Vilniaus universiteto Teisės
fakulteto
Viešosios teisės katedra

Miglės Vilkaitės,
V kurso, Tarptautinės ir
Europos Sąjungos teisės
šakos studentės

Magistro darbas

Asmens duomenų perdavimas į trečiąsias valstybes: praktika ir problematika

Vadovas: Lekt. dr. Inga Martinkutė

Recenzentas: Asist. dr. Deimilė Prapiestytė

Vilnius
2023

ANOTACIJA IR PAGRINDINIAI ŽODŽIAI

Šiame darbe analizuojami duomenų perdavimo sampratos ir duomenų perdavimo pagrindai, leidžiantys valstybėms narėms perduoti asmens duomenis iš Europos Sąjungos į trečiasias valstybes. Darbo temai atskleisti analizuojami laisvo duomenų srauto interesai bei jų apsauga. Darbe atskleidžiami ne tik duomenų perdavimo mechanizmai pagal Bendrąjį duomenų apsaugos reglamentą, bet ir analizuojama kiekvieno iš jų problematika. Praktinė Bendrojo duomenų apsaugos reglamento nuostatų V skyriaus praktinė problematika atskleidžiama tyrinėjant praktines situacijas. Galiausiai, atsižvelgiant į pirmųjų darbo dalių analizės rezultatus, aprašomos su duomenų perdavimu kylančios problemos pasirinktose pasaulio valstybėse.

Pagrindiniai žodžiai: duomenų perdavimas, trečioji valstybė, duomenys, tinkamos apsaugo spriemonės, duomenų tvarkymas, principai.

ANNOTATION AND KEY WORDS

This paper analyzes the concepts of data transfer and the basics of data transfer, which allow member states to transfer personal data from the European Union to third countries. The interests of free data flow and their protection are analyzed to reveal the topic of the work. The work reveals not only the data transfer mechanisms according to the General Data Protection Regulation, but also analyzes each of their problems. Practical problems of Chapter V of the General Data Protection Regulation are revealed by studying practical situations. Finally, taking into account the results of the analysis of the first parts of the work, the problems arising with data transfer in selected countries of the world are described.

Keywords: data transfer, third country, data, adequate protection measures, data management, principles.

Turinys

ĮVADAS 4

1. Asmens duomenų tvarkymo principai, perdavimo samprata ir trečiosios šalies apibrėžtis pagal BDAR 8

1.1. Trečiųjų šalių apibrėžimas 10

1.2. Asmens duomenų perdavimo samprata 12

2. Bendrieji duomenų perdavimo principai 15

2.1. Asmens duomenų perdavimas remiantis sprendimu dėl tinkamumo 16

2.1.1. Sprendimų dėl tinkamumo priėmimo procedūra. 18

2.1.1. Tinkamumo kriterijai. 20

2.1.1. Sprendimo dėl tinkamumo panaikinimas, pakeitimas ar sustabdymas. 23

2.1. Asmens duomenų perdavimas taikant tinkamas apsaugos priemones 24

2.2.1 Standartinės sutarčių sąlygos 25

2.2.2. Įmonei privalomos taisyklės 27

2.2.3. Patvirtinti elgesio kodeksai ir sertifikavimo mechanizmai 29

2.2. Asmens duomenų perdavimas taikant nukrypti leidžiančias nuostatas 31

2.1. Sutikimas. 33

3. Asmens duomenų perdavimo į trečiąsias šalis problematika didžiųjų pasaulio valstybių atžvilgiu 35

3.1. Duomenų perdavimas į Kiniją 35

3.1. Duomenų perdavimas į Jungtinę Karalystę po "Brexit" 37

3.2. Duomenų perdavimas į Rusiją 40

IŠVADOS 42

LITERATŪROS SĄRAŠAS.....43
SANTRAUKA 47
SUMMARY 48

ĮVADAS

Duomenų perdavimas į trečiąsias šalis reiškia asmeninės arba neskelbtinos informacijos judėjimą iš vienos šalies į kitą už jurisdikcijos, iš kurios buvo gauti duomenys, ribų. Mūsų tarpusavyje susijusiame skaitmeniniame pasaulyje, kuriame informacija sklandžiai plinta tarp valstybių, itin svarbu užtikrinti šių duomenų privatumą, saugumą ir teisėtą perdavimą.

Duomenų perdavimas į trečiąsias šalis sulaukė didelio dėmesio dėl sudėtingumo, atsirandančio dėl skirtingų duomenų apsaugos įstatymų, reglamentų ir kultūrinių skirtumų skirtinguose regionuose. Šie duomenų perdavimai įvyksta dėl daugybės priežasčių: pasaulinių verslo operacijų, debesies teikiamų paslaugų, užsakomųjų paslaugų iki tarptautinio bendradarbiavimo ir partneryščių. Tačiau tokie perdavimai susiduria su iššūkiais, pirmiausia kylančiais dėl skirtingų teisinių sistemų, susijusių su duomenų apsauga ir privatumu. Pavyzdžiui, kai kurios šalys gali turėti išsamius duomenų apsaugos įstatymus, tokius kaip Europos Sąjungos Bendrasis duomenų apsaugos reglamentas (BDAR), kuris nustato griežtus asmens duomenų perdavimo už ES ribų standartus. Priešingai, kitose šalyse gali trūkti panašių tvirtų sistemų, todėl kyla susirūpinimas dėl tinkamos asmenų privatumo ir teisių apsaugos. Duomenų perdavimo į trečiąsias šalis teisėtumo ir saugumo užtikrinimas dažnai apima tokius mechanizmus kaip standartinės sutarties sąlygos, privalomos įmonių taisyklės, aiškaus duomenų subjektų sutikimo gavimas arba sertifikatų ir elgesio kodeksų, kurie atitinka griežtus duomenų apsaugos standartus, panaudojimas. Didelio atgarsio sulaukę duomenų pažeidimai, privatumo pažeidimai ir teisiniai ginčai pabrėžė esminį poreikį sukurti skaidrius, saugius ir standartizuotus duomenų perdavimo tarpvalstybinius metodus. Tam būtinas vyriausybių, reguliavimo institucijų, organizacijų ir technologijų ekspertų bendradarbiavimas, kad būtų galima naršyti sudėtingame tarptautinio duomenų perdavimo aplinkoje, kartu gerbiant asmenų teises į duomenų apsaugą ir privatumą. Be to, pastarieji įvykiai, pvz., Europos Sąjungos Teisingumo Teismo sprendimas Schrems II, dar labiau supaprastino ir tikrino duomenų perdavimo mechanizmus, pabrėždami, kad reikia tvirtų apsaugos priemonių ir trečiųjų šalių įstatymų vertinimo. Galiausiai išlaikyti pusiausvyrą tarp laisvo duomenų srauto, skirto naujovėms, ekonomikos augimui ir pasauliniam bendradarbiavimui, kartu užtikrinant asmenų privatumo teises, išlieka nuolatinis iššūkis. Tobulėjant technologijoms ir stiprėjant pasauliniam tarpusavio ryšiui, norint veiksmingai spręsti šiuos iššūkius, reikia gerai suprasti teisinius,

etinius ir techninius aspektus, kad būtų užtikrintas atsakingas ir saugus duomenų perdavimas į trečiąsias šalis.

Temos aktualumas. Duomenų perdavimo į trečiąsias šalis svarba apima įvairias sritis, įskaitant ekonomines, socialines ir technologijų sritis, ir tai daro didelį poveikį įmonėms, visuomenėms ir asmenims. Ekonominiu požiūriu sklandus duomenų srautas tarp valstybių yra šiuolaikinių įmonių gyvybės šaltinis, įgalinantis pasaulinę prekybą, tarpvalstybines investicijas ir efektyvų tarptautinių korporacijų funkcionavimą. Tačiau, jei nėra patikimų saugaus ir teisėto duomenų perdavimo mechanizmų, įmonės susiduria su kliūtimis siekdamos pasinaudoti masto ekonomija, vykdyti tarptautinius sandorius ir teikti paslaugas klientams visame pasaulyje. Gebėjimas orientuotis duomenų perdavimo taisyklių sudėtingumo srityje tiesiogiai veikia prieigą prie rinkos, konkurencingumą ir naujovių potencialą pasaulinėje rinkoje. Visuomeniniu lygmeniu atsakingas ir etiškas duomenų perdavimas yra labai svarbus siekiant išsaugoti demokratines vertybes ir apsaugoti asmens teises. Privatumo pažeidimai, neteisėta prieiga prie duomenų arba netinkamos apsaugos priemonės tarpvalstybinio duomenų perdavimo metu gali sumenkinti pasitikėjimą institucijomis ir turėti įtakos piliečių pasitikėjimui skaitmeninėmis technologijomis ir platesne skaitmenine ekonomika. Taigi asmens duomenų apsaugos užtikrinimas tarptautinio perdavimo metu yra labai svarbus siekiant išsaugoti asmens autonomiją, orumą ir laisvę vis labiau tarpusavyje susijusiame pasaulyje. Technologiška pažanga, tokia kaip debesų kompiuterija, dirbtinis intelektas ir internetas, labai priklauso nuo laisvo duomenų srauto. Dėl šių naujovių dažnai reikia apibendrinti ir analizuoti didžiulius duomenų kiekius, kurie dažnai peržengia nacionalines sienas. Tačiau dėl šio didesnio tarpusavio ryšio atsiranda atsakomybė užtikrinti, kad duomenys būtų apsaugoti ir privatumo teisės būtų paisomos įvairiose jurisdikcijose. Galimybė sklandžiai perduoti duomenis, laikantis aukštų saugumo ir privatumo standartų, yra esminis dalykas skatinant technologinę pažangą nepažeidžiant asmenų teisių. Be to, besivystant skaitmeninei aplinkai, geopolitinė įtampa ir skirtinga nacionalinė politika dar labiau pabrėžia veiksmingo duomenų perdavimo į trečiąsias šalis valdymo svarbą. Prieštaringi duomenų apsaugos įstatymai, skirtingi standartai ir skirtingų vyriausybių skirtingi požiūriai į stebėjimą ir prieigą prie duomenų sukuria sudėtingumą, kuris turi tiesioginės įtakos įmonėms, vyriausybėms ir tarptautiniam bendradarbiavimui. Iš esmės duomenų perdavimo trečiosioms šalims svarba viršija vien techninį ar teisinį atitikimą; ji apima platesnę ekonomikos augimo, visuomenės pasitikėjimo, technologinių naujovių ir tarptautinių santykių struktūrą. Pusiausvyra tarp duomenų srauto palengvinimo siekiant pasaulinės

pažangos, kartu užtikrinant tvirtą asmenų privatumo ir teisių apsaugą, tebėra esminis iššūkis šiandieniniame tarpusavyje susijusiame ir duomenimis pagrįstame pasaulyje.

Darbo tikslas. Magistro darbu, vadovaujantis teisine literatūra, Teisingumo Teismo praktika, galiojančiomis teisės aktų nuostatomis, siekiama konstruktyviai atskleisti duomenų perdavimo už Europos Sąjungos ribų problematiką ir reikšmę Europos Sąjungos teisėje. Šio tikslo kontekste siekiama atlikti dualią terminų analizę – visų pirma, identifikuoti duomenų perdavimo mechanizmų sampratą pagal Europos Sąjungos teisę. Antru lygmeniu, siekiama įvertinti kokios problemos gali kilti praktikoje perduodant asmens duomenis už ES ribų.

Darbo uždaviniai. Siekiant įgyvendini magistro darbo tikslą, buvo iškelti šie uždaviniai:

1. Nagrinėjant teisinę literatūrą ir Teisingumo Teismo praktiką, atskleisti duomenų apsaugos ir laisvo duomenų judėjimo Europos Sąjungoje reikšmę.
2. Išanalizuoti duomenų perdavimo bei trečiosios valstybės sampratų reikšmę BDAR kontekste.
3. Identifikuoti duomenų perdavimo būdus pagal BDAR ir su jais susijusia praktine problematika.
4. Išanalizuoti duomenų perdavimo problematiką pasirinktose valstybėse.

Darbo objektas. Magistro darbo objektą sąlygoja darbo tikslas bei jam pasiekti iškelti uždaviniai. Darbo tyrimo objektas – asmens duomenų perdavimo būdų analizės problematika per BDAR ir teisinės literatūros prizmę. Atsižvelgiant į tai, kad magistro darbą sudaro trys esminės struktūrinės dalys, pirmoje magistro darbo dalyje siekiama atskleisti duomenų perdavimo į trečiasias valstybes būdų sampratas. Antroje darbo dalyje yra nagrinėjama duomenų perdavimo mechanizmų problematika. Trečioje darbo dalyje, vadovaujantis pirmose darbo dalyse gautomis išvadomis, vertinama duomenų apsauga bei duomenų perdavimas į pasirinktas valstybes.

Tyrimo metodai. Darbo objektas analizuojamas pasitelkiant lingvistinį, teleologinį, istorinį, sisteminį ir loginį metodą.

1. Lingvistinis - šis metodas magistro darbe taikomas analizuojamo Bendrojo duomenų apsaugos reglamento nuostatų, susijusioms su duomenų perdavimu į trečiasias valstybes, reikšmei atskleisti.
2. Teleologinis - šis metodas padeda išsiaiškinti ES pirminės ir antrinės teisės normų pobūdį, tikslą ir jų taikymo sferą.
3. Istorinis - šio metodo pagalba siekiama atskleisti Bendrojo duomenų apsaugos reglamento raidą ir pritaikymą.
5. Loginis - šio metodo pagalba autorė vertina teismų sprendimuose bei teisės doktrinoje esančių pozicijų pagrįstumą, formuoja atitinkamą poziciją magistro darbe keliamais probleminiais klausimais.

Darbo originalumas. Autorės žiniomis, duomenų perdavimo į trečiasias valstybes problematika plačiai nėra nagrinėta. Daugiausia dėmesio literatūroje yra skirta analizuojant duomenų perdavimą ir problematiką tarp ES ir JAV. Būtent duomenų perdavimo problematika, kuri susijusi ir su kitomis šalimis, Lietuvoje, autorės žiniomis, plačiau analizuota nebuvo. Užsienio teisinėje literatūroje yra darbų, nagrinėjusių atskirus šios temos aspektus: esama darbų nagrinėjančių JAV ir ES laisvo duomenų judėjimo kontekstą, nagrinėti ir atitinkamų valstybių narių, pavyzdžiui Jungtinės Karalystės, duomenų apsaugos užtikrinimo ir perdavimo klausimai.

Pagrindiniai šaltiniai. Atsižvelgiant į magistro darbo tikslus, uždavinius bei darbo objektą, didžiausią svarbą turi Teisingumo Teismo praktika ir Europos Sąjungos teisės šaltiniai. Taip pat svarbūs ir kiti šaltiniai: M. Krzysztofek, W. Kuan Hon, L. Wittershagen, C. Kuner, L. A Bygrave, C. Docksey, L. Drechsler bei užsienio teisininkų moksliniai darbai ir teisiniai straipsniai atskirais šio magistro darbo temos aspektais.

