti, kad tikslas – tai tiksliai nustatytas duomenų tvarkymas, ir pagrįsti pasirinktus politinius sprendimus, kuriais remiantis taip apibrėžtas tikslas.

([12]) Generalinio advokato Bot 2008 m. spalio 14 d. nuomonė *Airija prieš Europos Parlamentą ir Tarybą* (Byla C- 301/06), 108 punktas.

([13]) 2006 m. gegužės 30 d. Teismo sprendimas *Europos Parlamentas prieš Europos Sąjungos Tarybą* (C-317/04) ir *Europos Bendrijų Komisiją* (C-318/04), Sujungtos bylos C-317/07 ir C-318/04, Rink. [2006], p. I-4721.

Visuotinė transatlantinė saugumo erdvė

27. Plati šios ataskaitos taikymo sritis turėtų būti vertinama atsižvelgiant į visuotinę transatlantinės saugumo erdvės perspektyvą, kurią aptarė „Ateities grupė“ ([14]). 2008 m. birželio mėn. paskelbtoje šios grupės ataskaitoje šiek tiek dėmesio skirta vidaus reikalų politikos išorės aspektui. Joje nurodoma, kad *„iki 2014 m. Europos Sąjunga turėtų apsispręsti dėl politinio tikslo – sukurti euroatlantinę bendradarbiavimo su Jungtinėmis Valstijomis laisvės, saugumo ir teisingumo srityse erdvę“*. Bendradarbiaujama būtų ne tik saugumo klausimais siaurąja prasme, bet bent jau tose srityse tokiais klausimais, kurie numatyti dabartinėje EB sutarties IV antraštinėje dalyje, t. y. imigracijos, vizų, prieglobsčio ir bendradarbiavimo civilinės teisės srityse, klausimais. Būtina kelti klausimą, kaip susitarimas dėl pagrindinių duomenų apsaugos principų, pavyzdžiui, paminėtų HLCG ataskaitoje, galėtų ir turėtų būti keitimosi informacija tokioje plačioje srityje pagrindas.

28. Iš esmės iki 2014 m. ramsčių struktūros nebeliks, o bus vienas teisinis duomenų apsaugos pagrindas pačios ES viduje (pagal Lisabonos sutartį, Sutarties 16 straipsnis dėl Europos Sąjungos veikimo). Tačiau iš tiesų tai, kad duomenų apsaugos *reglamentavimas* yra suderintas ES lygiu, nereiškia, kad bet kokiame susitarime su trečiąja šalimi būtų numatyta galimybė *perduoti* asmens duomenis bet kokiu tikslu. Atsižvelgiant į duomenų tvarkymo aplinkybes ir sąlygas, tam tikrose srityse, pavyzdžiui, teisėsaugos, gali reikėti keisti duomenų apsaugos garantijas. EDAPP rekomenduoja rengiant būsimą susitarimą atsižvelgti į tokių skirtingų aspektų padarinius.

III.2. **Susitarimo pobūdis**

Europos institucinė struktūra

29. Bet kokiu atveju trumpalaikiu laikotarpiu itin svarbu nustatyti, pagal kurį ramstį bus vedamos derybos dėl susitarimo. To ypač reikia asmens duomenų apsaugos vidaus reglamentavimo sistemos, kuriai toks susitarimas turės įtakos, atžvilgiu. Ar tai bus pirmasis ramstis-pagrindas – iš esmės Direktyva 95/46/EB, kurioje numatyta speciali duomenų perdavimo trečiosioms šalims tvarka, – ar tai bus trečiasis ramstis-pagrindas, kuriame būtų numatyta ne tokia griežta duomenų perdavimo trečiosioms šalims tvarka? ([15])

30. Nors, kaip jau minėta, teisėsaugos tikslai yra pagrindiniai, HLCG ataskaitoje taip pat nurodytas duomenų rinkimas iš privačiojo sektoriaus subjektų, o tikslai taip pat gali būti aiškinami plačiąja prasme, įtraukiant ne tik saugumo, bet ir imigracijos ir sienų kontrolės klausimus, o galbūt ir visuomenės sveikatos klausimus. Atsižvelgiant į tokį netikrumą, būtų labai pageidautina palaukti ramsčių suderinimo pagal ES teisę, kaip numatyta Lisabonos sutartyje, kad būtų aiškiai nustatytas teisinis derybų pagrindas ir tiksliai apibrėžtas Europos institucijų, ypač Europos Parlamento ir Komisijos, vaidmuo.

Privalomas susitarimo pobūdis

31. Reikėtų aiškiai nustatyti, ar remiantis diskusijų išvadomis bus sudarytas susitarimo memorandumas arba kitoks neprivalomas susitarimas, ar tai bus privalomas tarptautinis susitarimas.

32. EDAPP pritaria ataskaitoje pateiktai nuomonei, kad reikalingas privalomas susitarimas. EDAPP nuomone, oficialus privalomas susitarimas būtinas tam, kad būtų vykdomas duomenų perdavimas už ES ribų, nesvarbu, kokiu tikslu duomenys perduodami. Duomenys trečiajai šaliai negali būti perduodami, jei nesilaikoma atitinkamų sąlygų ir apsaugos priemonių, numatytų konkrečiame (ir privalomame) teisiniame pagrinde. Kitaip tariant, susitarimo memorandumas ar kitoks neprivalomas susitarimas gali būti naudingas derybų dėl kitų privalomų susitarimų gairėms nustatyti, tačiau jokiu būdu negali pakeisti būtino privalomo susitarimo.

Tiesioginis poveikis

33. Susitarimo nuostatos turėtų būti privalomos tiek JAV, tiek ES bei jos valstybėms narėms.

34. Be to, reikėtų užtikrinti, kad asmenys turėtų teisę naudotis savo teisėmis ir ypač gauti žalos atlyginimą pagal susitartus principus. EDAPP nuomone, šį rezultatą galima geriausiai pasiekti, jei esminės susitarimo nuostatos yra taip suformuluotos, kad jos turi tiesioginį poveikį Europos Sąjungos gyventojams ir gali būti taikomos teisme. Todėl susitarime turi būti aiškiai nurodytas tiesioginis tarptautinio susitarimo nuostatų poveikis bei jų perkėlimo į Europos ir nacionalinę teisę siekiant užtikrinti priemonių veiksmingumą sąlygos.

