TARTU ÜLIKOOL

ÕIGUSTEADUSKOND

Avaliku õiguse osakond

Maigi Kalluste

ASJAKOHASTE KAITSEMEETMETE RAKENDAMISE ÕIGUSLIKUD PROBLEEMID ISIKUANDMETE EDASTAMISEL KOLMANDATE RIIKIDE ANDMETÖÖTLEJATELE

Magistritöö

Juhendajad: *dr iur* Mario Rosentau, *LLM* Mari-Liis Orav

Tartu

2023

SISUKORD

SISSEJUHATUS

Andmeid peetakse tänapäeval üheks väärtuslikumaks ressursiks maailmas.[1] Isikuandmed puudutavad igaüht ning need on muutunud keskseks väärtust loovaks „tooraineks“, mille abil luua uusi ja kaasaegseid ärimudeleid.[2] Digitaalajastu, sealhulgas interneti areng, suhtlusvõrgustikud, pilveteenused ja kultuuriline globaliseerumine on toonud kaasa suure hulga isikuandmete piiriülest jagamist ja nende põhjal ettevõtluse arendamist. Seetõttu on muutunud väga oluliseks tagada tõhus andmekaitse nii Euroopa Liidus (EL-is) kui ka väljaspool seda, et säilitada väärtusi ja järgida põhimõtteid isikuandmete töötlemisel.

Ettevõtted on viimasel kümnendil muutnud oma äriprotsesse, hallates oma tegevust seal, kus see neile kõige tulusam on. Varem tsentraliseeritud funktsioone nagu maksete töötlemine, klienditeenindus või tehniline tugi, saab hallata ülemaailmselt, et kasutada ära eriteadmisi mitmes kohas. Sagedased on krediitkaarditehingute, telefoniarvete ja meditsiiniliste dokumentide töötlemine paljudes eri riikides, et kasutada ära madalamaid kulusid ja eriteadmisi. Paljud ettevõtted on loonud *offshore*-klienditeninduskeskused, et vastata oma klientide ootustele abi kättesaadavuse osas reaalajas. Ööpäevaringselt päringutele vastamine Euroopa ettevõtte jaoks võib tähendada andmete viimist riikidesse, kus on tugipersonali tavapärane tööaeg samal ajal, kui siin on öötunnid.[3] Rahvusvaheline ärimudel hõlmab lisaks äriprotsesside haldamisele erinevates riikides ka isikuandmete edastamist EL-ist väljapoole.

Andmekaitsealaste õigusaktide üks eesmärk on tagada, et EL-is asuvate isikute andmete kaitse liiguks andmetega[4] kõikjale kaasa.[5] Andmekaitse on EL-is põhiõigus, mida kaitsevad Euroopa

[1] “Maailma kõige väärtuslikum ressurss pole enam nafta, vaid andmed”, hüüdlause ajalehe The Economist artiklist, vt Parkins, D. The world’s most valuable resource is no longer oil, but data. (06.05.2017). – The Economist. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (26.02.2023). Sama ideed on korratud mitmete ekspertide poolt, vt: Pringle, R. „Data is the new oil“: Your personal information is now the world’s most valuable commodity. (25.08.2017). – CBC News. https://www.cbc.ca/news/science/data-is-the-new-oil-1.4259677 (26.02.2023); Burri, M. Data flows and global trade law. Big data and global trade law. Cambridge University Press, 2020, lk 12.

[2] Aaronson, S. A. Data is different, and that's why the world needs a new approach to governing cross-border data flows. - Digital Policy, Regulation and Governance, 03/2019, lk 444.

[3] OECD. Report on the cross-border enforcement of Privacy Laws. - The Organisation for Economic Co-operation and Development, 10/2006, lk 7.

[4] Andmete all mõistetakse käesolevas töös isikuandmeid üldmääruse tähenduses ning neid kahte terminit käsitletakse töös samaväärsetena.

[5] Houser, K.A., Voss, W.G. Personal data and the GDPR: providing a competitive advantage for US companies. – American Business Law Journal, 19.06.2020, lk 297.