1. Asmens duomenų tvarkymo principai, perdavimo samprata ir trečiosios šalies apibrėžtis pagal BDAR

BDAR[1] 5 straipsnio 1 dalyje nurodyti penki asmens duomenų tvarkymo principai. Svarbu tai, kad kiekviena asmens duomenų tvarkymo operacija (įskaitant perdavimą) privalo atitikti šiuos principus. Pagal šiuos principus reikalaujama, kad asmens duomenys būtų:

- tvarkomi sąžiningai, skaidriai ir teisėtai. Šis principas apima reikalavimą, kad kiekviena asmens duomenų tvarkymo operacija privalo remtis BDAR nustatyta teisėto tvarkymo sąlyga ir duomenų subjektui būtų pateikiama pakankamai informacijos apie jo asmens duomenų tvarkymą, kad jis turėtų galimybę žinoti, kaip tvarkomi jo asmens duomenys. Skaidrumo ir sąžiningumo principai yra glaudžiai susiję su BDAR 13 ir 14 straipsnių taikymu. BDAR 13 ir 14 straipsniuose yra nurodyta, kokią informaciją duomenų valdytojas privalo pateikti duomenų subjektui. Šio magistrinio darbo kontekste svarbus yra BDAR 13 straipsnio 1 dalies f punktas ir 14 straipsnio 1 dalies f punktas, kurie numato, kad duomenų valdytojas privalo pateikti informaciją duomenų subjektui apie duomenų valdytojo ketinimą asmens duomenis perduoti į trečiąją valstybę arba tarptautinei organizacijai ir Europos komisijos sprendimo dėl tinkamumo buvimą ar nebuvimą, arba 46 ar 47 straipsniuose arba 49 straipsnio 1 dalies antroje pastraipoje nurodytų perdavimų atveju – tinkamas arba pritaikytas apsaugos priemones ir būdus, kaip gauti jų kopiją arba kur suteikiama galimybė su jais susipažinti;
- renkami konkrečiu, aiškiai apibrėžtu ir teisėtu tikslu ir toliau netvarkomi nesuderinamais su tais tikslais. Duomenų tvarkymo tikslo apribojimo principo tikslas – apsaugoti duomenų subjektą duomenų valdytojams nustatant ribas, kurių neperžengdami jie gali naudoti duomenų subjektų duomenis ir užtikrinti tvarkymo sąžiningumą;
- adekvatūs, tinkami ir ne pertekliniai, atsižvelgiant į tikslus, dėl kurių jie renkami. Pažymėtina, kad duomenų kiekio mažinimo principas yra glaudžiai susijęs su duomenų tvarkymo tikslo apribojimo principu. Įgyvendinant duomenų kiekio mažinimo principą, reikia užtikrinti tinkamą duomenų tvarkymo tikslų ir duomenų apimties santykį. Tvarkomų duomenų kiekį turi apibrėžti iš anksto duomenų valdytojo įvardytas duomenų tvarkymo tikslas.;

[1] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – BDAR).

• tikslūs ir, jei reikia, nuolat atnaujinami; saugomi tokia forma, kad duomenų subjektą būtų galima identifikuoti ne ilgiau, nei tai yra būtina duomenų tvarkymo tikslui pasiekti (žr. Gairės 4/2019 dėl 25 straipsnio, Versija 2.0 Priimta 2020 m. spalio 20 d., p. 15-26).

Pagal BDAR asmens duomenys apibrėžiami kaip „asmens duomenys – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius“ (BDAR 4 straipsnio 1 punktas).

Asmens duomenų tvarkymo sąvoka yra pateikta BDAR 4 straipsnio 2 punkte, kuriame nurodyta, kad asmens duomenų tvarkymas – bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka, kaip antai rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas. Atsižvelgiant į tai, asmens duomenų perdavimas (įskaitant perdavimą į trečiąsias valstybes) patenka į asmens duomenų tvarkymo sąvoką.

Pagal Europos Sąjungos (toliau – ES arba Europos Sąjunga) teisę duomenų perdavimas gali būti uždraustas, jei yra „reali ir rimta rizika, kad perdavus asmens duomenis kitai Šaliai bus apeinamos Konvencijos nuostatos“ arba jei Šalis yra įpareigota tai daryti „suderintų apsaugos taisyklių, kuriomis dalijasi valstybės, priklausančios regioninei tarptautinei organizacijai“.

Iš esmės Europos Sąjungos teisėje bei Bendrajame duomenų apsaugos reglamente, nustatyta, kad duomenys Europos Sąjungoje gali judėti laisvai. Tačiau jame nustatyti specialūs reikalavimai, susiję su asmens duomenų perdavimu užsienio trečiosioms šalims ir tarptautinėms organizacijoms. Reglamente pripažįstama tokio duomenų judėjimo svarba, visų pirma atsižvelgiant į tarptautinę prekybą ir bendradarbiavimą, be to, pripažįstama didesnė asmens duomenims kylanti rizika. Todėl reglamentu siekiama užtikrinti, kad, perduodant duomenis trečiosioms šalims, būtų užtikrinamas toks pat asmens duomenų apsaugos lygis, kuris galioja ES (Europos duomenų apsaugos teisės vadovas. 2018 m., p. 258-261).

Europos Sąjungos Teisingumo Teismas (toliau – ESTT) byloje Shrems II yra nurodęs jog „visos [šio] skyriaus nuostatos taikomos siekiant užtikrinti, kad nebūtų pakenkta šiuo

reglamentu garantuojamam fizinių asmenų apsaugos lygiui“. Todėl šis apsaugos lygis turi būti užtikrintas, kad ir kokia būtų to skyriaus nuostata, kuria remiantis asmens duomenys perduodami į trečiąją šalį. BDAR V skyriumi siekiama užtikrinti šio aukšto apsaugos lygio tęstinumą, kai asmens duomenys perduodami į trečiąją šalį, vadovaujantis šio reglamento 6 konstatuojamojoje dalyje nurodytu tikslu.“ (Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas byloje C-311/18, 92-93 p.).

Atsižvelgiant į išvardintų duomenų perdavimo trečiosioms šalims pagrindų svarbumą bei į tai, kad visi BDAR V skyriuje išvardinti duomenų perdavimo būdai yra savarankiški, toliau darbe bus analizuojamas kiekvienas perdavimo būdas bei su juo susijusi problematika.

1.1. Trečiųjų šalių apibrėžimas

Europos Sąjungoje ir kitose Europos Ekonominės Erdvės (toliau – EEE arba Ekonominė erdvė) šalyse yra nustatyti unikalūs griežti asmens duomenų apsaugos standartai. Europos Komisija jau yra nustačiusi, kad kelios ne ES narės užtikrinama ES lygmens duomenų apsaugos lygį. Tačiau ne visos didžiosios pasaulio valstybės pritaria šiam duomenų perdavimo modeliui modeliui. Būtent dėl to, kad kai kuriose šalyse nėra tinkamų duomenų apsaugos priemonių, gali kilti konfliktų dėl Europos piliečių asmens duomenims taikomų apsaugos priemonių tais atvejais, kai tokie duomenys perduodami į tas šalis. Vienas iš tokių neatitikimų pavyzdžių yra tai, kad ES yra nustačiusi bendrąsias duomenų tvarkymo taisykles, kurios taikomos neatsižvelgiant į duomenų valdytojo sektorių, o Jungtinėse Amerikos Valstijose (toliau – JAV) yra taikomas sektorinis mechanizmas, pagal kurį derinamas reguliavimas ir savireguliavimas įvairiose ekonomikos ir socialinio gyvenimo srityse, kurios laikomos ypač svarbiomis. Kitas svarbus skirtumas yra tas, kad JAV teisė saugo tik JAV piliečių privatumą, o ES teisės nuostatos dėl privatumo apsaugos taikomos ne tik Europos piliečiams, bet ir trečiųjų šalių

piliečių duomenims, kai tokie duomenys tvarkomi Europos Sąjungoje. Todėl labai svarbu įgyvendinti priemones, kuriomis būtų užtikrinta į ES nepriklausančias šalis perduodamų asmens duomenų apsauga, prilygstanti Europos standartams, tačiau kartu nesudarant nereikalingų kliūčių ES valstybių narių eksportui ar tarptautiniam bendradarbiavimui kitose srityse. Europos Taryba turėjo tai omenyje priimdama 1981 m. sausio 28 d. Konvenciją Nr. 108 (toliau - Konvencija Nr. 108) dėl dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu. Konvencijos Nr. 108 preambulėje nurodyta, kad "pageidautina išplėsti kiekvieno žmogaus teisių ir pagrindinių laisvių, ypač teisės į privataus gyvenimo gerbimą, garantijas, atsižvelgiant į didėjantį automatizuotai tvarkomų asmens duomenų srautą per sienas", ir pareiškė, kad "kartu [ji] yra įsipareigojusi užtikrinti informacijos laisvę nepriklausomai nuo sienų". Siekdama užkirsti kelią bet kokiam šių dviejų vertybių konfliktui, ji pareiškė, kad "būtina suderinti pagrindines vertybes - pagarbą privatumui ir laisvą informacijos judėjimą tarp žmonių". Poreikis suderinti asmens duomenų apsaugos taisykles tarp Ekonominio bendradarbiavimo ir plėtros organizacijos šalių narių, t. y. santykiuose tarp ES / EEE valstybių narių ir trečiųjų šalių, įskaitant JAV, atsispindi 2013 m. liepos 11 d. Ekonominio bendradarbiavimo ir plėtros organizacijos (toliau – EBPO) rekomendacijoje "EBPO privatumo Sistema". Sąlygos, kurių turi būti laikomasi perduodant asmens duomenis trečiosioms valstybėms, nustatytos BDAR 44-49 straipsniuose. Tačiau norint patikslinti šių nuostatų taikymo sritį, pirmiausia reikia apibrėžti "trečiąsias šalis" ir "asmens duomenų perdavimą" kaip duomenų tvarkymo aspektą. Vienas iš pagrindinių principų - neribotas keitimasis asmens duomenimis tarp ES valstybių narių. Šis principas išplaukia iš keturių pagrindinių judėjimo laisvių, kuriomis apibrėžiama Europos Sąjunga, t. y. laisvo asmenų, prekių, paslaugų ir kapitalo judėjimo, įvesto 1957 m. Romos sutartimi, kuria buvo įsteigta Europos ekonominė bendrija ir kuri tebėra ES pagrindas. Tai aiškiai numatyta ir BDAR 1 straipsnio 3 dalyje, pagal kurią draudžiamas bet koks laisvo asmens duomenų judėjimo ES ribojimas ar draudimas. Kartu su laisvo keitimosi asmens duomenimis ES principo suformulavimu nustatomas vienodas duomenų apsaugos standartas. Taip užkertamas kelias galimoms tarptautinio ekonominio bendradarbiavimo kliūtims Europos Sąjungoje, kurios galėtų atsirasti dėl duomenų perdavimo tarp valstybių narių ribojimo. Kartu užtikrinama, kad būtų gerbiama valstybių narių piliečių teisė į jų asmens duomenų apsaugą. Kad reikia asmens duomenų perdavimą ES reglamentuojančių teisinių nuostatų, paaiškėjo 1989 m., kai Prancūzijos asmens duomenų apsaugos institucija CNIL papriešta ravo, kad Prancūzijos "Fiat"| filialas perduotų asmens duomenis Italijos filialui, motyvuodama tuo, kad Italijoje tuo metu nebuvo asmens duomenų apsaugos įstatymo. CNIL nustatė, kad duomenų perdavimas

priklauso nuo Italijos filialo sutartinio įsipareigojimo užtikrinti perduodamiems duomenims apsaugą, lygiavertę Prancūzijoje taikomai apsaugai. Kaip nurodyta pirmiau, laisvas keitimasis asmens duomenimis ES viduje ir duomenų perdavimo į trečiąsias šalis apribojimas yra bendra taisyklė.

Reikia pažymėti, kad teisinės sąvokos „asmens duomenų perdavimas į trečiąją šalį arba tarptautinei organizacijai“ apibrėžties BDAR nerasime, o duomenų perdavimo apibrėžties praktika yra ribota. Laisvas duomenų perdavimas taikomas ne tik ES, bet ir 1992 m. gegužės 2 d. Porto mieste pasirašytam ir nuo 1994 m. sausio 1 d. galiojančiam Ekonominės erdvės susitarimui, kuris yra laisvosios prekybos zonos, apimančios visas ES valstybes nares ir tris iš keturių Europos laisvosios prekybos asociacijos (ELPA) valstybių narių (Islandija, Lichtenšteinas ir Norvegija) teisinis pagrindas. Todėl šios šalys nėra trečiosios šalys, kaip apibrėžta BDAR 44 ir kituose straipsniuose. Kita vertus, Šveicarija, taip pat ELPA valstybė narė, yra trečioji šalis, nes ji nėra EEE narė, priešingai nei kitos trys ELPA narės. Duomenis Šveicarijai, kaip trečiajai šaliai, leidžiama perduoti pagal 2000 m. liepos 26 d. Komisijos sprendimą 2000/518/EB dėl Šveicarijoje teikiamų asmens duomenų tinkamos apsaugos (GDPR: Personal Data Protection in the European Union, Mariusz Krzysztofek, 2021 m., p. 261-263).

1.2. Asmens duomenų perdavimo samprata

Nepaisant savo išsamumo asmens duomenų apsaugos atžvilgiu BDAR taip pat nepateikia ir teisinės duomenų perdavimo apibrėžties. Nepriklausomai nuo to, duomenų perdavimo ypatybė (kaip apibrėžta BDAR 44-49 straipsniuose) yra ta, kad iš esmės pakanka vien asmens duomenų judėjimo už Europos ekonominės erdvės ribų, kad juos būtų galima laikyti duomenų perdavimu į trečiąsias šalis. Be to, BDAR nediferencijuojami duomenų perdavimui taikomi

reikalavimai pagal numatomą jų tvarkymo trečiojoje šalyje po perdavimo apimtį. Todėl duomenų perdavimo už EEE ribų leistinumo taisyklės taikomos neatsižvelgiant į tai, ar duomenys bus aktyviai naudojami, ar tik saugomi. Lindqvist[2] sprendime yra nurodoma, kad duomenų perdavimas turėtų būti aktyvus veiksmas, apimantis duomenų siuntimą, o ne tik pasyvią prieigą prie jų. Tačiau tai nebūtinai reiškia, jog prieigos prie duomenų suteikimas taip pat negali būti laikomas duomenų „perdavimu“. Iš tiesų panašu, kad minėtas sprendimas grindžiamas keletu konkrečių veiksnių (būtinybė interneto naudotojui asmeniškai imtis veiksmų, kad galėtų susipažinti su interneto svetaine, faktas, kad visa informacija buvo pateikta švedų kalba ir nebuvo skirta skaityti ir naudoti už šios šalies ribų, taip pat ankstyvas interneto technologijų išsivystymo lygis tuo metu), kurie gali apriboti bylos faktines aplinkybes (The EU General Data Protection Regulation (GDPR): A Commentary 2020 m. C. Kuner, L. A Bygrave, C. Docksey, L. Drechsler; p. 762-763). Akivaizdu, kad Direktyvoje 95/46/EB[3] numatyta, jog asmens duomenys gali būti „perduodami“ fiziškai gabenant į trečiąją šalį fizinę įrangą arba laikmeną, kurioje „laikomi“ asmens duomenys sudarantys bitų modeliai. Duomemnų gabenimas ne elektroninėmis priemonėmis laikomas „perdavimu“, jei gabenami asmens duomenys yra „skirti tvarkyti trečiojoje šalyje po perdavimo“. Taigi, „perdavimas“ gali apimti disketės su asmens duomenimis išsiuntimą į trečiąją šalį arba net darbuotojo kelionę už EEE ribų su nešiojamuoju kompiuteriu, kuriame yra asmens duomenys. Taip pat asmens duomenys gali būti „perduodami" į trečiąją šalį be trečiosios šalies gavėjo, kaip pirmiau pateiktame „kelionės su nešiojamuoju kompiuteriu“ pavyzdyje. Tačiau daugelyje duomenų perdavimo atvejų trečiosios šalys yra gavėjai. Yra numatyti trys „perdavimo“ tipai, susiję su asmens duomenų perdavimu atitinkamai:

a) Bendrijoje įsikūrusio duomenų valdytojo - kitam trečiojoje šalyje įsikūrusiam duomenų valdytojui;

b) Bendrijoje įsikūręs duomenų valdytojas - trečiojoje šalyje įsikūrusiam duomenų tvarkytojui, tvarkančiam duomenis duomenų valdytojo vardu;

c) Bendrijoje įsikūręs duomenų subjektas - trečiojoje šalyje įsikūrusiam duomenų valdytojui.