Sąsaja su kitais dokumentais

35. Kitas esminis klausimas – kiek susitarimas gali būti taikomas atskirai arba kiekvienu konkrečiu atveju papildytas kitais susitarimais dėl konkretaus keitimosi duomenimis. Iš tiesų kyla klausimas, ar atskiras susitarimas, kuriame nustatyti bendri standartai, galėtų tinkamai aprėpti daugybę duomenų tvarkymo trečiojo ramsčio klausimais ypatumų. Dar daugiau abejonių kyla dėl to, ar be papildomų diskusijų ir nenumačius apsaugos priemonių būtų galima taip paprastai patvirtinti asmens duomenų perdavimą, neatsižvelgiant į atitinkamų asmenų tikslą ir pobūdį. Be to, susitarimai su trečiosiomis šalimis nebūtinai yra

([14]) Europos vidaus reikalų politikos ateities neoficialios aukšto lygio patariamosios grupės ataskaita „Laisvė, saugumas, privatumas – Europos vidaus reikalai atvirame pasaulyje“, 2008 m. birželio mėn., pateikta tinklavietėje adresu register.consilium.europa.eu

([15]) Žr. šios nuomonės 7 punkte paminėto sprendimo (DAPS) 11 ir 13 straipsnius.

nuolatiniai, nes jie gali būti susiję su tam tikromis grėsmėmis, peržiūrimi arba jiems taikomos nuostatos dėl laikino galiojimo. Kita vertus, privalomame susitarime pripažinti bendri būtiniausi standartai galėtų sudaryti palankesnes sąlygas toliau diskutuoti dėl asmens duomenų perdavimo, susijusio su konkrečia duomenų baze ar duomenų tvarkymo veiksmais.

36. Todėl EDAPP pritartų tam, kad būtų parengti būtiniausi duomenų apsaugos kriterijai, kuriuos kiekvienu konkrečiu atveju papildytų papildomos konkrečios nuostatos, kaip paminėta HLCG ataskaitoje, o nebūtų vadovaujamasi vienu atskiru susitarimu. Šios papildomos konkrečios nuostatos yra būtinos tam, kad būtų numatyta galimybė perduoti duomenis konkrečiu atveju. Tai paskatintų taikyti suderintą duomenų apsaugos metodą.

Galiojančių susitarimų taikymas

37. Reikėtų taip pat nagrinėti, kaip galimas bendras susitarimas būtų suderintas su jau galiojančiais ES ir JAV sudarytais susitarimais. Reikėtų pažymėti, kad šie galiojantys susitarimai neturi tokio pat privalomo pobūdžio: visų pirma, pažymėtinas PNR susitarimas (suteikiantis daugiau teisinio tikrumo), Europolo ir Eurojusto susitarimai arba SWIFT pasikeitimas laiškais ([16]). Ar šie nauji bendri teisės aktai papildytų šiuos galiojančius susitarimus, ar jie liktų nepakitę, ir nauji teisės aktai būtų taikomi tik keitimuisi asmens duomenimis ateityje? EDAPP nuomone, siekiant teisinio suderinamumo reikėtų parengti suderintas taisykles, taikomas tiek galiojantiems, tiek būsimiems privalomiems susitarimams dėl duomenų perdavimo ir juos papildantiems.

38. Bendro susitarimo taikymas galiojantiems susitarimams turėtų privalumą – sustiprintų jų privalomą pobūdį. Visų pirma tai būtų pageidautina teisiškai neprivalomų susitarimų, pavyzdžiui, SWIFT pasikeitimo laiškais, atžvilgiu, nes taip būtų nustatytas reikalavimas laikytis bendrų privatumo principų.

IV. **BENDRO POBŪDŽIO TEISINIS ĮVERTINIMAS**

39. Šiame skyriuje bus nagrinėjama, kokiu būdu turi būti įvertintas konkrečia sistema ar dokumentu užtikrinamos apsaugos lygis, įskaitant taikytinus kriterijus ir būtinus pagrindinius reikalavimus.

([16]) Žr. 2 išnašą.

Tinkamas apsaugos lygis

40. Anot EDAPP, turėtų būti akivaizdu, jog vienas iš būsimų susitarimo pagrindinių pasiekimų – užtikrinimas, kad asmens duomenys Jungtinėms Valstijoms būtų perduodami tik tuo atveju, jei Jungtinių Amerikos Valstijų institucijos garantuoja tinkamą apsaugos lygį (ir atvirkščiai).

41. EDAPP nuomone, asmens duomenų apsaugos lygį tinkamai garantuotų tik realus tinkamumo testas. Jis teigia, kad bendrasis susitarimas, kurio taikymo sritis būtų tokia pat plati, kaip HLCG parengtos ataskaitos, pats savaime vargu ar išlaikytų realų tinkamumo testą. Bendrasis susitarimas galėtų būti pripažintas tinkamu tik tuo atveju, jei jis būtų susietas su kiekvienu konkrečiu atveju sudarytais tinkamais specialiais susitarimais.

42. Trečiųjų šalių užtikrinamos apsaugos lygio įvertinimas nėra neįprasta užduotis, visų pirma Europos Komisijai: pagal pirmąjį ramstį tinkamumas yra vienas iš perdavimui taikytinų reikalavimų. Remiantis konkrečiais kriterijais tinkamumas buvo keletą kartų įvertintas pagal Direktyvos 95/46/EB 25 straipsnį – tai patvirtinta Europos Komisijos sprendimais ([17]). Pagal trečiąjį ramstį tokia sistema nėra aiškiai numatyta: vertinti apsaugos tinkamumą įpareigojama tik pamatinio sprendimo dėl duomenų apsaugos (dar nepriimtas) 11 ir 13 straipsniuose apibrėžtais konkrečiais atvejais ([18]) ir ši pareiga yra skirta valstybėms narėms.