Liidu toimimise leping[6] (ELTL) ja Euroopa Liidu põhiõiguste harta (harta).[7] Selle keskmes on inimeste õigus privaatsusele ja eraelu puutumatusele, mistõttu on andmekaitse ka sotsiaalne väärtus. Ent andmekaitset saab mõista erinevates õigus- ja kultuuriruumides erinevalt.[8] Euroopas on andmekaitse põhiõigust mõistetud eraelu puutumatuse elemendina, samas kui näiteks USA seadusandluses ei mõisteta andmekaitset põhiõigusena.[9]

EL-is reguleerib andmekaitset Euroopa Parlamendi ja nõukogu määrus 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (üldmäärus),[10] mis jõustus 25. mail 2018 ja on kohaldatav kõikides EL-i liikmesriikides. Üldmäärus reguleerib isikuandmete kogumist ja töötlemist EL-is ning kehtestab vastutavatele töötlejatele ja volitatud töötlejatele mitmed andmekaitsekohustused. Üldmäärus vastab oma eelkäijast, Euroopa Parlamendi ja nõukogu direktiivist 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta,[11] enam tänapäeva digitaliseerunud maailma vajadustele. Üldmäärust peetakse Euroopa andmekaitseõiguse kujundajaks, mis on kehtestatud põhiõiguste kaitseks ning see on esmane õigusakt EL-is, mis reguleerib andmekaitset ning seda ka põhiõiguse tähenduses.[12]

Üldmääruse kohaldamisala ulatub kaugemale EL-i territooriumist, selle reeglid rakenduvad artikli 3 kohaselt isikuandmete töötlejatele ka väljaspool liitu, kui töötlemine on seotud liidus asuvate andmesubjektide andmetega. Eksterritoriaalsuse põhimõttest lähtuvalt laieneb üldmääruse kohaldamisala kolmandate riikide andmetöötlejatele näiteks olukorras, kus tööandja kasutab Euroopas asuvate töötajate ja klientide andmete haldamiseks, varundamiseks ning taastamiseks pilvandmebaasi, mida pakub kolmanda riigi ettevõte nagu Amazon Web Services[13] või Dropbox[14];

---

[6] 26. oktoobri 2012. aasta Euroopa Liidu toimimise lepingu konsolideeritud versioon. – ELT C 326, lk 1-390.
[7] 26. oktoobri 2012. aasta Euroopa Liidu põhiõiguste harta. – ELT L 2012/C 326/02, lk 391–407.
[8] European Data Protection Supervisor. Data Protection. - https://edps.europa.eu/data-protection/data-protection_en (25.11.2022).
[9] Houser, K.A., Voss, W.G., lk 297.
[10] 27. aprilli 2016. aasta Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). – ELT L 119, 4.5.2016, lk 1-88.
[11] 24. oktoobri 1995. aasta Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. – ELT L 281, 23.11.1995, lk 31-50.
[12] Euroopa Komisjon. Andmekaitse EL-is. - https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_et (21.11.2022)
[13] Amazon Web Service. Privacy Notice. (10.01.2023). - https://aws.amazon.com/privacy/, (03.04.2023).
[14] Dropbox Help centre. Where is my data stored? - https://help.dropbox.com/security/physical-location-data-storage, (07.02.2023).

samuti kohaldub üldmäärus näiteks USA ettevõttele masinõppel põhineva juturoboti ChatGPT Euroopa kasutajate isikuandmete töötlemisel.[15] Kolmanda riigina tuleb üldmääruse ja käesoleva töö mõistes käsitleda riiki, mis ei kuulu Euroopa Majanduspiirkonda. EMP riikide hulka kuuluvad lisaks Euroopa Liitu kuuluvatele riikidele ka Island, Norra, Lichtenstein.[16]

Isikuandmete kaitse teema on teravalt tähelepanu keskmes seoses isikuandmete edastamisega EL-i piiridest väljapoole. Andmete kaitse piiriülestes küsimustes on üks keerulisemaid probleeme selles valdkonnas. Paljud Euroopa ettevõtted teevad pidevat koostööd kolmandate riikide ettevõtetega ning seega on oluline tagada, et isikuandmete töötlemine ka väljaspool EL-i vastaks samadele kõrgetele andmekaitse standarditele nagu liidusisestel andmetöötlustegevustel.

Andmete edastamine EL-ist kolmandate riikide andmetöötlejatele toob kaasa täiendavaid õiguslikke riske, mis võivad ohustada isikuandmete kaitset seoses erinevate õiguskordade ja kohalduva õigusega ning seetõttu on käesoleva töö õiguslikuks probleemiks see, et Euroopa Liidus asuvate andmesubjektide isikuandmete kaitse tase vastavalt üldmäärusele ei pruugi olla väljaspool EL-i samaväärne liidus tagatuga.