„Perdavimas“ paaiškintas kaip „bet kokia procedūra, pagal kurią duomenys bus perduoti už Europos Sąjungos ribų“, neatsižvelgiant į tai, kas perduoda duomenis, įskaitant perdavimą „asmenims, atsakingiems už duomenis perduodančio asmens interneto svetaines“, ir kai

[2] Europos Sąjungos Teisingumo Teismo 2003 m. lapkričio 6 d. sprendimas Lindqvist.

[3] 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 (toliau - Direktyva 95/46/EB).

duomenys „perduodami už Europos Sąjungos teritorijos ribų“, išskyrus perdavimą ambasadai trečiojoje šalyje, nes pagal tarptautinę teisę ambasadoms taikoma atitinkama nacionalinė teisė. Kaip parodyta pirmiau, sąvoka „perdavimas“ reiškia daugelį dalykų. (Data Localization Laws and Policy, 2017 m., W. Kuan Hon, p. 71-73) Duomenų perdavimas į trečiąsias šalis apima duomenų prieinamumą, kaip numatyta BDAR 4 straipsnio 2 dalyje, taip pat duomenų tvarkymą, įskaitant duomenų tvarkymą duomenų valdytojui priklausančiuose serveriuose, esančiuose trečiojoje šalyje. Todėl duomenų perdavimas taip pat apima jų perdavimą duomenų valdytojui priklausančioje informacinių technologijų sistemoje, duomenis perduodant tarp duomenų valdytojo padalinių (skyrių, filialų, bendrų paslaugų centrų). Todėl akivaizdu, kad duomenų perdavimas į trečiąsias šalis taip pat laikomas duomenų perdavimu, kai duomenys perduodami tarp atskirų duomenų valdytojų, net jei jie priklauso tai pačiai įmonių grupei, taip pat kai duomenys perduodami duomenų tvarkytojui, kad jis juos tvarkytų duomenų valdytojo vardu, ir tais atvejais, kai duomenys pateikiami trečiųjų šalių valdžios institucijoms. Duomenų perdavimo taisyklės taikomos visoms perdavimo formoms, įskaitant asmens duomenų siuntimą el. paštu, prieigos prie klientų duomenų bazės suteikimą, keitimąsi duomenimis per specialią programą, duomenų perdavimą telefoninio pokalbio metu arba jų perdavimą popieriniuose dokumentuose ir pan. Trečiosios šalies subjekto nuotolinė prieiga prie EEE esančių duomenų taip pat laikoma duomenų perdavimu. Duomenys perduodami ne tik „duomenų gavėjams“, kaip apibrėžta BDAR 4 straipsnio 9 dalyje. Duomenų, perduodamų pagal BDAR 44 ir paskesnius straipsnius, importuotojas nėra duomenų gavėjo, kaip apibrėžta BDAR 4 straipsnio 9 dalyje, sinonimas. Į gavėjo apibrėžties taikymo sritį neįtrauktos „institucijos, kurios gali gauti duomenis vykdydamos konkretų tyrimą“. Tiesa nėra pagrindo daryti išvadą, kad duomenų perdavimas tokioms valdžios institucijoms esančioms trečiosiose šalyse nėra duomenų perdavimas, kaip apibrėžta BDAR 44-49 straipsniuose. Duomenų gavėjo statusas, kaip apibrėžta BDAR 4 straipsnio 9 dalyje, nėra duomenų perdavimą apibrėžiantis kriterijus. (GDPR: Personal Data Protection in the European Union; Mariusz Krzysztofek; 2021 m., p. 262-263).

2. Bendrieji duomenų perdavimo principai

Vertinant duomenų perdavimo už ES ribų teisėtumą taip pat labai svarbus ES garantuojamas pagrindinių teisių ir laisvių apsaugos lygis. Tolesnėje šio tyrimo eigoje vertinant tokio perdavimo reikalavimus reikėtų nepamiršti Europos apsaugos sistemos ir jos nuostatų. Kai asmens duomenys iškeliauja iš ES, kyla neriboto naudojimosi duomenimis rizika. Todėl asmens duomenis perduoti už ES ribų leidžiama tik laikantis konkrečių BDAR nustatytų reikalavimų. Siekdamos nustatyti, ar konkretus asmens duomenų perdavimas gavėjams trečiosiose šalyse yra teisėtas pagal BDAR, įmonės turi atlikti dviejų etapų priimtinumo patikrą. Pirmiausia reikia įsitikinti, kad planuojamas perdavimas atitinka bendruosius BDAR principus ir reikalavimus. Asmens duomenų perdavimas bet kuriai trečiajai šaliai pagal BDAR, nepriklausomai nuo jos buvimo vietos, patenka į duomenų tvarkymo sąvoką ir turi atitikti pagrindinius BDAR principus. Svarbiausia, kad asmens duomenų tvarkymas turi būti teisėtas ir pagrįstas vienu iš BDAR 6 straipsnyje nustatytų teisinių pagrindų. Antrasis žingsnis - patikrinti, ar laikomasi V skyriuje nurodytų konkrečių duomenų perdavimo reikalavimų. Bendrojo duomenų apsaugos reglamento 44 straipsniu siekiama „užtikrinti, kad nebūtų pakenkta reglamentu garantuojamam fizinių asmenų apsaugos lygiui“, kai asmens duomenys perduodami gavėjui už ES ribų. BDAR 44 straipsniu ribojamas asmens duomenų perdavimas į trečiąsias šalis ir leidžiamas tik tuo atveju, jei pateikiamas vienas iš trijų pakopų struktūros teisinių duomenų perdavimo už ES ribų pagrindų. Perduoti duomenis gavėjui trečiojoje šalyje leidžiama, jei gavėjas yra šalyje, dėl kurios Komisija priėmė sprendimą dėl tinkamumo (BDAR 45 straipsnis) (pagal I dalį). Jei tokio sprendimo dėl tinkamumo nėra, duomenų perdavimui taikomos tinkamos apsaugos priemonės (BDAR 46 straipsnis) (pagal II dalį). Jeigu sprendimo dėl tinkamumo ir tinkamų apsaugos priemonių nėra, taikomos BDAR nustatytos nukrypti leidžiančios nuostatos (BDAR 49 straipsnis) (pagal III dalį). Pažymėtina, kad BDAR 44 straipsnyje taip pat paaiškinta, kad konkretūs duomenų perdavimo už ES ribų reikalavimai taikomi tolesniam asmens duomenų perdavimui iš trečiosios šalies į kitą trečiąją šalį (The Transfer of Personal Data from the European Union to the United Kingdom post-Brexit, 2022 m., L. Wittershagen, p. 52-53).

2.1. Asmens duomenų perdavimas remiantis sprendimu dėl tinkamumo

BDAR 45 straipsnio 1 dalis nurodo, jog asmens duomenis trečiojoje šalyje esančiam gavėjui galima perduoti, jeigu Europos Komisija (toliau – Komisija) nusprendė, kad toje trečiojoje šalyje, teritorijoje arba viename ar keliuose konkrečiuose tos trečiosios šalies sektoriuose užtikrinamas tinkamas asmens duomenų apsaugos lygis. Būtent tokiais Komisijos (pagal BDAR 45 straipsnio 3 dalį priimtais) sprendimais dėl tinkamumo užtikrinamas aukščiausias apsaugos standartas perduodant asmens duomenis už Europos Sąjungos ribų. Priėmus sprendimą dėl tinkamumo, perduodant asmens duomenis į trečiąją šalį nereikia jokio papildomo leidimo. Šio sprendimo pagrindu perduodami asmens duomenys yra prilyginami duomenų perdavimui tarp ES narių, vadovaujantis joms tiesiogiai taikomomis BDAR nuostatomis. Tokiu būdu sudaromos sąlygos visiškai laisvam ir nevaržomam duomenų srautui iš ES į atitinkamą šalį (The Transfer of Personal Data from the European Union to the United Kingdom post-Brexit, L. Wittershagen; 2022 m., p. 53-54). Ar sprendimas dėl tinkamumo, ar tarptautinis susitarimas yra naudojamas kaip teisinis pagrindas duomenų perdavimui į kitą šalį priklauso nuo įvairių teisinių ir politinių veiksnių. Sprendimas dėl tinkamumo yra grindžiamas išsamesniu duomenų apsaugos standartų trečiosiose šalyse tyrimu, nei paprastai įmanoma derantis dėl tarptautinio susitarimo. Teisės aktų pakeitimai taip pat palengvino sprendimų dėl dalijimosi duomenimis tinkamumo priėmimą; pavyzdžiui, dabar Komisija taip pat gali priimti tokius sprendimus pagal Direktyvą (ES) 2016/680[4]. Tiesa Komisija nustatė, kad duomenų perdavimas tarptautinės prekybos kontekste turi būti įteisintas sprendimais dėl tinkamumo, o ne tarptautiniais susitarimais, nes taip siekiama išvengti galimų politinių ginčų. Tačiau tarptautinių susitarimų ir sprendimų dėl tinkamumo teisinis ryšys tebėra painus, kaip rodo vadinamasis „Skėtinis susitarimas“ (angl. Umbrella Agreement) tarp ES ir JAV susitarimas dėl asmeninės informacijos, susijusios su nusikalstamų veikų prevencija, tyrimu, nustatymu ir

[4] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR (toliau - Direktyva (ES) 2016/680).

patraukimu baudžiamojon atsakomybėn, apsaugos[5]. (The EU General Data Protection Regulation (GDPR): A Commentary 2020 m. C. Kuner, L. A Bygrave, C. Docksey, L. Drechsler; p. 777-778). Tarptautinės prekybos kontekste taip pat labai svarbus buvo 2000 m. liepos 26 d. Komisijos sprendimas 2000/520/EB dėl „Saugaus uosto" (angl. Safe Harbor) ir 2016 m. liepos 12 d. Europos Komisijos įgyvendinimo sprendimas (ES) 2016/1250, kuriuo deklaruojamas tinkamas duomenų apsaugos lygis pagal ES ir JAV privatumo skydo (angl. Privacy Shield) schemą. Šie sprendimai buvo vienas iš galimų teisinių pagrindų teisėtam asmens duomenų perdavimui iš ES į JAV (tačiau tai nebuvo vienintelis teisinis pagrindas, nes duomenų eksportuotojai galėjo ir tebegali naudotis BDAR 46-49 straipsniuose nurodymis priemonėmis). Subjektams, pateikusiems „Saugaus uosto" ir „Privatumo skydo" laikymosi deklaraciją ir atitinkantiems jų principus, Komisijos sprendimu buvo panaikinta kliūtis, atsiradusi dėl JAV kaip trečiosios šalies statuso. Šie sprendimai buvo taikomi konkretiems JAV importuotojams, o ne JAV kaip šaliai. Tačiau ESTT 2015 m. spalio 6 d. sprendimu byloje C-362/14 Maximilian Schrems prieš Duomenų apsaugos komisarą pripažino negaliojančiu Komisijos sprendimą 2000/520/EB („Saugaus uosto sprendimas"). Tiesa Privatumo skydo sprendimą, kuris vėliau buvo pakeitęs pripažintą negaliojančiu „Saugaus uosto" sprendimą kaip tarptautinio duomenų perdavimo teisinį pagrindą, ESTT taip pat pripažino negaliojančiu 2020 m. liepos 16 d. sprendimu byloje C-311/18 Duomenų apsaugos komisaras prieš Facebook Ireland ir Maximilian Schrems (Schrems II) (GDPR: Personal Data Protection in the European Union, Mariusz Krzysztofek, 2021 m., p. 266). Toliau pateikiama bendra informacija apie sprendimus dėl tinkamumo ir tinkamumo (priėmimo) procesą.

[5] Viena vertus, „Skėtiniame susitarime" teigiama, kad juo nesuteikiamas teisinis pagrindas duomenų perdavimui, kita vertus, skėtiniame susitarime taip pat skelbiama, kad pagal jį tvarkomi duomenys laikomi atitinkančiais teisės aktus, kuriais ribojamas tarptautinis duomenų perdavimas, todėl jis panašus į sprendimą dėl tinkamumo.

2.1.1. Sprendimų dėl tinkamumo priėmimo procedūra

45 straipsnyje kalbama apie oficialių Komisijos sprendimų dėl tinkamumo priėmimą. Tokie sprendimai yra įgyvendinimo aktai, priimami remiantis vadinamojo komitologijos reglamento[6] 5 straipsnyje nustatyta nagrinėjimo procedūra. Sprendimo dėl tinkamumo priėmimas ir derybos dėl jo paprastai prasideda tada, kai trečioji šalis kreipiasi į Komisiją ir prašo pradėti diskusijas. Komisijos ir trečiosios šalies derybos dėl tinkamumo paprastai trunka kelerius metus ir gali būti susijusios su politiniais veiksniais, dėl kurių gali kilti įtampa. Vykstant šiai procedūrai Komisija paprastai pati atlieka tyrimus dėl duomenų apsaugos tinkamumo trečiosiose šalyse, taip pat rengia akademinių ekspertų ataskaitas. Komisijos sprendimai dėl tinkamumo arba sprendimai, kuriais nustatoma, kad tinkamas apsaugos lygis užtikrinamas arba nebeužtikrinamas, turi būti skelbiami ES oficialiajame leidinyje. Prieš priimdama sprendimą dėl tinkamumo, Komisija privalo konsultuotis su Europos duomenų apsaugos valdyba (toliau – EDAV arba Valdyba). Komisija turi pateikti Valdybai visus susijusius dokumentus, įskaitant susirašinėjimą, išvadas ir Komisijos ataskaitą apie apsaugos lygį trečiojoje šalyje arba tarptautinėje organizacijoje. Tuomet EDAV turi pateikti savo nuomonę dėl Komisijos išvadų. Reikia pažymėti, jog tai, kad BDAR nėra minimi EDAV įgaliojimai patvirtinti Komisijos sprendimą, rodo, kad jos nuomonė nėra privaloma[7]. Sprendime dėl tinkamumo turi būti pateikta bent ši informacija:

1. Jame turi būti konkrečiai nurodyta, kad trečioji šalis arba tarptautinė organizacija užtikrina, tinkamą duomenų apsaugą pagal savo vidaus teisę arba tarptautinius įsipareigojimus (Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d. aprendimas *Schrems, 97 p*).