43. Šiuo atveju užduotis susijusi su teisėsaugos tikslais, o diskusijas rengia Komisija prižiūrint Tarybai. Aplinkybės lyginant su „saugaus uosto“ privatumo principų ar Kanados teisės aktų tinkamumo vertinimu skiriasi ir labiau siejamos su derybomis dėl PNR duomenų tvarkymo, kurios neseniai buvo surengtos su JAV ir Australija pagal trečiajam ramsčiui priskiriamus teisės aktus. Tačiau HLCG principai buvo paminėti ir diskutuojant dėl vizų režimo netaikymo programos, kuri susijusi su sienų apsaugos ir imigracijos klausimais – taigi, pirmojo ramsčio klausimais.

44. EDAPP rekomenduoja visus tinkamumo vertinimus pagal galimą būsimą susitarimą atlikti remiantis patirtimi

([17]) Komisijos sprendimai dėl asmens duomenų apsaugos tinkamumo trečiosiose šalyse, įskaitant Argentiną, Kanadą, Šveicariją, Jungtines Valstijas, Gernsiu, Meno salą ir Džersį (pateikiami tinklavietėje adresu http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm).

([18]) Tik tuo atveju, jei valstybė narė perduoda trečiajai šaliai ar tarptautinei organizacijai kitos valstybės narės kompetentingos institucijos pateiktus duomenis.

minėtose įvairiose srityse. Jis rekomenduoja galimame būsimame susitarime dar labiau išplėsti „tinkamumo“ sąvoką remiantis panašiais kriterijais, kurie buvo taikomi apibrėžiant ankstesnes tinkamumo sąvokas.

Abipusis pripažinimas – abipusiškumas

45. Dar vienas apsaugos lygio aspektas siejamas su abipusiu ES ir JAV sistemų pripažinimu. HLCG ataskaitoje šiuo klausimu nurodyta, kad tikslas – „siekti viena kitos privatumo ir duomenų apsaugos sistemų veiksmingumo pripažinimo srityse, kurioms taikomi minėti principai“ ([19]) ir užtikrinti „lygiavertį ir abipusį privatumo ir asmens duomenų apsaugos teisės aktų taikymą“.

46. EDAPP akivaizdu, kad abipusis pripažinimas (arba abipusiškumas) įmanomas tik tuo atveju, jei yra užtikrintas tinkamas apsaugos lygis. Kitaip tariant, būsimame susitarime turėtų būti suderintos nuostatos dėl būtiniausio apsaugos lygio (atliekant tinkamumo vertinimą, atsižvelgiant į specialių susitarimų poreikį kiekvienu konkrečiu atveju). Abipusis pripažinimas yra įmanomas tik laikantis šios būtinos sąlygos.

47. Pirmasis elementas, į kurį reikia atsižvelgti – esminių nuostatų dėl duomenų apsaugos abipusiškumas. EDAPP nuomone, susitarime esminių nuostatų dėl duomenų apsaugos abipusiškumo sąvoka turėtų būti nagrinėjama taip, jog būtų užtikrinta, kad, viena vertus, tvarkant duomenis ES teritorijoje (ir JAV) būtų visiškai laikomasi vietos teisės aktų dėl duomenų apsaugos ir, kita vertus, kad tvarkant susitarimo taikymo sričiai priklausančius duomenis ne kilmės šalyje būtų laikomasi tame susitarime numatytų duomenų apsaugos principų.

48. Antrasis aspektas – žalos atlyginimo mechanizmų abipusiškumas. Turėtų būti užtikrinta, kad Europos piliečiams būtų garantuojamos tinkamos žalos atlyginimo priemonės, kai su jais susiję duomenys tvarkomi Jungtinėse Valstijoje (neatsižvelgiant į tokiam duomenų tvarkymui taikomą teisės aktą), ir kad lygiai taip pat Europos Sąjunga ir jos valstybės narės suteiktų lygiavertes teises JAV piliečiams.

49. Trečiasis aspektas – abipusis teisėsaugos institucijų teisės susipažinti su asmens duomenimis užtikrinimas. Jei kokiu nors dokumentu Jungtinių Valstijų institucijoms būtų suteikta prieiga prie ES duomenų, abipusiškumas reikštų, kad tokia pati prieiga prie JAV duomenų turėtų būti suteikta ES institucijoms. Abipusiškumas neturi pakenkti duomenų subjekto apsaugos veiksmingumui. Tai viena iš teisėsaugos institucijoms suteikiamos „transatlantinės“ prieigos būtinų sąlygų. Konkrečiai tai reiškia, kad:

— Jungtinių Valstijų institucijoms tiesioginė prieiga prie duomenų ES teritorijoje (ir atvirkščiai) neturėtų būti suteikta. Prieiga turėtų būti suteikta tik netiesiogiai pagal aktyviąją sistema („*push*“ sistema).

— Tokios prieigos sąlygas turėtų kontroliuoti šalies, kurioje tvarkomi duomenys, duomenų apsaugos institucijos ir teisminės institucijos.

— Jungtinių Valstijų institucijų prieigą prie ES turimų duomenų bazių turėtų reglamentuoti esminės nuostatos dėl duomenų apsaugos (žr. aukščiau) ir tokios prieigos atžvilgiu duomenų subjektui turėtų būti užtikrintos visapusiškos žalos atlyginimo priemonės.

Susitarimo tikslumas

50. Labai svarbu tiksliai apibrėžti įvertinimo (tinkamumo, lygiavertiškumo, abipusio pripažinimo) sąlygas, nes tai lemia apsaugos turinį tikslumo, teisinio tikrumo ir veiksmingumo požiūriu. Būsimo dokumento turinys turi būti tikslus ir išsamus.