2. Jame turi būti nurodytas teritorinis ir sektorinis sprendimo taikymas (BDAR 45 straipsnio 3 dalis).

3. Jame turi būti numatytas periodinės sprendimo peržiūros mechanizmas (BDAR 45 straipsnio 3 dalis).

[6] 2011 m. vasario 16 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 182/2011, kuriuo nustatomos valstybių narių vykdomos Komisijos naudojimosi įgyvendinimo įgaliojimais kontrolės mechanizmų taisyklės ir bendrieji principai.

[7] Todėl Komisija patvirtino sprendimą dėl tinkamumo, apimantį Japonijos įstatymą dėl informacijos apie asmenis 2019 m., nepaisant to, kad EDAV nuomonėje dėl šio sprendimo (EDPB 2018) buvo pateikta tam tikra kritika.

4. Jame turi būti nurodyta priežiūros institucija ar institucijos, atsakingos už duomenų apsaugos taisyklių laikymosi užtikrinimą ir vykdymą (BDAR 45 straipsnio 2 dalies b punktas ir 3 dalis).

Be to, sprendimu dėl tinkamumo neturi būti ribojami Duomenų apsaugos institucijos (toliau – DAI) įgaliojimai tirti skundus dėl to, ar Komisijos sprendime dėl tinkamumo nustatytas apsaugos lygis atitinka pagrindines teises. Duomenų perdavimams pagal sprendimus dėl tinkamumo nereikia jokių papildomų DAI ar kitų institucijų leidimų. Sprendimai dėl tinkamumo gali būti priimami bet kurioje šalyje, kuri nėra ES valstybė narė ar EEE šalis. Tai reiškia, kad duomenų perdavimui į tris EEE šalis sprendimo dėl tinkamumo nereikia. Komisijos sprendimas dėl tinkamumo taikomas EEE šalyse, kai tik jis įtraukiamas į EEE jungtinio komiteto sprendimų sąrašą, kas buvo padaryta su esamais sprendimais (Japonija). Bendrasis duomenų apsaugos reglamentas buvo pažymėtas kaip EEE aktualus ir įtrauktas į EEE susitarimą. Taigi jis taip pat taikomos duomenų perdavimui iš Islandijos, Lichtenšteino ir Norvegijos (The EU General Data Protection Regulation (GDPR): A Commentary 2020 m. C. Kuner, L. A Bygrave, C. Docksey, L. Drechsler, p. 784-786).

Nors sprendimas dėl tinkamumo ir užtikrina teisėtą, Europos Sąjungos teisei prilygstančią duomenų apsaugą, tačiau autorės nuomone jis nėra be trūkumų. Tai, kad sprendimo priėmimas dėl ilgo jo priėmimo proceso gali užtrukti kelis metus apsunkina valstybėms galimybę perduoti duomenis „čia ir dabar“. Taip pat, vien faktas, jog sprendimas dėl tinkamumo yra priimtas tik kelių valstybių atžvilgiu parodo, jog tik kelios šalys gauna naudos iš sprendimo dėl tinkamumo[8]. Taip pat neramumą kelia ir tai, kad sprendimas dėl tinkamumo gali būti bet kada atšauktas. Nors ir yra priimtas sprendimas dėl tinkamumo Izraelio atžvilgiu, tačiau jis rizikuoja iškristi iš patvirtintų šalių sąrašo. Pirmus neramumus dėl duomenų apsaugos Izraelis sukėlė dar 2020 metais sukūrus naują technologiją, leidžiančią sudaryti koronaviruso plitimo žemėlapį sekant pacientų mobiliuosius duomenis[9]. Tačiau šiuo metu vykstančios teismų reformos Izraelyje gali ištikrūjų turėti realios įtakos 2011 m. priimtam ES sprendimui dėl Izraelio

[8] Europos Komisija iki šiol tinkama apsauga pripažino Andorą, Argentiną, Kanadą (komercinės organizacijos), Farerų salas, Gernsį, Izraelį, Meno salą, Japoniją, Džersį, Naująją Zelandiją, Korėjos Respubliką, Šveicariją, Jungtinę Karalystę pagal BDAR ir LED, Jungtines Amerikos Valstijas (komercinės organizacijos, dalyvaujančios ES ir JAV duomenų privatumo sistemoje) ir Urugvajų. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[9] https://www.independent.co.uk/news/world/middle-east/coronavirus-israel-cases-tracking-mobile-phone-nso-spyware-covid-19-a9410011.html

tinkamumo (https://iapp.org/news/a/potential-judicial-reforms-in-israel-could-impact-adequacy/). Dėl šių priežasčių šiuo metu sprendimas yra peržiūrimas ir keliamas klausimas ar Komisija mano, kad Izraelio siūlomos teismų reformos yra suderinamos su Izraelio siekiu ir toliau užtikrinti tinkamą privatumo apsaugos lygį? (https://www.europarl.europa.eu/doceo/document/E-9-2023-002290_EN.html#def2). Kol kas nėra aišku koks bus šių svarstymų rezultatas, tačiau tai, kad Izraelis kelia susirūpinimą dėl tinkamos duomenų apsaugos šalies viduje užtikrinimo yra pavyzdys, kad net jeigu ir Komisija yra priėmusi srpendimą dėl tinkamumo šalies atžvilgiu, dar nereiškia, jog toks sprendimas negali būti atšauktas. Tai kelia tam tikrą susirūpinimą, todėl, kad sustabdžius arba panaikimus tokį teisinį pagrindą perduoti duomenis į kitą šalį įvyktų tam tikra duomenų srautų stagnacija.

2.1.1. Tinkamumo kriterijai.

Vertinimas ir sprendimas dėl tinkamumo daugiausia grindžiami duomenų apsaugos užsienyje lygiu ir tuo, ar jis gali būti laikomas tinkamu, palyginti su Europos duomenų apsaugos teisės aktuose nustatytu apsaugos lygiu. Kriterijai, į kuriuos reikia atsižvelgti vertinant tinkamumą, nustatyti BDAR 45 straipsnio 2 dalyje:

„a) ar tai yra teisinė valstybė, ar joje užtikrinama pagarba žmogaus teisėms ir pagrindinėms laisvėms, ar įteisinti atitinkami bendrieji ir sektoriniai teisės aktai, įskaitant susijusius su viešuoju saugumu, gynyba, nacionaliniu saugumu ir baudžiamąja teise bei valdžios institucijų prieiga prie asmens duomenų, taip pat tokių teisės aktų įgyvendinimas, duomenų apsaugos taisyklės, profesinės taisyklės ir saugumo priemonės, įskaitant tolesnio asmens duomenų perdavimo kitai trečiajai šaliai ar tarptautinei organizacijai taisykles, kurių laikomasi toje šalyje ar tarptautinėje organizacijoje. Taip pat atsižvelgiama į teismų praktiką, taip pat veiksmingas

ir įgyvendinamas duomenų subjekto teises ir veiksmingą administracinę ir teisminę duomenų subjektų, kurių asmens duomenys perduodami, teisių gynybą;
(b) ar trečiojoje šalyje arba tarptautinėje organizacijoje egzistuoja ir veiksmingai veikia viena ar daugiau nepriklausomų priežiūros institucijų, atsakingų už duomenų apsaugos taisyklių laikymosi užtikrinimą ir vykdymą, įskaitant atitinkamus vykdymo užtikrinimo įgaliojimus, pagalbą ir konsultavimą duomenų subjektams naudojantis jų teisėmis ir bendradarbiavimą su valstybių narių priežiūros institucijomis; ir
(c) atsižvelgiama į atitinkamos trečiosios šalies ar tarptautinės organizacijos prisiimtus tarptautinius įsipareigojimus arba kitus įsipareigojimus, kylančius iš teisiškai privalomų konvencijų ar dokumentų, taip pat iš jos dalyvavimo daugiašalėse ar regioninėse sistemose, visų pirma susijusius su asmens duomenų apsauga.“

Iš šios formuluotės matyti, kad šis sąrašas nėra baigtinis ir jame pateikiama tik keletas nuorodų, kaip nustatyti, ar trečioji šalis užtikrina tinkamą duomenų apsaugos lygį. Tiesa BDAR 45 straipsnyje sąvoka „tinkamumas“ niekaip neapibrėžta ir nenustatyta, kokius standartus turi atitikti minėti kriterijai, kad būtų užtikrintas tinkamas apsaugos lygis (The Transfer of Personal Data from the European Union to the United Kingdom post-Brexit, 2022 m., L. Wittershagen, p. 59-61).

Tinkamas duomenų apsaugos lygis nereiškia, kad apsauga turi būti tiksliai tokia, kaip numatyta BDAR. Tai vienareikšmiškai užkirstų kelią bet kokiam duomenų perdavimui iš ES į ne EEE šalis (su keliomis išimtimis), nes ES asmens duomenų apsaugos modelis ir taikymo sritis yra unikalūs. Todėl BDAR numatytas „tinkamas“ duomenų apsaugos lygis turi būti suprantamas kaip „iš esmės lygiavertis“ Europos Sąjungos teisės lygiui. Apsauga neturi būti žemesnio lygio, nes neturi nukentėti BDAR garantuojama fizinių asmenų apsauga, kaip ji aiškinama atsižvelgiant į BDAR (44 straipsnis). BDAR 45 straipsnio 2 dalyje nustatytus kriterijus, pagal kuriuos vertinamas trečiųjų šalių užtikrinamas apsaugos lygis. 29 straipsnio darbo grupė išsamiau paaiškino savo darbiniuose dokumentuose šiuos kriterijus[10]. Šiuose dokumentuose 29 straipsnio darbo grupė remiasi ES asmens duomenų apsaugos principais kaip pagrindinėmis tinkamos apsaugos sąlygomis:

-tikslo ribojimo principas, pagal kurį duomenys gali būti tvarkomi tik tam tikrais tikslais ir negali būti toliau tvarkomi su tais tikslais nesuderinamu būdu.

[10] 1997 m. birželio 26 d. Nr. 4 dėl pirmųjų gairių dėl asmens duomenų perdavimo trečiosioms šalims ir 1997 m. birželio 24 d. Nr. dėl asmens duomenų perdavimo trečiosioms šalims pagal Direktyvos 25 ir 26 straipsnius.

-duomenų kokybės ir duomenų kiekio mažinimo (duomenų proporcingumo) principas, pagal kurį duomenys turėtų būti tikslūs, prireikus atnaujinami ir ne pertekliniai atsižvelgiant į duomenų perdavimo tikslus.

- skaidrumo principas, pagal kurį duomenų subjektams turėtų būti suteikta informacija, susijusi su jų asmens duomenų tvarkymo aspektais, visų pirma apie duomenų tvarkymo tikslą ir duomenų valdytojo trečiojoje šalyje tapatybę.

-saugumo principas, pagal kurį turėtų būti imamasi techninių ir organizacinių duomenų saugumo priemonių, atitinkančių duomenų tvarkymo keliamą riziką; bet koks duomenų tvarkymas duomenų valdytojo nurodymu turi atitikti duomenų tvarkytojui suteikto leidimo apimtį.

- teisė susipažinti su duomenimis, juos ištaisyti ir nesutikti (teisė prieštarauti), pagal kurią duomenų subjektas turėtų turėti teisę gauti informaciją apie jo tvarkomus duomenis, įskaitant duomenų kopiją, teisę reikalauti, kad tie duomenys būtų ištaisyti, jei jie yra netikslūs, ir tam tikrais atvejais teisę nesutikti, kad duomenys būtų tvarkomi.

- tolesnio duomenų perdavimo apribojimai, pagal kuriuos tolesnis asmens duomenų perdavimas trečiosios šalies subjektui turėtų būti leidžiamas tik tuo atveju, jei tolesnis subjektas taip pat privalo laikytis taisyklių, užtikrinančių tinkamą apsaugos lygį.

- principas, pagal kurį duomenų subjektams užtikrinama galimybė naudotis procedūriniais ir vykdymo užtikrinimo mechanizmais, leidžiančiais nepriklausomai nagrinėti jų skundus ir reikalauti tinkamos kompensacijos asmens duomenų tvarkymo principų pažeidimo atvejais; taip pat reikalaujama, kad būtų nepriklausoma priežiūros institucija, atsakinga už duomenų apsaugos teisės aktų laikymosi užtikrinimą, ir veiksmingos teisminės ir administracinės duomenų subjektų teisių vykdymo užtikrinimo procedūros (GDPR: Personal Data Protection in the European Union, Mariusz Krzysztofek, 2021 m., p. 267-268).

Problema gali kilti jeigu valstybė neužtiktina šių reikalavimų ir dėl šios priežasties sprendimas dėl tinkamumo nebus priimtas. Pavyzdžiui dar 2001 m. ES Komisija svarstė Australijos tinkamumo sprendimą. 29 straipsnio darbo grupė nustatė, kad kelios Australijos privatumo įstatymo sritys neatitinka tinkamumo standarto. Vėliau Australijos vyriausybė neperžiūrėjo Australijos duomenų apsaugos įstatymų, kad jie atitiktų reikalaujamą standartą (Art. 29 Data Protection Working Party, ‘Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000’ (2001) WP 40 final).

2.1.1. Sprendimo dėl tinkamumo panaikinimas, pakeitimas ar sustabdymas

45 straipsnyje pateikiamos išsamios nuostatos dėl situacijų, kai trečioji šalis, teritorija arba vienas ar daugiau konkrečių sektorių trečiojoje šalyje, arba tarptautinė organizacija nebeužtikrina tinkamo apsaugos lygio. Tokios situacijos gali susidaryti kai „informacija atskleidžia“, kad tinkama apsauga nebetaikoma (pvz., kai tokia informacija tampa žinoma iš pranešimų naujienų žiniasklaidoje). Tokiu atveju Komisija turi panaikinti, iš dalies pakeisti arba sustabdyti savo sprendimą dėl tinkamumo įgyvendinimo aktu, priimdama įgyvendinimo aktą pagal nagrinėjimo procedūrą 93 straipsnio 2 dalyje nurodytą procedūrą, išskyrus „tinkamai pagrįstus privalomus skubos atvejus“, kai Komisija turi priimti nedelsiant taikytinus įgyvendinimo aktus pagal 93 straipsnio 3 dalyje nurodytą procedūrą. 45 straipsnio 5 dalyje teigiama, kad Komisija „imasi“ tokių veiksmų, taigi ji turi pareigą tai daryti tokiose situacijose. Sprendimo dėl tinkamumo panaikinimas, pakeitimas ar sustabdymas neturi grįžtamosios galios, o tai yra nukrypimas nuo įprastos ES teisės, nes paprastai, kai ES teisės aktas yra panaikinamas, jis išnyksta iš ES teisinės tvarkos nuo tos dienos, kai įsigaliojo (ex tunc). Kai Komisija panaikina, iš dalies pakeičia arba sustabdo sprendimo dėl tinkamumo galiojimą, ji privalo pradėti konsultacijas su trečiąja šalimi arba tarptautine organizacija, kad ištaisytų padėtį. Toks sprendimas nepažeidžia asmens duomenų perdavimo, atliekamo pagal 46-49 straipsnius. Tai reiškia, kad net jei Komisija panaikina sprendimą dėl tinkamumo, duomenų perdavimui į paveiktą trečiąją šalį ar tarptautinę organizaciją, atliktam pagal tinkamas apsaugos priemones pagal 46 straipsnį, privalomas įmonių taisykles pagal 47 straipsnį arba nukrypti leidžiančias nuostatas pagal 49 straipsnį, tai neturi įtakos (GDPR): A Commentary 2020 m. C. Kuner, L. A Bygrave, C. Docksey, L. Drechsler, p. 789-790).