51. Be to, turėtų būti akivaizdu, kad vėlesniame etape sudarytuose specialiuose susitarimuose taip pat reikės išsamiai ir visapusiškai apibrėžti apsaugos priemones dėl duomenų apsaugos, taikytinas numatomo keitimosi duomenimis objektui. Tik tokie dviejų lygių konkretaus pobūdžio duomenų apsaugos principai užtikrintų būtiną bendrojo susitarimo ir specialių susitarimų „glaudžią sąsają“, kaip jau nurodyta šios nuomonės 35 ir 36 punktuose.

Kitoms trečiosioms šalims skirto modelio nustatymas

52. Ypatingą dėmesį reikėtų skirti tam, kiek susitarimas su JAV gali būti pavyzdžiu kitų trečiųjų šalių atžvilgiu. EDAPP pažymi, kad pirmiau minėtoje Ateities grupės ataskaitoje strateginėmis ES partnerėmis įvardyta net tik JAV, bet ir Rusija. Atsižvelgiant į tai, kad principai yra neutralūs ir atitinka esmines ES apsaugos priemones, jie galėtų sudaryti vertingą precedentą. Tačiau ypatumai, susiję, pavyzdžiui, su duomenis gaunančios šalies teisine sąranga arba duomenų perdavimo tikslu, trukdytų vien tik perkelti susitarimo nuostatas. Vienodai lemiamas veiksnys bus demokratijos padėtis trečiosiose šalyse: reikėtų įsitikinti, kad principai, dėl kurių bus susitarta, bus veiksmingai garantuojami ir įgyvendinami duomenis gaunančioje šalyje.

Kokie kriterijai taikomi siekiant įvertinti apsaugos lygį?

53. Tačiau vertinant numanomą ar aiškų tinkamumą reikėtų laikytis tarptautinių bei europinių teisės aktų ir visų pirma apsaugos priemonių duomenų apsaugos srityje, dėl kurių bendrai susitarta. Jie yra nustatyti Jungtinių Tautų

([19]) A skyrius. Privalomas tarptautinis susitarimas, p. 8.

gairėse, Europos Tarybos konvencijoje Nr. 108 ir jos papildomame protokole, OECD gairėse ir pamatinio sprendimo dėl duomenų apsaugos projekte, o pirmojo ramsčio aspektais – Direktyvoje 95/46/EB ([20]). Visuose šiuose dokumentuose nustatyti panašūs principai, kurie iš esmės pripažinti kaip pagrindiniai duomenų apsaugos principai.

54. Atsižvelgiant į galimo susitarimo, pavyzdžiui, numatytojo HLCG ataskaitoje, poveikį, labai svarbu tinkamai atsižvelgti į pirmiau nurodytus principus. Dokumentas, kuris apimtų visą trečiosios šalies *vykdymo užtikrinimo* sektorių, iš tiesų reikštų precedento neturinčią situaciją. Galiojantys sprendimai dėl tinkamumo pirmojo ramsčio srityje ir su trečiosiomis šalimis sudaryti susitarimai ES trečiojo ramsčio srityje (Europolas, Eurojustas) visuomet buvo susiję su konkrečiu duomenų perdavimu, tačiau atsižvelgiant į visapusišką siektiną tikslą (kova su nusikalstamumu, nacionalinis bei visuomenės saugumas, sienų saugumo užtikrinimas) ir tai, kad nežinomas atitinkamų duomenų bazių skaičius, šiuo metu kalbame apie galimybę perduoti duomenis daug didesniu mastu.

Pagrindiniai reikalavimai

55. Sąlygos, kurių būtina laikytis perduodant asmens duomenis trečiosioms šalims, nustatytos 29 straipsnio darbo grupės darbiniame dokumente ([21]). Visi susitarimai dėl būtiniausių privatumo principų turėtų užtikrinti atitikties testo reikalavimus, užtikrinančius apsaugos priemonių dėl duomenų apsaugos veiksmingumą.

— Dėl esmės: duomenų apsaugos principai turėtų numatyti aukšto lygio apsaugą ir atitikti su ES principais suderintus standartus. HLCG ataskaitoje nustatyti 12 principų bus šiuo atžvilgiu toliau analizuojami šio nuomonės V skyriuje.

— Dėl specifiškumo: atsižvelgiant į susitarimo pobūdį ir visų pirma tuo atveju, jei tai oficialus tarptautinis susitarimas, taisyklės ir procedūros turėtų būti pakankamai išsamios, kad susitarimą būtų galima veiksmingai įgyvendinti.

— Dėl priežiūros: siekiant užtikrinti atitiktį taisyklėms, dėl kurių susitarta, turėtų būti įdiegti konkretūs kontrolės mechanizmai vidaus kontrolės (auditas) ir išorės kontrolės (peržiūros) srityse. Šie mechanizmai turi būti vienodai prieinami abiem susitarimo šalims. Priežiūra apima mechanizmus, kuriais siekiama užtikrinti atitiktį makro lygiu, pavyzdžiui, bendros peržiūros mechanizmai, ir atitiktį mikro lygiu, pavyzdžiui, atskiros žalos atlyginimo priemonės.

56. Be šių trijų pagrindinių reikalavimų ypatingą dėmesį reikėtų skirti specifiškumui, siejamam su asmens duomenų tvarkymu teisėsaugos tikslais. Tai iš tiesų yra sritis, kurioje pagrindinės teisės gali būti šiek tiek apribotos. Todėl kompensuojant asmens teisių apribojimus ir atsižvelgiant į poveikį asmeniui turėtų būti patvirtintos apsaugos priemonės visų pirma toliau nurodytais aspektais:

— Skaidrumas: informacija apie asmens duomenis ir teisė su jais susipažinti gali būti suteikta tik teisėsaugos tikslais, pavyzdžiui, atsižvelgiant į vykdomų slaptų tyrimų poreikius. Nors ES tradiciškai nustatomi papildomi mechanizmai tokiam pagrindinių teisių apribojimui kompensuoti (dažnai pasitelkiant nepriklausomas duomenų apsaugos institucijas), vis dėlto turi būti užtikrinta, kad informaciją perdavus trečiajai šaliai bus galima naudotis panašiais kompensavimo mechanizmais.

— Žalos atlyginimo priemonės: dėl pirmiau nurodytų priežasčių asmenims turėtų būti užtikrintos alternatyvios galimybės apginti savo teises, visų pirma naudojantis nepriklausomos priežiūros institucijos paslaugomis ir teisme.

— Duomenų saugojimas: duomenų saugojimo laikotarpio pagrindimas nebūtinai gali būti skaidrus. Turi būti imtasi priemonių užtikrinti, kad tai duomenų subjektams ar priežiūros institucijoms netrukdytų veiksmingai naudotis teisėmis.

([20]) — 1990 m. gruodžio 14 d. Generalinės Asamblėjos priimtos Jungtinių Tautų gairės dėl kompiuterizuotų asmens duomenų bylų, pateikiamos tinklavietėje adresu www.unhchr.ch/html/menu3/b/71.htm
— 1981 m. sausio 28 d. Europos Tarybos konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu, pateikiama tinklavietėje adresu www.conventions.coe.int/treaty/en/Treaties/html/108.htm
— 1980 m. rugsėjo 23 d. EOCD gairės dėl privatumo apsaugos ir asmens duomenų tarpvalstybinių srautų, pateikiama tinklavietėje adresu www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html
— Tarybos pamatinio sprendimo dėl asmens duomenų, tvarkomų vykdant policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, apsaugos, projektas, pateikiamas tinklavietėje adresu http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=193371
— 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (OL L 281, 1995 11 23, p. 31).

([21]) 1998 m. liepos 24 d. darbinis dokumentas dėl asmens duomenų perdavimų trečiosioms šalims: ES duomenų apsaugos direktyvos 25 ir 26 straipsnių taikymas; DG 12.

— Teisėsaugos institucijų atskaitomybė: tuo atveju, jei skaidrumas nėra veiksmingas, asmenų arba institucinių subjektų taikomi kontrolės mechanizmai negali būti visapusiški. Vis dėlto labai svarbu turėti patikimai veikiančius kontrolės mechanizmus atsižvelgiant į neskelbtiną tokių duomenų pobūdį ir prievartos priemones, kurias galima taikyti asmenims duomenų tvarkymo pagrindu. Atskaitomybė yra lemiamas klausimas duomenis gaunančios šalies nacionalinių kontrolės mechanizmų atžvilgiu bei duomenų kilmės šalyje ar regione esamų peržiūros galimybių atžvilgiu. Tokie peržiūros mechanizmai numatyti specialiuose susitarimuose, pavyzdžiui, susitarime dėl PNR duomenų, ir EDAPP primygtinai rekomenduoja juos taip pat įtraukti į bendrąjį susitarimą.

V. **PRINCIPŲ ANALIZĖ**

Įvadas

57. Šiame skyriuje atsižvelgiant į toliau nurodytus principus nagrinėjami HLCG dokumente numatyti 12 principų:

— Šie principai rodo, kad JAV ir ES laikosi tam tikro bendro požiūrio dėl principų apimties, nes galima įžvelgti panašumų su Konvencijoje Nr. 108 nustatytais principais.

— Tačiau sutarimo dėl principų apimties nepakanka. Siekiant užtikrinti atitiktį, reikalingas pakankamai griežtas teisinis dokumentas.

— EDAPP apgailestauja, kad prie principų nėra pridėtas aiškinamasis memorandumas.

— Turėtų būti akivaizdu, kad dar prieš apibrėždamos principus abi šalys turi vienodai aiškinti vartojamas formuluotes, pavyzdžiui, dėl asmens duomenų ar saugomų asmenų. Todėl būtų palankiai įvertintas sprendimas pateikti sąvokų apibrėžtis.

1. Išsamus tikslo apibūdinimas

58. Pirmasis HLCG ataskaitos priede nurodytas principas – asmens duomenys tvarkomi teisėtais teisėsaugos tikslais. Kaip nurodyta pirmiau, ES tai reiškia nusikaltimų prevenciją, nustatymą, tyrimą ar patraukimą baudžiamojon atsakomybėn. Tačiau Jungtinėse Valstijose teisėsaugos sąvoka aiškinama plačiau, ją siejant ne vien su nusikaltimų sritimi, bet ir „sienų saugumo, visuomenės saugumo ir nacionalinio saugumo tikslais“. Tokių ES ir JAV nurodytų tikslų neatitikimo pasekmės neaiškios. Nors ataskaitoje minima, kad iš principo šie tikslai gali didžia dalimi sutapti, ir toliau yra labai svarbu tiksliai žinoti, kiek šie tikslai *ne*sutampa. Teisėsaugos srityje atsižvelgiant į asmenims taikomų priemonių poveikį būtina griežtai laikytis tikslo ribojimo principo, o nurodyti principai privalo būti aiškūs ir apriboti. Atsižvelgiant į ataskaitoje numatytą abipusiškumą, taip pat būtų labai svarbu suderinti šiuos tikslus. Trumpai, būtina patikslinti tai, kaip šis principas suprantamas.

2. Vientisumas/duomenų kokybė

59. EDAPP palankiai vertina nuostatą, pagal kurią reikalaujama laiku pateikti tikslius, aktualius ir išsamius asmens duomenis, kurie reikalingi teisėto tvarkymo tikslais. Toks principas yra viena iš pagrindinių veiksmingo duomenų tvarkymo sąlygų.