Taigi reikia pažymėti, jog tinkamo duomenų apsaugos lygio, užtikrinamo trečiojoje šalyje, įvertinimas yra labai sudėtingas procesas, kurio metu reikia atlikti išsamų tyrimą ir palyginti trečiojoje šalyje galiojančias taisykles ir praktiką su ES apsaugos standartais. Sprendimai dėl

tinkamumo nėra tik formalumas, o tinkamumo procesas nėra trivialus dalykas. Turi būti užtikrintas aukštas pagrindinių teisių apsaugos standartas, kuris turi būti griežtai vertinamas. Reikia nustatyti, ar įstatymas teoriškai atitinka duomenų subjekto tikrovę. Tinkamumo vertinimas turi apimti analizę, ar trečioji šalis turi veikiančią ir veiksmingą teisinę sistemą, leidžiančią kreiptis į teismą, jei teisė pažeidžiama.

2.1. Asmens duomenų perdavimas taikant tinkamas apsaugos priemones

Nesant sprendimo pagal BDAR 45 straipsnio 3 dalį, duomenų valdytojas arba duomenų tvarkytojas gali perduoti asmens duomenis į trečiąją šalį arba tarptautinei organizacijai tik tuo atveju, jei duomenų valdytojas arba duomenų tvarkytojas yra numatęs tinkamas apsaugos priemones ir su sąlyga, kad duomenų subjektai turi įgyvendinamas duomenų subjekto teises ir veiksmingas teisių gynimo priemones.

BDAR 46 straipsnio 1 dalyje nustatytų tinkamų apsaugos priemonių taikymo sritis yra siauresnė nei sprendimų dėl tinkamumo, jos susijusios tik su asmens duomenų perdavimu tarppartiniuose santykiuose ir yra pritaikytos konkretiems duomenų perdavimams ar jų rūšims. Duomenų valdytojai ir duomenų tvarkytojai gali įgyvendinti tinkamas apsaugos priemones, kad palengvintų duomenų perdavimą į trečiąją šalį pagal BDAR. Pagal BDAR 46 straipsnio 2 dalį tinkamos apsaugos priemonės, nereikalaujant priežiūros institucijos leidimo, gali būti tokios:

„a) teisiškai privalomas ir vykdytinas valdžios institucijų ar įstaigų tarpusavio dokumentas; b) privalomos įmonių taisyklės pagal BDAR 47 straipsnį; c) standartinės duomenų apsaugos sąlygos, kurias Komisija priėmė pagal BDAR 93 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą; d) standartinės duomenų apsaugos sąlygos, kurias priėmė priežiūros institucija ir patvirtino Komisija pagal BDAR 93 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą; (e) patvirtintas elgesio kodeksas pagal BDAR 40 straipsnį kartu su privalomais ir vykdytinais

duomenų valdytojo arba duomenų tvarkytojo įsipareigojimais trečiojoje šalyje taikyti tinkamas apsaugos priemones, įskaitant susijusias su duomenų subjektų teisėmis; arba f) patvirtintas sertifikavimo mechanizmas pagal BDAR 42 straipsnį kartu su privalomais ir vykdytinais duomenų valdytojo arba duomenų tvarkytojo įsipareigojimais trečiojoje šalyje taikyti tinkamas apsaugos priemones, įskaitant susijusias su duomenų subjektų teisėmis.“

Panaikinus reikalavimą apie kiekvieną duomenų perdavimą į trečiąją šalį iš anksto pranešti duomenų apsaugos institucijoms ir gauti specialų jų leidimą, grindžiamą tinkamomis apsaugos priemonėmis, buvo supaprastinta BDAR tinkamų apsaugos priemonių sistema. Kitos tinkamos apsaugos priemonės gali būti numatytos „a) duomenų valdytojo arba duomenų tvarkytojo ir duomenų valdytojo, duomenų tvarkytojo arba asmens duomenų gavėjo trečiojoje šalyje sutartinėse nuostatose; arba b) nuostatose, kurios turi būti įtrauktos į valdžios institucijų arba įstaigų administracinius susitarimus, kuriuose numatytos vykdytinos ir veiksmingos duomenų subjekto teisės“ - abiem atvejais reikalingas papildomas kompetentingos priežiūros institucijos leidimas. Toliau bus nagrinėjamos įvairios tinkamos apsaugos priemonės. Daugiausia dėmesio bus skiriama privalomoms įmonėms taikomoms taisyklėms ir standartinėms sutarčių sąlygoms, pastarosios yra populiariausia tinkama apsaugos priemonė (The Transfer of Personal Data from the European Union to the United Kingdom post-Brexit, 2022 m., L. Wittershagen, p. 269).

2.2.1 Standartinės sutarčių sąlygos

Pagrindinis principas - asmens duomenis perduoti į trečiąsias šalis, kurios Europos Komisijos sprendimu nebuvo pripažintos užtikrinančiomis tinkamą duomenų apsaugos standartą, leidžiama tik tuo atveju, jei duomenų eksportuotojas užtikrina, kad perdavus duomenis bus taikomos tinkamos apsaugos priemonės. Viena iš tokių apsaugos priemonių kategorijų yra standartinės duomenų apsaugos sąlygos (dar vadinamos standartinėmis sutarčių sąlygomis (SCC)), kurias priėmė Europos Komisija arba priėmė priežiūros institucija ir

patvirtino Europos Komisija (BDAR 46 straipsnio 2 dalies c ir d punktai). Tinkamas apsaugos lygis, t. y. lygiavertis ES lygiui, apima draudimą rinkti arba tvarkyti surinktus duomenis neteisėtu būdu. Pavyzdžiui, kai duomenys turi būti tvarkomi gavus duomenų subjekto sutikimą, toks sutikimas turi būti nedviprasmiškas ir duotas laisva valia, o atsisakymas nesukeltų jokių galimų neigiamų pasekmių. Standartinės sutarčių sąlygos yra pagrindas perduoti duomenis už įmonių grupės ribų (t. y. subjektams, kurie nepriklauso grupei, bet bendradarbiauja su grupės nariais; tai apima ir subjektus, kuriems duomenų tvarkymas perduotas išorės paslaugų teikėjams), priešingai nei įmonei privalomos taisyklės, kurios yra naudojamos įmonių grupėse. Dėl teisiškai privalomo pobūdžio, standartinėmis sutarčių sąlygomis užtikrinama tinkama duomenų apsauga po perdavimo, atitinkanti ES standartą, neatsižvelgiant į trečiosios šalies teisinį statusą, susijusį su duomenų apsauga, net ir tais atvejais, kai trečioji šalis neturi bendrųjų ar sektorinių teisės aktų, atitinkančių BDAR nustatytą standartą. Standartinės sąlygos naudojamos kaip sisteminio didelio kiekio duomenų perdavimo pagrindas. Tokiomis aplinkybėmis duomenų perdavimas, pavyzdžiui, gavus duomenų subjekto sutikimą, būtų nesuderinamas su BDAR, t. y. su principu, pagal kurį duomenys gali būti perduodami tik tuo atveju, jei užtikrinama tinkama jų apsauga. Be to, tai būtų nepraktiška ir neracionalu kaip sisteminė priemonė, atsižvelgiant į tai, kad sutikimas yra savanoriškas ir gali būti atšauktas. Naudotis šia priemone tokioms įstaigoms, kurios vykdydamos savo veiklą būtinai masiškai ir sistemingai perduoda asmens duomenis, Europos duomenų apsaugos valdyba rekomenduoja 2018 m. gegužės 25 d. Gairėse 2/2018 dėl 49 straipsnio nukrypti leidžiančių nuostatų pagal Reglamentą 2016/67958. Pagal BDAR standartinės duomenų apsaugos sąlygos, kaip Europos Komisijos priimtų arba priežiūros institucijos priimtų ir Komisijos patvirtintų sąlygų paketas, yra teisinis pagrindas perduoti duomenis į trečiąją šalį be atskiro priežiūros institucijos leidimo (GDPR: Personal Data Protection in the European Union, Mariusz Krzysztofek, 2021 m., p. 276-278)

Skiriami du skirtingi standartinių sąlygų tipai: Valstybės narės priežiūros institucijos priimtos ir ES Komisijos patvirtintos standartinės sąlygos (pagal BDAR 93 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą) ir valstybės narės priežiūros institucijos patvirtintos standartinės sąlygos (pagal BDAR 93 straipsnio 2 dalyje nurodytą nagrinėjimo procedūrą). Iki šiol pastaroji dar nėra priimta. ES Komisija, remdamasi Direktyvos 95/46 26 straipsnio 4 dalimi, yra priėmusi du skirtingus standartinių sutarčių sąlygų rinkinius: ES Komisija priėmė sprendimą dėl asmens duomenų perdavimo iš ES esančio duomenų valdytojo trečiojoje šalyje įsisteigusiam duomenų valdytojui (Sprendimas 2001/497/EB) ir Sprendimas 2004/915/EB. Be to, ES Komisija priėmė duomenų perdavimo iš duomenų valdytojų ES teritorijoje duomenų

tvarkytojams, esantiems trečiosiose šalyse, standartinių sutarčių sąlygų rinkinį (Sprendimas 2010/87/ES). Į kiekvieną standartinių sutarčių sąlygų rinkinį įtrauktos sąlygos, apibrėžiančios abipuses teises ir pareigas, įskaitant šalių atsakomybę, pareigą bendradarbiauti su priežiūros institucijomis, sutarties nutraukimo ir keitimo galimybes, taip pat apibrėžiančios teises, kurios turi būti suteiktos trečiosioms šalims pagal trečiųjų šalių naudos gavėjų The Transfer of Personal Data from the European Union to the United Kingdom post-Brexit, 2022 m., L. Wittershagen, p. 73-75). Tačiau standartinių sutarčių sąlygos turi būti naudojamos nepakeistos. Kartu su jomis turi būti leidžiami papildomi su verslu susiję terminai. Standartinių sutarčių sąlygos gali būti didesnės komercinės sutarties dalis. Tačiau parengti tokį projektą taip, kad būtų išvengta prieštaravimų, nėra paprasta. Kita problema yra tai, kad duomenų perdavimai gali būti laikomi negaliojančiais, jeigu paaiškėja, jog naudojamos „neteisingos“ standartinių sutarčių sąlygos (Data Localization Laws and Policy, 2017 m., W. Kuan Hon, p. 198-199)

2.2.2. Įmonei privalomos taisyklės

Įmonei privalomos taisyklės apibrėžiamos kaip „asmens duomenų apsaugos politika, kurios laikosi valstybės narės teritorijoje įsisteigęs duomenų valdytojas arba duomenų tvarkytojas, perduodamas asmens duomenis arba jų rinkinį duomenų valdytojui arba duomenų tvarkytojui vienoje ar keliose trečiosiose šalyse, priklausančiam įmonių grupei arba bendrą ekonominę veiklą vykdančių įmonių grupei“. Įmonei privalomos taisyklės taikomos atliekant duomenų perdavimus gavėjams įmonių grupės viduje. Sąvoka „įmonių grupė“ apibrėžiama kaip „kontroliuojančioji įmonė ir jos kontroliuojamos įmonės“. Sąvokos „įmonių, vykdančių bendrą ekonominę veiklą, grupė“ apibrėžties BDAR nėra. Tačiau sąvoka „įmonė“ apibrėžiama kaip „fizinis ar juridinis asmuo, vykdantis ekonominę veiklą, neatsižvelgiant į jo teisinę formą, įskaitant ūkines bendrijas ar asociacijas, reguliariai vykdančias ekonominę veiklą“. Taigi sąvoka „įmonių grupė, vykdanti bendrą ekonominę veiklą“ gali būti aiškinama kaip ne mažiau kaip dviejų fizinių ar juridinių asmenų grupė, nepriklausomai nuo to, ar jie yra susiję, ar ne,

kurie bendradarbiauja vykdydami ekonominę veiklą, tačiau nebūtinai priklauso tai pačiai įmonių grupei. Derybose dėl BDAR buvo sutarta, kad bendra ekonominė veikla turi būti stabili. Pavyzdžiui, į BDAR 47 straipsnio 1 dalies a punkto taikymo sritį nepateks neribotas subrangos sutarčių sudarymas su subtiekėjais, įtraukiant juos į įmonių bendradarbiavimą, kai ne kiekvienas santykis su subtiekėju būtų pakankamai stabilus. Įmonės, kurių tarpusavio ryšiai yra silpni, paprastai neatitinka BDAR 47 straipsnio 2 dalyje nurodytų privalomų reikalavimų. Duomenų perdavimas tarp skirtingų grupių, atskirai priėmusių BDAR, tikriausiai turės atitikti BDAR nustatytas tolesnio duomenų perdavimo sąlygas. Kompetentinga priežiūros institucija turi patvirtinti įmonei privalomos taisykles, taikydama BDAR 63 ir tolesniuose straipsniuose nustatytus nuoseklumo mechanizmus The Transfer of Personal Data from the European Union to the United Kingdom post-Brexit, 2022 m., L. Wittershagen p. 71-73)

Tačiau nors ir įmonei privalomos taisyklės yra lankstesnės nei standartinės sutarčių sąlygos, jų patvirtinimas užima daug laiko, nes užtrunka mėnesius ar net metus. Jų patvirtinimo procesas įtraukia daug vidaus padalinių ir išorės teisininkų keliose valstybėse narėse, taip pat pagrindines ir antrines DAI. Proceso metu taip pat renkami patvirtinimai ar paraiškos ir (arba) pranešimai iš valstybių narių. Taip pat įmonei privalomų taisyklių peržiūros ir atnaujinimai, kartais dažniau nei kartą per metus, didina administracinę naštą, pvz., kai nariai prisijungia arba išstoja; didelėse grupėse gali būti šimtai ar tūkstančiai narių. Todėl įmonei privalomos taisyklės yra brangus ir reikalaujantis daug priežiūros duomenų perdavimo būdas. Kai kurie duomenų valdytojai netgi paskiria darbuotojus, kuriems pavesta valdyti ir prižiūrėti šį mechanizmą. Dėl reikalingo laiko, sąnaudų ir žinių įmonei privalomų taisyklių mechanizmas iš esmės neprieinamas pradedančiosioms įmonėms (Data Localization Laws and Policy, 2017 m., W. Kuan Hon, p. 205-206).

2.2.3. Patvirtinti elgesio kodeksai ir sertifikavimo mechanizmai

Elgesio kodeksą gali rengti asociacijos arba kitos įstaigos, atstovaujančios tam tikrų kategorijų duomenų valdytojams arba duomenų tvarkytojams (vadinamiesiems kodų savininkams), pavyzdžiui, prekybos ir atstovų asociacijoms, sektorių organizacijoms, akademinėms organizacijoms ir interesų grupėms. Kompetentinga priežiūros institucija turi patvirtinti perdavimą ketinantį kompetencijos pažymėjimą. EDAV turi pateikti nuomonę dėl priežiūros institucijos sprendimo patvirtinti perkėlimui skirtą kodą projekto. Bendrajame duomenų apsaugos reglamente netgi numatyta galimybė ES Komisijai priimti įgyvendinimo aktą, kuriuo būtų nuspręsta, kad duomenų perdavimui skirtas kodeksas, kurį patvirtino priežiūros institucija, visuotinai galioja ES (The Transfer of Personal Data from the European Union to the United Kingdom post-Brexit, 2022 m., L. Wittershagen, p. 75-76).

Tačiau elgesio kodai ir (arba) sertifikatai, skirti debesijai, neatitiks BDAR tikslų, nebent bus oficialiai patvirtinti pagal BDAR nustatytus kriterijus ir procesus (kodams ir sertifikatams taikomi atskiri reikalavimai). Iš tiesų, DAI pabrėžė, kad kodeksuose ir (arba) sertifikatuose daugiausia dėmesio turi būti skiriama duomenų apsaugos įpareigojimams (ne tik saugumui), todėl daugelio galiojančių kodeksų ir (arba) sertifikatų gali nepakakti be esminių pakeitimų. Nors tiek kodeksų, tiek sertifikavimo atveju turi būti atsižvelgiama į „specifinius poreikius“, kodekso ir ypač sertifikavimo laikymasis vis tiek gali pareikalauti daug laiko ir išlaidų. Pavyzdžiui, Portugalijos buvimo vietos stebėjimo startuoliui „Movvo“ prireikė dvejų metų, kad gautų Vokietijos sertifikavimo organizacijos „EuroPriSe“ privatumo ženklą (Data Localization Laws and Policy, 2017 m., W. Kuan Hon, p. 211-212).

Svarbu atkreipti dėmesį, kad ESTT 2020 m. liepos 16 d. sprendimu byloje C-311/18 nustatė, kad, atsižvelgiant į padėtį vienoje ar kitoje trečiojoje valstybėje, duomenų valdytojui gali būti būtina imtis papildomų priemonių šio apsaugos lygio laikymuisi užtikrinti (Sprendimo 133 punktas). Be to, iš šio sprendimo matyti, kad vien BDAR 46 straipsnyje nustatyto asmens duomenų teikimo į trečiąsias valstybes įrankio, įskaitant standartinių sutarties sąlygų, pasirinkimas nėra savaime laikomas užtikrinančiu pakankamą ir tinkamą asmens duomenų apsaugą[11], todėl duomenų valdytojas arba duomenų tvarkytojas, visų pirma, kiekvienu atveju ir prireikus bendradarbiaudamas su duomenų gavėju, turi įvertinti, ar pagal paskirties trečiosios

[11] BDAR 46 straipsnyje įtvirtinti įrankiai, įskaitant standartines sutarčių sąlygas, neturėtų būti vertinami atskirai nuo kitų BDAR reikalavimų, pavyzdžiui, jie nepašalina pareigos sudaryti susitarimą pagal BDAR 28 straipsnį.

šalies teisę užtikrinama tinkama, atsižvelgiant į Europos Sąjungos teisę, asmens duomenų, perduodamų remiantis vienu iš BDAR 46 straipsnyje įtvirtintų asmens duomenų teikimo į trečiąsias valstybes įrankių, apsauga ir prireikus suteikiama papildomų garantijų (sprendimo 134 punktas). Tuo atveju, jei asmens duomenų teikimas būtų atliekamas nesilaikant BDAR V skyriuje nustatytų reikalavimų ir (ar) nesiėmus papildomų apsaugos priemonių, tokia asmens duomenų tvarkymo veikla galėtų būti vertinama kaip nesuderinama su BDAR.

EDAV rekomendacijose Nr. 01/2020 „Dėl priemonių asmens duomenų teikimo priemonėms papildyti, siekiant užtikrinti atitiktį Europos Sąjungos asmens duomenų apsaugos lygiui“ (toliau – Rekomendacijos) yra nustačiusi žingsnius, kurių turi laikytis bet kuris duomenų valdytojas (duomenų tvarkytojas), siekiantis įvertinti, kokios papildomos apsaugos priemonės turi būti taikomos perduodant asmens duomenis į tam tikrą trečiąją valstybę (pastebėtina ir tai, kad atlikus numatytus žingsnius gali paaiškėti, kad bet kurios papildomos apsaugos priemonės būtų nepakankamos ir tinkama asmens duomenų apsauga negalėtų būti užtikrinta). Minėtą vertinimą atlikti yra duomenų valdytojo pareiga, kuri kyla nepriklausomai nuo to, ar asmens duomenis siekiama perduoti duomenų valdytojui ar duomenų tvarkytojui, taip pat nuo to, kokiu įrankiu, įtvirtintu BDAR 46 straipsnyje, būtų vadovaujamasi.

Rekomendacijose pažymėta, kad „BDAR 46 straipsnyje nurodytos standartinės sutarčių sąlygos[12] ir kitos duomenų perdavimo priemonės neveikia vakuume. Teismas nurodo, kad duomenų valdytojai arba duomenų tvarkytojai, atliekantys duomenų eksportuotojų funkciją, kiekvienu konkrečiu atveju ir prireikus bendradarbiaudami su duomenų importuotoju trečiojoje valstybėje privalo patikrinti, ar trečiosios valstybės teisė ar praktika mažina BDAR 46 straipsnyje nurodytoms perdavimo priemonėms skirtų tinkamų apsaugos priemonių veiksmingumą. Tais atvejais Teismas vis tiek palieka duomenų eksportuotojams galimybę įgyvendinti papildomas priemones, kurios užpildo šias apsaugos spragas ir padidina apsaugos lygį iki reikalaujamo ES teisės aktais. Teismas nepatikslina, kokios priemonės tai galėtų būti. Tačiau Teismas pabrėžia, kad duomenų eksportuotojai turi jas nurodyti kiekvienu konkrečiu atveju. Tai atitinka BDAR 5 straipsnio 2 dalyje nustatytą atskaitomybės principą, pagal kurį duomenų valdytojai turi būti atsakingi už BDAR principų dėl asmens duomenų tvarkymo laikymąsi ir gebėti įrodyti, kad jų laikomasi.“

Taigi, „EDAV siekdama padėti duomenų eksportuotojams (nesvarbu, ar jie duomenų valdytojai, ar duomenų tvarkytojai, privatūs subjektai ar viešosios įstaigos, tvarkančios asmens duomenis BDAR taikymo srityje) atlikti sudėtingą užduotį – įvertinti trečiąsias valstybes ir

[12] Teismas taip pat patvirtina standartinių sutarčių sąlygų, kaip perdavimo priemonės, galinčios padėti užtikrinti iš esmės lygiavertį į trečiąsias valstybes perduodamų duomenų apsaugos lygį, tinkamumą.

prireikus nustatyti tinkamas papildomas priemones“, priėmė Rekomendacijas, kuriuose yra aptarusi kaip duomenų valdytojams, siekiantiems perduoti asmens duomenis į trečiąją valstybę, įvertinti, ar jų konkrečiu atveju reikalingos papildomos saugumo priemonės. Pabrėžtina, kad minėtą vertinimą atlikti yra duomenų valdytojo pareiga. Rekomendacijose pateikiami ir kai kurių saugumo priemonių pavyzdžiai, tačiau taip pat akcentuojama, kad nė viena iš šių priemonių nėra savarankiška ir pati savaime (netaikant kitų) nėra pakankama (https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf)
EDAV pažymi, kad, remiantis ESTT byla C-311/18, „perduodanti valdžios institucija ar įstaiga EEA, prireikus padedant priimančiajai valdžios institucijai ar įstaigai, turi įvertinti, ar trečiojoje šalyje laikomasi Europos Sąjungos teisės aktų reikalaujamo apsaugos lygio, siekiant nustatyti, ar praktikoje galima laikytis tarptautiniame susitarime[13] pateiktų apsaugos priemonių sąrašo, atsižvelgiant į galimą kišimąsi, kurį sukelia trečiųjų šalių teisės aktai, laikantis šių apsaugos priemonių. (EDAV gairių Nr. 2/2020, 13 punktas)

Taip pat, EDAV pažymi, kad siekiant užtikrinti Gairėse Nr. 2/2020 išvardytas duomenų apsaugos priemones, tarptautiniai susitarimai gali būti grindžiami jau esamais trečiosios šalies nacionalinės teisės elementais arba tarptautinėmis vidaus taisyklėmis / tarptautinės organizacijos reguliavimo sistema (EDAV priimtų Gairių Nr. 2/2020, 14 punktas).

2.2. Asmens duomenų perdavimas taikant nukrypti leidžiančias nuostatas

Pagal BDAR 49 str. 1d. asmens duomenų perdavimas trečiajai šaliai gali būti pateisinamas, net jei nėra tinkamo sprendimo ar apsaugos priemonių, pavyzdžiui, standartinių sutarčių sąlygų arba privalomų įmonių taisyklių, bet kuria iš šių aplinkybių:

[13] Tarptautiniame susitarimo sąvoka apima: teisiškai privalomas ir vykdytinu valdžios institucijų arba įstaigų tarpusavio dokumentas ar administracinis susitarimas.

„a) duomenų subjektas aiškiai sutiko su siūlomu duomenų perdavimu po to, kai buvo informuotas apie galimus tokių perdavimų pavojus duomenų subjektui dėl to, kad nepriimtas sprendimas dėl tinkamumo ir nenustatytos tinkamos apsaugos priemonės;

b) duomenų perdavimas yra būtinas duomenų subjekto ir duomenų valdytojo sutarčiai vykdyti arba ikisutartinėms priemonėms, kurių imtasi duomenų subjekto prašymu, įgyvendinti;

c) duomenų perdavimas yra būtinas, kad būtų sudaryta arba įvykdyta duomenų subjekto interesais sudaroma duomenų valdytojo ir kito fizinio ar juridinio asmens sutartis;

d) duomenų perdavimas yra būtinas dėl svarbių viešojo intereso priežasčių;

e) duomenų perdavimas yra būtinas siekiant pareikšti, vykdyti ar ginti teisinius reikalavimus;

f) duomenų perdavimas yra būtinas, kad būtų apsaugoti gyvybiniai duomenų subjekto arba kitų asmenų interesai, jeigu duomenų subjektas dėl fizinių ar teisinių priežasčių negali duoti sutikimo;

g) duomenys perduodami iš registro, pagal Sąjungos arba valstybės narės teisę skirto teikti informaciją visuomenei, su kuria gali susipažinti plačioji visuomenė arba bet kuris asmuo, galintis įrodyti teisėtą interesą, tačiau tik tiek, kiek konkrečiu atveju laikomasi pagal Sąjungos arba valstybės narės teisę nustatytų susipažinimo su tokiame registre esančia informacija sąlygų. “

Kai netaikoma nė viena iš šių sąlygų ir kai duomenų perdavimas negali būti grindžiamas sprendimu dėl tinkamumo arba tinkamomis apsaugos priemonėmis, perdavimas gali būti atliekamas tik tada, kai jis nėra pasikartojantis, susijęs su ribotu duomenų subjektų skaičiumi ir yra būtinas siekiant Duomenų valdytojo įtikinamų teisėtų interesų, jei duomenų subjekto teisės nėra viršesnės už juos. Tokiais atvejais duomenų valdytojas turi įvertinti perdavimo aplinkybes ir numatyti apsaugos priemones. Jis taip pat turi informuoti priežiūros instituciją ir paveiktus duomenų subjektus apie perdavimą ir jį pateisinantį teisėtą interesą. Tai, kad leidžiančios nukrypti nuostatos yra paskutinė teisėto perdavimo priemonė (naudojamos tik nesant sprendimo dėl tinkamumo ir jei nėra kitų apsaugos priemonių), pabrėžia jų išskirtinį pobūdį ir dar labiau pabrėžiama BDAR konstatuojamosiose dalyse. Taigi leidžiančios nukrypti nuostatos yra priimamos kaip galimybė „perdavimui tam tikromis aplinkybėmis“ remiantis sutikimu ir kai „perdavimas yra atsitiktinis ir būtinas“ dėl sutarties ar teisinio reikalavimo. Be to, remiantis 29 straipsnio darbo grupės gairėmis, nukrypti leidžiančios nuostatos konkrečiose situacijose turi būti išimtinės, pagrįstos atskirais atvejais ir negali būti naudojamos masiniam ar pasikartojančiam perdavimui. Europos duomenų apsaugos priežiūros pareigūnas taip pat pabrėžė išskirtinį pobūdį nukrypti leidžiančių nuostatų, naudojamų kaip teisinių perdavimų

pagrindą pagal Reglamentą Nr. 45/2001, pažymint, kad šis sprendimas turėtų būti naudojamas „ribotais atvejais“ ir „retkarčiais perdavimams“. Jei nėra priimtas sprendimas dėl tinkamumo, ES arba jos valstybės narės yra įgaliotos dėl svarbių viešųjų interesų priežasčių nustatyti konkrečių kategorijų asmens duomenų perdavimo trečiajai šaliai apribojimus, nepaisant to, kad tenkinamos kitos tokio perdavimo sąlygos. Šios ribos turėtų būti laikomos išskirtinėmis, o valstybės narės privalo pranešti apie atitinkamas nuostatas Komisijai (Europos duomenų apsaugos teisės vadovas, 2018, p. 271-273).

2.1. Sutikimas.

Pagal BDAR 49 straipsnio 1 dalies a punktą asmens duomenis leidžiama perduoti į trečiąją šalį, jei duomenų subjektas aiškiai duoda sutikimą siūlomam duomenų perdavimui į trečiąją šalį po to, kai jis buvo informuotas apie galimą tokio perdavimo riziką, kuri gali kilti dėl to, kad nėra sprendimo dėl tinkamumo ir tinkamų apsaugos priemonių. Apskritai turi būti paisoma duomenų subjekto valios, jei jis sąmoningai nusprendžia siųsti savo duomenis į trečiąją šalį, kurioje nėra tinkamų duomenų apsaugos teisės aktų. BDAR 49 straipsnio 1 dalies a punktas yra dar griežtesnis nei BDAR 6 straipsnio 1 dalies a punktas ir, kaip ir BDAR 9 straipsnio 1 dalies a punktas (sutikimas dėl specialių kategorijų asmens duomenų), reikalauja aiškaus sutikimo, išskyrus bet kokią numanomo sutikimo formą. Bendro sutikimo nepakanka. Taikomi bendrieji BDAR 7 straipsnio reikalavimai. Pagal BDAR 49 straipsnio 1 dalies a punktą, prieš duodamas aiškų sutikimą, duomenų subjektas iš pradžių turi būti informuotas apie sprendimo dėl tinkamumo ir tinkamų apsaugos priemonių nebuvimą, taip pat apie galimą tokio duomenų perdavimo riziką duomenų subjektui, kylančią dėl sprendimo dėl tinkamumo ir tinkamų apsaugos priemonių nebuvimo. Neaišku, kokio išsamumo informacija apie riziką pateikta duomenų subjektui. Kai kurie autoriai teigia, kad numatomas duomenų naudojimas ir duomenų rinkimo bei tvarkymo praktika trečiojoje šalyje turi būti aprašyti taip išsamiai, kad duomenų subjektas žinotų apie galimas pasekmes, susijusias su jo duomenų perdavimu į šalį, kurioje taikomas kitoks apsaugos lygis. Galima su tuo sutikti, nes pagal BDAR 49 straipsnio 1 dalies

a punktą perduodant asmens duomenis apskritai neturėtų būti pakenkta Europos teisės garantuojamam apsaugos lygiui. Reikėtų išsamesnės informacijos, įskaitant informaciją apie konkrečius pavojus, kylančius dėl konkretaus asmens duomenų naudojimo, leidžiamo pagal konkrečios trečiosios šalies nacionalinius teisės aktus, taip pat apie BDAR teikiamos apsaugos trūkumą (The Transfer of Personal Data from the European Union to the United Kingdom post-Brexit, 2022 m., L. Wittershagen, p. 78-79).