3. Būtinumas/proporcingumas

60. Pagal šį principą turi būti aiški surinktos informacijos ir šios informacijos būtinumo įstatymu nustatytam teisėsaugos tikslui įvykdyti sąsaja. Šis teisinio pagrindo reikalavimas yra teigiamas veiksnys tvarkymo teisėtumui nustatyti. Tačiau EDAPP teigia, kad nors tai ir sustiprina tvarkymo teisinį tikrumą, tokio tvarkymo teisinis pagrindas yra įtvirtintas trečiosios šalies įstatyme. Trečiosios šalies įstatymas pats savaime nesukuria teisėto pagrindo asmens duomenų perdavimui ([22]). Remiantis HLCG ataskaita, reikėtų daryti prielaidą, kad trečiosios šalies, t. y. Jungtinių Valstijų, įstatymo teisėtumas iš principo pripažįstamas. Vertėtų atkreipti dėmesį į tai, kad nors tokie motyvai gali būti vertinami kaip pagrįsti, atsižvelgiant į tai, kad Jungtinės Valstijos yra demokratinė valstybė, tokia pati schema santykiuose su kita trečiąja šalimi būtų negaliojanti ir jos santykiuose su ta šalimi perkelti negalima.

61. HLCG ataskaitos priede teigiama, kad bet koks asmens duomenų perdavimas turi būti tikslingas, būtinas ir tinkamas. EDAPP pabrėžia, kad siekiant išlaikyti tikslo proporcingumą, tvarkant duomenis neturi būti pernelyg kišamasi į asmens privatumą, o tvarkymo sąlygos turi būti subalansuotos atsižvelgiant į duomenų subjektų teises ir interesus.

62. Dėl šios priežasties teisė susipažinti su informacija turėtų būti suteikiama kiekvienu atveju atskirai, atsižvelgiant į konkretaus tyrimo praktinius poreikius. Trečiųjų šalių teisėsaugos institucijų nuolatinė prieiga prie ES esančių duomenų bazių būtų vertinama kaip neproporcinga tikslui ir nepakankamai pagrįsta priemonė. EDAPP primena, kad

([22]) Žr. visų pirma Direktyvos 95/46/EB 7 straipsnio c ir e punktus. 2002 m. spalio 24 d. nuomonėje 6/2002 dėl oro linijų bendrovių Jungtinėms Valstijoms perduodamų keleivio duomenų ir kitų duomenų 29 straipsnio darbo grupė nurodė, jog negalima sutikti su tuo, kad viešąjį interesą turinčiai trečiajai šaliai priėmus vienašališką sprendimą, būtų reguliariai perduodami išsamūs duomenys, kurie saugomi pagal direktyvą.

net remiantis galiojančiais susitarimais dėl keitimosi duomenimis, pavyzdžiui, susitarimu dėl PNR duomenų, duomenimis turi būti keičiamasi konkrečiomis aplinkybėmis ir susitarimas sudaromas tik ribotam laikui ([23]).

63. Vadovaujantis ta pačia logika, duomenų saugojimo laikotarpis turėtų būti reglamentuotas: atsižvelgiant į konkretų tikslą duomenys turėtų būti saugomi tik tol, kol jie būtini. Jeigu duomenys nustatytam tikslui nebeaktualūs, jie turėtų būti ištrinti. EDAPP griežtai prieštarauja pasiūlymui įsteigti duomenų saugyklas, kuriose būtų saugoma informacija apie neįtariamus asmenis, kad ateityje šia informacija prireikus būtų galima pasinaudoti.

4. Informacijos saugumas

64. Principuose apibrėžiamos priemonės ir procedūros, skirtos apsaugoti duomenis nuo panaudojimo netinkamais tikslais, duomenų pakeitimo ir kitų pavojų, taip pat nuostata, pagal kurią prieiga suteikiama tik įgaliotiems asmenims. EDAPP nuomone, tokios nuostatos pakanka.

65. Šį principą taip pat galėtų papildyti nuostata, kad turėtų būti vedami asmenų, turinčių teisę susipažinti su duomenimis, žurnalai. Tai sustiprintų apsaugos priemonių, skirtų apriboti teisę susipažinti su šiais duomenimis ir užkirsti kelią jų panaudojimui netinkamais tikslais, veiksmingumą.

66. Be to, reikėtų numatyti abipusį keitimąsi informacija saugumo pažeidimo atveju: duomenų gavėjai JAV ir ES būtų atsakingi už kolegų kitoje šalyje informavimą tuo atveju, jei duomenys, kurie jiems buvo pateikti, būtų neteisėtai atskleisti. Tai užtikrins didesnę atsakomybę, taigi, didesnį duomenų tvarkymo saugumą.

5. Specialios asmens duomenų kategorijos

67. EDAPP nuomone, principą, pagal kurį draudžiama tvarkyti neskelbtinus duomenis, labai susilpnina išimtis, suteikianti galimybę tvarkyti tuos neskelbtinus duomenis, kurių atžvilgiu šalies vidaus teisėje yra nustatytos „tinkamos apsaugos priemonės“. Būtent dėl neskelbtino duomenų pobūdžio bet kokia nuostata, leidžianti nukrypti nuo draudimo principo, turi būti tinkamai ir tiksliai pagrįsta, nustatant tikslų ir aplinkybių, kuriomis galima tvarkyti nustatytos rūšies neskelbtinus duomenis, sąrašą bei nurodant duomenų valdytojų, turinčių teisę tvarkyti tokių rūšių duomenis, kompetenciją. Išskyrus apsaugos priemones, kurias būtina patvirtinti, EDAPP nuomone, neskelbtini duomenys patys savaime nėra veiksnys, dėl kurio būtų galima pradėti tyrimą. Jais galėtų būti pasinaudota konkrečiomis aplinkybėmis, bet tik kaip papildoma informacija apie duomenų subjektą, kurio atžvilgiu jau atliekamas tyrimas. Ribotas tokių apsaugos priemonių ir sąlygų sąrašas turi būti pateiktas principą apibūdinančiame tekste.

6. Atskaitomybė

68. Šios nuomonės 55–56 punktuose teigiama, kad būtina veiksmingai užtikrinti asmens duomenis tvarkančių valstybės sektoriaus subjektų atskaitomybę ir susitarime nustatyti garantijas, kaip ši atskaitomybė bus užtikrinta. Tai juolab svarbiau atsižvelgiant į tai, kad trūksta skaidrumo, tradiciškai siejamo su asmens duomenų tvarkymu teisėsaugos srityje. Todėl paminėjimas (kaip yra dabartiniame priede), kad valstybės sektoriaus subjektai yra atskaitingi, nepateikiant jokių papildomų paaiškinimų dėl tokios atskaitomybės sąlygų ir padarinių, nėra pakankama garantija. EDAPP rekomenduoja tokį paaiškinimą pateikti susitarimo tekste.

7. Nepriklausoma ir veiksminga priežiūra

69. EDAPP visiškai pritaria tam, kad būtų įtraukta nuostata, numatanti nepriklausomą ir veiksmingą priežiūrą, kurią vykdytų viena ar kelios valstybės priežiūros institucijos. Jo nuomone, turėtų būti aišku, kaip turėtų būti aiškinamas nepriklausomumas, visų pirma nuo kokių institucijų šios institucijos yra nepriklausomos ir kam jos turi teikti ataskaitas. Šioje srityje būtina nustatyti kriterijus, kuriais turėtų būti atsižvelgta į institucijų ir funkcijų nepriklausomumą vykdomosios valdžios ir teisėkūros organų atžvilgiu. EDAPP primena, kad tai yra labai svarbus veiksnys siekiant užtikrinti veiksmingą atitiktį principams, dėl kurių susitarta. Be to, kaip nurodyta pirmiau, atsižvelgiant į valstybės sektoriaus subjektų atskaitomybės klausimą, itin svarbu minėtoms institucijoms suteikti intervencijos ir vykdymo užtikrinimo įgaliojimus. Duomenų subjektai turi būti aiškiai informuoti apie tai, kad tokios institucijos veikia ir kokią kompetenciją jos turi, kad jos galėtų naudotis joms suteiktomis teisėmis, ypač jei kompetencija atsižvelgiant į duomenų tvarkymo aplinkybes suteikta kelioms institucijoms.

70. Be to, EDAPP rekomenduoja būsimame susitarime taip pat numatyti priežiūros institucijų bendradarbiavimo mechanizmus.

8. Individuali prieiga ir taisymas

71. Teisėsaugos tikslais suteikiant prieigą prie duomenų ir juos taisyti būtinos specialios garantijos. Ta prasme EDAPP palankiai vertina principą, nurodantį, kad asmenims suteikiama/turėtų būti suteikta teisė susipažinti su savo asmens duomenimis ir užtikrintos priemonės siekti, kad „jų asmens duomenys būtų ištaisyti ir (arba) ištrinti“. Tačiau kai kurių neaiškumų vis dar yra dėl asmenų sąvokos apibrėžties (turėtų būti užtikrinta ne tik atitinkamos šalies piliečių, bet ir visų duomenų subjektų duomenų apsauga) ir sąlygų,

([23]) Susitarimas nustos galioti ir nebebus taikomas praėjus septyneriems metams nuo jo pasirašymo, nebent Šalys tarpusavyje susitartų jį pakeisti kitu susitarimu.

kuriomis asmenys galėtų prieštarauti duomenų apie juos tvarkymui. Būtina patikslinti „atitinkamus atvejus“, kuriais galima ir negalima prieštarauti. Duomenų subjektai turėtų būti aiškiai informuoti apie tai, kokiomis aplinkybėmis, atsižvelgiant, pavyzdžiui, į įgaliojimų rūšį, tyrimo rūšį ar kitus kriterijus, jie galės naudotis savo teisėmis.

72. Be to, jei nėra tiesioginės galimybės prieštarauti tvarkymui dėl pagrįstų priežasčių, turėtų būti numatyta galimybė paprašyti už tvarkymo priežiūrą atsakingos nepriklausomos institucijos atlikti netiesioginį patikrinimą.

9. Skaidrumas ir pranešimas

73. EDAPP dar kartą pabrėžia, kaip svarbu užtikrinti veiksmingą skaidrumą, kad asmenys galėtų naudotis savo teisėmis ir būtų prisidėta prie asmens duomenis tvarkančių valstybinių institucijų bendros atskaitomybės didinimo. Jis pritaria parengtiems principams ir primygtinai reikalauja visų pirma nustatyti reikalavimą pateikti asmeniui bendrą *ir* atskirą pranešimą. Tai nurodyta priedo 9 punkte apibrėžtame principe.

74. Tačiau ataskaitos 2 skyriaus B dalyje („Principai, dėl kurių susitarta“) paminėta, kad Jungtinėse Valstijose skaidrumo sąvoka gali apimti „atskirą arba bendrą paskelbimą Federaliniame registre bei atskirą pranešimą ir duomenų atskleidimą teismo procese“. Turi būti akivaizdu, kad vien tik paskelbimo Oficialiajame leidinyje nepakanka, kad būtų užtikrintas duomenų subjekto tinkamas informavimas. EDAPP primena, jog be to, kad duomenų subjektui turi būti pateiktas atskiras pranešimas, informacija jam turi būti pateikta lengvai suprantama forma ir kalba.

10. Žalos atlyginimas

75. Norėdami veiksmingai pasinaudoti jiems suteiktomis teisėmis, asmenys turi turėti galimybę pateikti skundą nepriklausomai duomenų apsaugos institucijai, taip pat siekti žalos atlyginimo nepriklausomame ir nešališkame teisme. Abi galimybės siekti žalos atlyginimo turėtų būti vienodai prieinamos.

76. Teisė kreiptis į nepriklausomą duomenų apsaugos instituciją yra būtina, nes tai yra lanksti ir pigesnė pagalbos priemonė teisėsaugos sąlygomis, kurios asmenims gali atrodyti gana neaiškios. Duomenų apsaugos institucijos taip pat gali suteikti pagalbą duomenų subjektams, norintiems pasinaudoti teisėmis susipažinti su savo asmens duomenimis, kai išimtys pastariesiems draudžia tiesioginę prieigą prie asmens duomenų.