Tiesa vienkartinio duomenų perdavimo atveju 29 darbo grupė[14] mano, kad duomenų subjektas gali duoti konkretų sutikimą „konkrečiam duomenų perdavimui arba konkrečiai duomenų perdavimo kategorijai“. Tačiau „pakartotinių ar struktūrinių“ perdavimų atveju sutikimas negali būti tinkama praktinė ilgalaikė duomenų perdavimo sistema (Darbo grupės nuomonės 11 psl). 29 darbo grupėje taip pat nepritariama sutikimui dėl perdavimo, kai šalys turi nevienodą derybinę galią; pavyzdžiui, darbuotojų sutikimas darbdaviams gali neatspindėti “laisvo” pasirinkimo (48 darbo grupė, p. 3). Be to, kad sutikimas būtų “laisvas”, jis turi būti atšaukiamas. Bet kokia abejonė dėl sutikimo nedviprasmiškumo taip pat gali lemti, kad išimtis nebus taikoma (p. 24). Kiti praktiniai sunkumai susiję su tuo, kad sutikimas turi būti duotas prieš duomenų perdavimą, o tam, kad išankstinis sutikimas galiotų, informacija apie būsimą duomenų perdavimą turi būti “iš anksto nustatyta, visų pirma kalbant apie tikslą ir gavėjų kategorijas”, ir apie tai turi būti pranešta, taip pat su sąlyga, kad sutikimas gali būti bet kada atšauktas. Todėl, nors renkant asmens duomenis internetu “sutikimo” būtų galima prašyti naudojant interneto svetainės formas, reguliariai ar pakartotinai perduodant duomenis komerciniuose santykiuose (pvz., naudojant debesiją) duomenų valdytojams saugesnis atrodo kitas nei sutikimas pagrindas. Be to, kai organizacijos naudoja debesiją savo individualių klientų duomenims tvarkyti pvz., užsakymams, reikalingas duomenų subjektų, kurie yra organizacijos klientai, sutikimas. Taigi, tvarkant asmens duomenis debesijos režimu, gali būti sunku gauti duomenų subjektų sutikimus ir įrodyti, kad jie buvo duoti laisva valia (konkretūs, informuoti ir nedviprasmiški). Dėl praktinių sunkumų, susijusių su sutikimų valdymu, ir dėl neigiamo DAI požiūrio į sutikimo naudojimą duomenų perdavimui, daugelis duomenų valdytojų gali rinktis mechanizmus, ypač susijusius su žmogiškųjų išteklių duomenimis (Data Localization Laws and Policy, 2017 m., W. Kuan Hon, p. 213-214).

[14] Article 29 Working Party, Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995.

3. Asmens duomenų perdavimo į trečiąsias šalis problematika didžiųjų pasaulio valstybių atžvilgiu

3.1. Duomenų perdavimas į Kiniją

Analizuojant duomenų perdavimąį trčiasias valstybes galima iškarto pastebėti, jog Europos Sąjunga daugiau dėmesio yra skyrusi ES ir JAV tarptautiniam duomenų perdavimui. Sprendimai Schrems[15] ir Schrems II[16] yra kertiniai sprendimai, kuriuose buvo nagrinėjamas asmens duomenų perdavimas iš ES į JAV ir pripažįstami negaliojančiais su tokiu perdavimu susiję sprendimai dėl tinkamumo. Priėmus sprendimą Schrems II, ES pradėjo sprendimo dėl naujos ES ir JAV duomenų privatumo sistemos tinkamumo priėmimo procesą. Tačiau panašu, kad Kinijai dėl duomenų perdavimo ES skiria mažiau dėmesio. Jungtinės Valstijos ir Kinija yra dvi šalys, kurios išsiskiria savo gebėjimu įsitraukti į duomenimis grindžiamą ekonomiką ir gauti iš jos naudos. Be to, Kinija yra svarbi ES prekybos partnerė[17]. Būtent dėl šių aplinkybių būtina užtikrinti didesnį teisinį tikrumą tarp ES ir Kinijos. (Processing of Personal Data by Public Authorities in China: Assessing Equivalence for Cross-border Transfers from the EU to China; Yueming Zhang, 2023). Kodėl tiek daug dėmesio yra skiriama JAV? Greičiausiai todėl, kad duomenų rinkos ekonomikoje jau daugelį metų dominuoja būtent JAV didžiųjų technologijų bendrovės, kurios atitinkamai sulaukė daug dėmesio. (Assessing the Implications of Schrems II for EU-US Data Flow, M. H. Murphy, 2021) Tačiau Kinijos interneto svetainių ir taikomųjų programų išpopuliarėjimas pasaulyje iš esmės leidžia suprasti, jog Kinijos produktų vartojimas tik kyla. Pavyzdžiui „TikTok“ yra pasaulinė programėlė, turinti antrą pagal dydį atsisiuntimų skaičių pasaulyje

[15] Europos Sąjungos Teisingumo Teismo 2015 m. spalio 6 d sprendimas Schrems
[16] Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas Schrems II
[17] EU Trade Relations with China' (The European Commission) (https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/china_en.)

(https://www.forbes.com/sites/johnkoetsier/2022/03/23/top-apps-of-2022-by-installs-spend-and-active-users-report/?sh=4ede0683d3ac)

Nepaisant to, nėra priimtas sprendimas dėl tinkamumo Kinijos atžvilgiu ir todėl naudojimasis Kinijos produktais ir tokiu būdų duomenų perdavimas iš ES taip pat kelia didelių neramumų. Tai įrodo ir 2021 m. Nyderlandų duomenų priežiūros institucijos skirta bauda Kinijos bendrovei "TikTok" už privatumo pažeidimus, susijusius su vaikais (https://edpb.europa.eu/news/national-news/2021/dutch-dpa-tiktok-fined-violating-childrens-privacy_en). Taigi galima suprasti, jog duomenų perdavimas iš ES į Kiniją išlieka vis dar keblus. Kol nėra priimtas sprendimas dėl tinkamumo Kinijos atžvilgiu nėra iki galo aišku, kaip reikėtų tinkamai apsaugoti ES piliečių duomenis. Kol kas, ES valstybės greičiausiai turės susilaikyti nuo duomenų perdavimo į Kiniją, o jeigu tai neįmanoma, pabandyti užtikrinti duomenų apsaugą kitomis apsaugos priemonėmis. Bet kokiu atveju, jau dabar galima pastebėti, jog Europos Sąjunga po truputį pradeda svarstymus dėl šių problemų (https://www.reuters.com/world/china/european-firms-urge-china-give-more-clarity-data-transfer-laws-2023-11-15/) .

3.1. Duomenų perdavimas į Jungtinę Karalystę po "Brexit"

2020 m. vasario 1 d. Jungtinė Karalystė ir Šiaurės Airijos Karalystė (toliau - JK) išstojo iš Europos Sąjungos ir Europos atominės energijos bendrijos. Dėl šios priežasties JK prilyginama trečiajai valstybei. 2021 m. sausio 1 d., pasibaigus pereinamajam laikotarpiui, įsigaliojo Prekybos ir bendradarbiavimo susitarimas tarp Europos Sąjungos ir Europos Atominės Energijos Bendrijos ir Jungtinės Didžiosios Britanijos ir Šiaurės Airijos Karalystės (Susitarimas), pagal kurį asmens duomenų perdavimas nebuvo laikomas perdavimu į trečiąją valstybę, kol Europos Komisija priims sprendimą dėl tinkamumo JK atžvilgiu arba kol pasibaigs keturių mėnesių terminas (su galimybe pratęsti dar dviem mėnesiams) nuo Susitarimo įsigaliojimo dienos. 2021 m. birželio 28 d. Europos Komisija priėmė sprendimus dėl tinkamumo JK atžvilgiu:

1. Komisijos įgyvendinimo sprendimą pagal Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 dėl tinkamos asmens duomenų apsaugos Jungtinėje Karalystėje;

2. Komisijos įgyvendinimo sprendimą pagal Europos Parlamento ir Tarybos direktyvą (ES) 2016/680 dėl tinkamos asmens duomenų apsaugos Jungtinėje Karalystėje.

Šie tinkamumo sprendimai užtikrina laisvą asmens duomenų perdavimą iš Europos Sąjungos į JK, nereikalaujant jokių papildomų leidimų asmens duomenų perdavimui. Sprendimais dėl tinkamumo laikoma, kad perduodamų asmens duomenų apsaugos lygis atitinka Bendrajame duomenų apsaugos reglamente ir Direktyvoje (ES) 2016/680 įtvirtintą asmens duomenų apsaugos lygį. (https://vdai.lrv.lt/uploads/vdai/documents/files/17%20DUK%20BREXIT%20atnaujinta_2021-07.pdf)

Pagal 2021 m. birželį Europos Komisijos priimtą sprendimą dėl tinkamumo pagal ES BDAR Jungtinė Karalystė yra laikoma„ tinkama“ valstybė duomenų perdavimo pagal BDAR standartus atžvilgiu.. Tačiau JK yra vienintelė valstybė, kurios sprendimui dėl tinkamumo taikoma „galiojimo“ sąlyga - JK sprendimas dėl tinkamumo automatiškai nustos galioti 2025 m. birželio 27 d., jei iki to laiko nebus atnaujintas kitu Komisijos sprendimu. Šiuo metu

Komisija peržiūri kitų šalių galiojančius sprendimus dėl tinkamumo, o rezultatus tikimasi paskelbti 2022 m. pabaigoje. Tačiau tie kiti sprendimai lieka galioti, nebent jie būtų nutraukti.

Taip pat ES Komisija turi nuolat stebėti pokyčius Jungtinėje Karalystėje, kad užtikrintų, jog Jungtinė Karalystė ir toliau užtikrintų lygiavertę duomenų apsaugą. Komisija gali iš dalies pakeisti, sustabdyti arba panaikinti sprendimus, jei nepavyksta išspręsti problemų. Be to, ES duomenų subjektai arba ES duomenų apsaugos institucija gali inicijuoti teisinį ginčą dėl sprendimų. Tuomet Europos Sąjungos Teisingumo Teismas turėtų nuspręsti, ar Jungtinė Karalystė iš esmės užtikrina lygiavertę apsaugą. (https://ico.org.uk/media/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail-1-0.pdf)

Taigi šie sprendimai dėl tinkamumo reiškia, kad duomenų perdavimo srautai tarp ES ir Jungtinės Karlystės gali būti tęsiami ir nereikia priimti papildomų apsaugos priemonių. Tačiau jeigu ES sprendimai dėl tinkamumo būtų peržiūrėti arba panaikinti, visi, perduodantys asmens duomenis iš ES / EEE į JK, tai darytų trečiosios šalies pagrindu. Įmonėms reikėtų įdiegti vieną iš papildomų apsaugos priemonių, nustatytų BDAR 46 straipsnyje arba BDAR 49 straipsnyje išvardintomis nukrypti leidžiančiomis nuostatomis.

Dėl aiškumo Jungtinės Karalystės Informacijos komisaro biuras (toliau – Komisaro biuras) pateikia gaires JK įmonėms, kurios gauna duomenis iš ES ir EEE šalių arba turi savo padalinių jose. Gairėse labai trumpai ir paprastai apžvelgiami duomenų apsaugos pokyčiai po JK išstojimo iš Europos Sąjungos. Komisaro biuras taip pat paskelbė „interaktyvią priemonę“, skirtą JK įmonėms, kurios gauna asmens duomenis į Jungtinę Karalystę iš Ekonominės zonos, kad nebūtų sutrukdomas duomenų srautas iš EEE į JK. Šia priemone siekiama padėti įmonėms nustatyti, ar duomenų srautui palaikyti yra reikalingos standartinės sutarties sąlygos, taip pat padeda pasirinkti tinkamas standartines sutarties sąlygas, jas suprasti ir užpildyti. Ši priemonė taip pat padeda įmonėms išsiaiškinti, ar jos naudoja ES įsikūrusius paslaugų teikėjus savo duomenims tvarkyti ir kokiu mastu. Pažymėtina, kad daugelis JK įmonių patenka į BDAR ekstrateritorinę taikymo sritį. Pagal BDAR 3 straipsnio 2 dalį Europos duomenų apsaugos teisės aktų taikymo sritis išplečiama ir apima visą ES neįsisteigusių įmonių verslo veiklą, susijusią su bet kokiu su vidaus rinka susijusiu asmens duomenų tvarkymu. Tokiais atvejais JK įmonės privalo laikytis BDAR. Praktiškai patartina laikytis BDAR nuostatų, net jei 2018 m. duomenų apsaugos institucija numato kokių nors nukrypimų nuo jo. Šiuo metu Jungtinėje Karalystėje toliau galioja senosios ES standartinių sutartčių sąlygos. Vis dėlto Komisaro biuras konsultavosi dėl alternatyvios duomenų perdavimo priemonės, kuri reglamentuotų asmens duomenų perdavimą iš JK į trečiąsias šalis. Komisaro biuras taip pat svarsto galimybę įvesti

alternatyvų ginčų sprendimo mechanizmą (arbitražo mechanizmą). Komisaro biuras taip pat paskelbė naujųjų ES standartinių sutartčių sąlygų papildymą, kad organizacijos galėtų pritaikyti ES standartinių sutartčių sąlygas. Be to, 2021 m. rugpjūtį Komisaro biuras paskelbė duomenų perdavimo rizikos vertinimo projektą[18], kuriame nustatytos priemonės, skirtos įvertinti riziką, susijusią su perdavimu į trečiąsias šalis, siekiant nustatyti, ar galima pasikliauti atitinkamu duomenų perdavimo mechanizmu. Šis projektas yra labai panašus į Europos duomenų apsaugos valdybos gaires dėl papildomų priemonių. Jei duomenų eksportuotojas abejoja dėl galimo duomenų perdavimo riziko, jis turi atlikti papildomą rizikos vertinimą, kuriame apsvarstytų galimą žalą duomenų subjektams ir rizikos mažinimo būdus. Komisaro biuras pateikia išsamias šio papildomo vertinimo gaires. Įdomu tai, jog Komisaro biuras ragina duomenų eksportuotoją atlikti duomenų perdavimą, net jei duomenų subjektams kiltų minimali arba net didesnė nei minimali rizika, o žalos rizika būtų nedidelė. Taigi, įvertinus visa tai, galima daryti išvadą, jog nepaisaint sudėtingos Jungtinės Karalystės situacijos, išstojimas iš Europos Sąjungos, nors ir kelia keblumų, tačiau neužkerta kelio asmens duomenų judėjimo tarp jos ir EU (The Transfer of Personal Data from the European Union to the United Kingdom post-Brexit; Leonie Wittershagen; 2022, Puslapis 279-282).

[18] ICO, 'Draft International Transfer Risk Assessment and Tool' (August 2021) https://ico. org.uk/media/about-the-ico/consultations/2620397/intl-transfer-risk-assessment-tool-20210804. pdf

3.2. Duomenų perdavimas į Rusiją

Nuo 2022 m. vasario 24 d. Rusijos Federacija (toliau - Rusija) yra faktinėje karo prieš Ukrainą būsenoje. Todėl 2022 m. kovo 16 d. ji buvo pašalinta iš Europos Tarybos. Todėl Rusija nebėra susitariančioji šalis tų Europos Taryboje sudarytų konvencijų ir protokolų, kurie yra atviri tik jos valstybėms narėms. Nuo 2022 m. rugsėjo 16 d. ji taip pat nustojo būti Europos žmogaus teisių konvencijos Aukštoji Susitariančioji Šalis.

Europos duomenų apsaugos valdyba primena, kad asmens duomenų perdavimas į trečiąją šalį, nesant Europos Komisijos sprendimo dėl tinkamumo pagal BDAR 45 straipsnį, galimas tik tuo atveju, jei duomenų valdytojas arba duomenų tvarkytojas yra numatęs tinkamas apsaugos priemones ir jei duomenų subjektai turi įgyvendinamas teises ir veiksmingas teisių gynimo priemones (BDAR 46 straipsnis). Jei nėra sprendimo dėl tinkamumo pagal BDAR 45 straipsnio 3 dalį arba tinkamų apsaugos priemonių pagal BDAR 46 straipsnį, konkrečiomis aplinkybėmis asmens duomenys į trečiąją šalį perduodami arba jų rinkinys perduodamas tik esant vienai iš sąlygų, nustatytų BDAR 49 straipsnyje („konkrečioms situacijoms taikomos nukrypti leidžiančios nuostatos“).

Rusija nėra gavusi Europos Komisijos išvados dėl tinkamumo pagal BDAR 45 straipsnį. Todėl asmens duomenys į Rusiją turi būti perduodami naudojant vieną iš kitų BDAR V skyriuje nurodytų alternatyvių duomenų perdavimo priemonių. Atsižvelgdama į tai, EDAV pažymi, kad kai asmens duomenys perduodami į Rusiją, duomenų eksportuotojai pagal BDAR turėtų įvertinti ir nustatyti duomenų perdavimo teisinį pagrindą ir priemonę, kuri bus naudojama iš tų, kurios numatytos BDAR V skyriuje (pvz., standartinės sutarčių sąlygos arba privalomos įmonių taisyklės), kad būtų užtikrintas tinkamų apsaugos priemonių taikymas.

Be to, EDAV primena, kad po sprendimo Schrems II ir pagal EDAV rekomendacijas dėl papildomų priemonių duomenų eksportuotojai turėtų įvertinti, ar, atsižvelgiant į nagrinėjamą duomenų perdavimą, Rusijoje galiojančiuose teisės aktuose ir (arba) praktikoje (visų pirma susijusioje su Rusijos valdžios institucijų prieiga prie asmens duomenų, ypač baudžiamosios teisėsaugos ir nacionalinio saugumo tikslais) yra kas nors, kas gali turėti įtakos nustatytų perdavimo priemonių tinkamų apsaugos priemonių veiksmingumui. Tokiu atveju duomenų

eksportuotojai turėtų nustatyti ir patvirtinti papildomas priemones, kurios yra būtinos siekiant užtikrinti, kad duomenų subjektams būtų suteiktas iš esmės lygiavertis apsaugos lygis, koks užtikrinamas Europos ekoniminėje zonoje. Jeigu atlikus tokį vertinimą padaroma išvada, kad atitiktis neužtikrinama (arba nebeužtikrinama) ir kad negalima nustatyti jokių papildomų priemonių, duomenų eksportuotojai turi sustabdyti duomenų perdavimą. Kelios EEE valstybės narės vis dar palaiko glaudžius ekonominius ir istorinius ryšius su Rusija, todėl šios šalys vis dar dažnai keičiasi asmens duomenimis su Rusija. Kai kurios nacionalinės duomenų apsaugos priežiūros institucijos jau nagrinėja duomenų perdavimo į Rusiją teisėtumą, įskaitant atliekamus tyrimus. Priežiūros institucijos ir toliau stebės teisės aktų pakeitimus ir kitus svarbius pokyčius Rusijoje, kurie gali turėti įtakos duomenų perdavimui. Jos nagrinės bylas, susijusias su duomenų perdavimu į Rusiją, atsižvelgdamos į padidėjusį poveikį duomenų subjektų teisėms ir laisvėms, kuris gali atsirasti dėl tokių duomenų tvarkymo operacijų, ir prireikus koordinuos veiksmus EDAV (https://edpb.europa.eu/system/files/2022-07/edpb_statement_20220712_transferstorussia_en.pdf).

Pvyzdžiui visai neseniai Suomijos duomenų apsaugos institucija laikinai uždraudė „Yango taksi“ tarnybai perduoti asmens duomenis iš Suomijos į Rusiją. Suomijos duomenų apsaugos institucija sužinojo apie rugsėjo pradžioje Rusijoje įsigaliosiančią įstatymų reformą, pagal kurią Rusijos Federacijos saugumo tarnybos turės teisę gauti taksi operacijų metu tvarkomus asmens duomenis. Buvo pastebėta, jog „Yango taksi“ programoje surinkta informacija gali apimti, pavyzdžiui, kliento vietos informaciją ir kelionės taksi adresą. Dėl šios priežasties Suomijos duomenų apsaugos institucija mano, kad po Rusijos įstatymų reformos negali apsaugoti „Yango taksi“ naudotojų asmens duomenų, kaip reikalaujama pagal ES teisę ir todėl įsakymas sustabdyti duomenų perdavimą į Rusiją yra būtinas (https://tietosuoja.fi/en/-/finnish-dpa-bans-yango-taxi-service-transfers-of-personal-data-from-finland-to-russia-temporarily).

IŠVADOS

1. Asmens duomenų perdavimui, kaip ir duomenų tvarkymui Europos Sąjungos teisė nurodo gana aiškius ir griežtus reikalavimus bei principus. Asmens duomenų apsauga yra neatsiejama nuo kitų pagrindinių žmogaus teisių. Pavyzdžiui, viena iš jų – teisė į privatumą.

2. Nors ir Bendrajame duomenų apsaugos reglamente yra visas atskiras skyrius nuosatų, kuriomis reikia vadovautis perduodant asmens duomenis į trečiasias valstybes, tačiau tokių pagrindinių sąvokų kaip "trečioji valstybė" arba "duomenų perdavimas į trečiąją valstybę" jis neišskiria. Remiantis praktika, duomenų perdavimu gali būti ne tik aktyvus, bet ir pasyvus duomenų perdavimas suteikiant prieigą.

3. Sprendimas dėl tinkamumo yra viena iš priemonių, numatytų pagal Bendrąjį duomenų apsaugos reglamentą, siekiant perduoti asmens duomenis iš ES į trečiąsias šalis, kurios, Komisijos vertinimu, užtikrina panašų asmens duomenų apsaugos lygį kaip ir Europos Sąjunga. Priėmus šį sprendimą duomenų perdavimas yra prilyginamas duomenų perdavimui tarp ES narių. Tačiau šio sprendimo priėmimo procesas yra labai sudėtingas, jį galima bet kada atšaukti, taip pat šis sprendimas yra priimtas tik dėl tam tikro skaičiaus šalių t. y. Sąrašas šalių, į kurias būtų norima perduoti asmens duomenis naudojantis šiuo sprendimu yra labai ribotas.

4. Tinkamos apsaugos priemonės yra alternatyvus asmens duomenų perdavimo būdas. Naudojantis šiomis priemonėmis nereikia laukti kol valstybė priims sprenimą dėl tinkamumo. Nors tinkamos apsaugos priemonės yra greitesnis duomenų perdavimo būdas nei sprendimas dėl tinkamumo, tačiau jų taikymo sritis yra siauresnė nei sprendimo dėl tinkamumo. Pavyzdžiui tinkamos apsaugos priemonės neapima jautrių duomenų perdavimo ir su tuo susijusio teisinio reguliavimo bei tinkamos apsaugos.

LITERATŪROS SĄRAŠAS

1. Teisės norminiai aktai:

1.1. ***Tarptautinės rekomendacijos, gairės, nuomonės:***

1) Europos duomenų apsaugos valdybos Gairės 4/2019 dėl 25 straipsnio Pritaikytoji ir standartizuotoji duomenų apsauga Versija 2.0 Priimta 2020 m. spalio 20 d.
2) Art. 29 Data Protection Working Party, 'Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000' (2001) WP 40 final.
3) Europos duomenų apsaugos valdybos 2021 m. birželio 18 d Nr. 01/2020 „Dėl priemonių asmens duomenų teikimo priemonėms papildyti, siekiant užtikrinti atitiktį Europos Sąjungos asmens duomenų apsaugos lygiui" .
4) Article 29 Working Party, Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995.
5) Europos duomenų apsaugos valdybos 2022 m. liepos 12 d.pareiškimas 02/2022 dėl asmens duomenų perdavimo Rusijos Federacijai.

1.2. Europos Sąjungos teisės aktai:

6) 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR.
7) 2011 m. vasario 16 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 182/2011, kuriuo nustatomos valstybių narių vykdomos Komisijos naudojimosi įgyvendinimo įgaliojimais kontrolės mechanizmų taisyklės ir bendrieji principai.
8) 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas).

2. **Specialioji literatūra:**

9) GDPR: Personal Data Protection in the European Union, Mariusz Krzysztofek, 2021 m.

10) The Transfer of Personal Data from the European Union to the United Kingdom post-Brexit, 2022 m., L. Wittershagen.

11) GDPR: A Commentary 2020 m. C. Kuner, L. A Bygrave, C. Docksey, L. Drechsler.

12) Data Localization Laws and Policy, 2017 m., W. Kuan Hon,.

13) Europos duomenų apsaugos teisės vadovas. 2018 m.

3. Teismų praktika:

3.1. Europos Sąjungos Teisingumo Teismo sprendimai:

14) Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas Schrems.

15) Europos Sąjungos Teisingumo Teismo 2003 m. lapkričio 6 d. sprendimas Lindqvist.

16) Europos Sąjungos Teisingumo Teismo 2020 m. liepos 16 d. sprendimas Schrems II.

4. **Kiti šaltiniai:**

17) Processing of Personal Data by Public Authorities in China: Assessing Equivalence for Cross-border Transfers from the EU to China; Yueming Zhang, 2023.

18) Assessing the Implications of Schrems II for EU-US Data Flow, M. H. Murphy, 2021.

19) European Commission. Adequacy decisions: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

20) 1997 m. birželio 26 d. Nr. 4 dėl pirmųjų gairių dėl asmens duomenų perdavimo trečiosioms šalims ir 1997 m. birželio 24 d. Nr. dėl asmens duomenų perdavimo trečiosioms šalims pagal Direktyvos 25 ir 26 straipsnius.

21) EU Trade Relations with China' (The European Commission) (https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/china_en.

22) Dutch DPA: TikTok fined for violating children's privacy: https://edpb.europa.eu/news/national-news/2021/dutch-dpa-tiktok-fined-violating-childrens-privacy_en.

23) Valstybinė duomenų apsaugos isnspekcija. DUK. BREXIT ir asmens duomenys. Svarbi informacija dėl asmens duomenų perdavimo ir gavimo iš Jungtinės Didžiosios Britanijos ir Šiaurės Airijos Karalystės https://vdai.lrv.lt/uploads/vdai/documents/files/17%20DUK%20BREXIT%20atnaujinta_2021-07.pdf

24) ICO, 'Draft International Transfer Risk Assessment and Tool' (August 2021) https://ico. org.uk/media/about-the-ico/consultations/2620397/intl-transfer-risk-assessment-tool-20210804. pdf

25) Coronavirus: Controversial Israeli spyware firm NSO builds software tracking mobile data to map Covid-19 ttps://www.independent.co.uk/news/world/middle-east/coronavirus-israel-cases-tracking-mobile-phone-nso-spyware-covid-19-a9410011.html

26) Parliamentary question - E-002290/2023 https://www.europarl.europa.eu/doceo/document/E-9-2023-002290_EN.html#def2.

27) Top Apps Of 2022 By Installs, Spend, And Active Users: Report https://www.forbes.com/sites/johnkoetsier/2022/03/23/top-apps-of-2022-by-installs-spend-and-active-users-report/?sh=4ede0683d3ac

28) European firms urge China to give more clarity on data transfer laws https://www.reuters.com/world/china/european-firms-urge-china-give-more-clarity-data-transfer-laws-2023-11-15/.

29) The Information Commissioner's Office. Data protection at the end of the transition period https://ico.org.uk/media/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail-1-0.pdf.

30) Finnish DPA bans Yango taxi service transfers of personal data from Finland to Russia temporarily https://tietosuoja.fi/en/-/finnish-dpa-bans-yango-taxi-service-transfers-of-personal-data-from-finland-to-russia-temporarily.

31) Potential judicial reforms in Israel could impact adequacy https://iapp.org/news/a/potential-judicial-reforms-in-israel-could-impact-adequacy/.

SANTRAUKA

Miglė Vilkaitė

Šiame magistro darbe nagrinėjama duomenų perdavimo į trečiasias šalis samprata, reikšmė ir problematika. Siekiant užtikrinti darbo aktualumą ir analizės kokybę, tema nagrinėjama trimis skirtingais lygmenimis.

Pirmajame lygmenyje analizuojama laisvo duomenų judėjimo, duomenų perdavimo bei trečiosios šalies samprata bei reikšmė. Analizuojant įvairius šaltinius analizuojamos bei nustatomos pagrindinės sąvokos, sampratos bei principai.

Antrasis lygmuo apima išsamesnę duomenų perdavimo būdų analizę, išskiriant juos į atskirus skyrius. Darbe nustatyta, kad duomenų perdavimo būdai yra: asmens duomenų perdavimas pagal sprendimą dėl tinkamumo; asmens duomenų perdavimas taikant tinkamas apsaugos priemones ir asmens duomenų perdavimas taikant nukrypti leidžiančias nuostatas. Analizuojant ir aprašant kiekvieną šį duomenų perdavimo mechanizmą taip pat įvardijami ir jų trūkumai bei kita problematika.

Atlikus minėtą analizę, darbe yra apžvelgiama, kokių trūkumų ir privalumų turi BDAR V skyriuje nurodyti duomenų perdavimo būdai.

SUMMARY

This master's thesis examines the concept, significance and issues of data transfer to a third party. In order to ensure the relevance of the work and the quality of the analysis, the topic is examined at three levels.

The first level analyzes the concept and meaning of free movement of data, data transfer and third party. By analyzing the sources, the main concepts, concepts and principles are analyzed and determined.

The second level includes a detailed analysis of data transfer methods, separating them into a separate section. The work established that the methods of data transfer are: transfer of personal data according to the decision on eligibility; transfer of personal data subject to appropriate safeguards and transfer of personal data subject to derogations. When analyzing and describing each of these data transmission mechanisms, their shortcomings and other problems are also identified.

After the aforementioned analysis, the paper reviews the advantages and disadvantages of the data transfer methods specified in Chapter V of the GDPR.