77. Teisė kreiptis į teismus yra papildoma ir būtina garantija, užtikrinanti, kad duomenų subjektai galėtų siekti žalos atlyginimo per instituciją, priklausančią demokratinės struktūros padaliniui, kuri nėra faktiškai duomenis apie juos tvarkanti valstybinė institucija. Šią veiksmingą teisės gynimo priemonę Europos Teisingumo Teismas ([24]) įvertino kaip būtiną priemonę, kuri asmeniui užtikrina veiksmingą jo teisės apsaugą. (...) [Ji] atspindi bendrąjį Bendrijos teisės principą, kuris yra valstybėms narėms bendrų konstitucinių tradicijų pagrindas ir kuris buvo įtvirtintas Europos konvencijos dėl žmogaus teisių ir pagrindinių laisvių apsaugos 6 ir 13 straipsniuose. Apie teisės gynimo priemonių taikymą taip pat aiškiai užsimenama Europos Sąjungos pagrindinių teisių chartijos 47 straipsnyje ir Direktyvos 95/46/EB 22 straipsnyje, nepažeidžiant jokių administracinių teisės gynimo priemonių.

11. Sprendimai atskirais automatizuoto duomenų tvarkymo atvejais

78. EDAPP palankiai vertina nuostatą, numatančią atitinkamas apsaugos priemones automatizuoto asmens duomenų tvarkymo atvejais. Jis pažymi, kad bendras supratimas apie tai, kas laikoma „atitinkamiems asmens interesams ypač nepalankiu veiksmu“, patikslintų šio principo taikymo sąlygas.

12. Tolesni duomenų perdavimai

79. Kai kurių tolesnių perdavimų nustatytos sąlygos yra neaiškios. Visų pirma, kai atliekant tolesnį perdavimą būtina laikytis tarptautinių susitarimų ir duomenis siunčiančių bei gaunančių šalių susitarimų, turėtų būti nurodyta, ar tai taikytina pirmąjį perdavimą inicijavusių dviejų šalių susitarimams ar su tolesniu perdavimu susijusių dviejų šalių susitarimams. Pasak EDAPP, bet kuriuo atveju būtini pirmąjį perdavimą inicijavusių dviejų šalių susitarimai.

80. EDAPP taip pat atkreipia dėmesį į labai plačią „teisėtų viešųjų interesų“, kuriais vadovaujantis galima toliau perduoti duomenis, sąvokos apibrėžtį. Visuomenės saugumo sritis tebėra neaiški, o perdavimų išplėtimas etikos pažeidimo atveju ar reglamentuojamų profesijų srityje yra nepagrįsta ir neadekvati priemonė teisėsaugos srityje.

VI. **IŠVADA**

81. EDAPP palankiai vertina bendrą ES ir JAV institucijų darbą teisėsaugos srityje, kai labai svarbu užtikrinti duomenų apsaugą. Vis dėlto, jis primygtinai pabrėžia, kad tai yra labai sudėtingas klausimas, visų pirma tikslios taikymo

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

srities ir pobūdžio požiūriu, todėl jį būtina atidžiai ir išsamiai nagrinėti. Tarpvalstybinio susitarimo dėl duomenų apsaugos poveikį reikėtų atidžiai svarstyti remiantis galiojančiais teisės aktais ir atsižvelgiant į padarinius piliečiams.

82. EDAPP reikalauja daugiau aiškumo ir konkrečių nuostatų visų pirma dėl šių aspektų:

— turi būti patikslintas dokumento pobūdis; siekiant užtikrinti pakankamą teisinį tikrumą, tai turėtų būti teisiškai privalomas dokumentas;

— turi būti atliktas išsamus tinkamumo įvertinimas, pagrįstas būtiniausiais reikalavimais dėl schemos esmės, specifiškumo ir priežiūros aspektų. EDAPP nuomone, bendrojo dokumento tinkamumą galima pripažinti tik tuo atveju, jei toks dokumentas yra susietas su kiekvienam konkrečiam atvejui skirtais specialiais susitarimais;

— turi būti nustatyta apribota taikymo sritis, pateikiant aiškią ir bendrą teisėsaugos tikslų, kuriems kyla pavojus, sąvokos apibrėžtį;

— turi būti tiksliai apibrėžtos sąlygos, kuriomis privačius subjektus galima įtraukti į duomenų perdavimo schemas;

— turi būti laikomasi proporcingumo principo, numatant, kad duomenimis turi būti keičiamasi kiekvienu atveju, kai tam yra konkretus poreikis;

— turi būti nustatyti griežti priežiūros mechanizmai ir duomenų subjektams prieinami žalos atlyginimo mechanizmai, įskaitant administracines ir teismines teisės gynimo priemones;

— turi būti nustatytos veiksmingos priemonės, garantuojančios, kad savo teisėmis galės naudotis visi duomenų subjektai, neatsižvelgiant į jų pilietybę;

— turi būti numatyta galimybė dalyvauti nepriklausomoms duomenų apsaugos institucijoms, visų pirma priežiūros ir duomenų subjektams teikiamos pagalbos srityse.

83. EDAPP primygtinai reikalauja vengti skubos rengiant principus, nes tokiu būtų patvirtinti tik netinkami sprendimai, o tai turėtų neigiamų pasekmių tiems, kuriems jie skirti duomenų apsaugos srityje. Todėl šiame etape geriausia būtų parengti veiksmų planą, kuriuo vadovaujantis būtų siekiama galimo susitarimo vėlesniame etape.

84. EDAPP taip pat reikalauja daugiau skaidrumo duomenų apsaugos principų rengimo procese. Demokratiškos diskusijos dėl dokumento būtų naudingos ir dokumentu būtų užsitikrinta būtina parama ir pripažinimas tik tuo atveju, jei diskusijose dalyvautų visi suinteresuoti subjektai, įskaitant Europos Parlamentą.

Priimta Briuselyje, 2008 m. lapkričio 11 d.

Peter HUSTINX

Europos duomenų apsaugos priežiūros pareigūnas