Magistritöö eesmärk on välja selgitada, kas ja kuidas üldmääruse artiklis 46 toodud isikuandmete kolmandate riikide andmetöötlejatele edastamise tingimused kaitsevad isikuandmeid, mis on nende piirangute peamised õiguslikud probleemid ning kas ja kuidas on võimalik parandada kaitset isikuandmete edastamisel kolmandate riikide andmetöötlejatele. Magistritööga otsitakse vastuseid järgmistele küsimustele:

1) Missugune on Euroopa Liidu isikuandmete kaitse õiguslik taust ja regulatsioon, arvestades muuhulgas üldmääruse eksterritoriaalset mõju ja eesmärke?
2) Missugune on üldmääruse V peatüki kaitsestandard isikuandmete edastamisel kolmandate riikide andmetöötlejatele ning kas üldmääruse artiklis 46 sätestatud kaitsemeetmed (standardsete andmekaitseklauslite näitel) tagavad üldmääruses sätestatud isikuandmete kaitse taseme ja vastavuse üldmääruse eesmärkidele?
3) Millised õiguslikud võimalused võiksid tagada isikuandmete kolmandate riikide andmetöötlejatele edastamisel nende piisava kaitse taseme?

[15] Open AI Privacy Policy. 23.01.2023. - https://openai.com/policies/privacy-policy. (04.04.2023).

[16] Üldmääruse pealkirja juures olev täiendus viitab, et üldmääruse tekst on kohaldatav kõikides EMP riikides. Käesolevas töös tähendab Euroopa Liit (EL) üldmääruse kontekstis kõiki EMP riike.

Töö koosneb kolmest peatükist. Esimeses peatükis tuuakse välja isikuandmete kaitse õiguslik taust, kujunemine ja õigusraamistik EL-is, andmekaitse kui põhiõigus ja selle seos teiste põhiõigustega ning tuuakse välja peamised õigusaktides sisalduvad põhimõtted, mis on olulised isikuandmete edastamise käsitluses väljapoole EL-i. Lisaks avatakse mõnede mõistete sisu, millel on oluline tähendus töös. Töö teises peatükis vaadeldakse, milline on Euroopa kaitsestandardi sisu andmekaitses üldmääruse V peatüki tähenduses; samuti, millised on põhimõtted ja eesmärgid ning problemaatika selliste eesmärkide saavutamisel.

Üldmääruse V peatükk näeb isikuandmete edastamisel kolmandate riikide andmetöötlejatele ette järjekorra õiguslikest tingimustest. Esmalt, kui Euroopa Komisjon on vastavalt üldmääruse artiklile 45 teinud otsuse riigi või organisatsiooni kaitse piisavuse kohta, ei ole täiendavate tingimuste rakendamine andmeedastusel vajalik ning andmevahetus toimub nii nagu liidus. Kui EL-i välisel riigil, kuhu andmeid edastatakse, kaitse piisavuse otsust pole, peab andmete edastaja tuginema üldmääruse artikli 46 õiguslikele kaitsemeetemete ning lisaks läbi viima mõjuhinnangu[17], mis on sisult sarnane kaitse piisavuse otsusele artiklis 45, veendumaks, et kolmanda riigi õiguskord ei kahjusta isikuandmete kaitse taset. Üldmääruse artiklite 45 kui 46 meetmete puudumisel on võimalik tugineda eranditele üldmääruse artiklis 49.

Selleks, et tagada EL andmesubjektide isikuandmete kaitse kolmandates riikides samal tasemel nagu Euroopa Liidus, näeb üldmääruse artikkel 46 ette kohaldatavate asjakohaste kaitsemeetmete rakendamise, millega koos on vajalik andmetöötlejal läbi viia mõjuhinnang. See on andmetöötleja jaoks õiguslikult keeruline ja ajamahukas protsess ning selliste meetmete rakendamine ei pruugi tagada isikuandmete kaitset samaväärselt EL-is tagatuga. Kaitsemeetmete all mõistetakse käesolevas töös üldmääruse V peatüki artikli 46 lõikes 2 ette nähtud õiguslikke meetmeid, mida tuleb rakendada isikuandmete edastamisel kolmandate riikide andmetöötlejatele. Sisuliselt on tegemist üldmäärusega kehtestatud isikuandmete edastamispiirangutega kolmandate riikide andmetöötlejatele.

Kaitsemeetmete eesmärk on kaitsta isikuandmeid teiste riikide ametiasutuste piiramatu ligipääsu eest, mida on käsitletud kohtuasjas C-362/14, *Maximillian Schrems versus Data Protection*

[17] Mõjuhinnangu (ingl. *Transfer Impact Assessment)* kohta täpsemalt: European Data Protection Board. EDPB adopts final version of Recommendations on supplementary measures, letter to EU Institutions on the privacy and data protection aspects of a possible digital euro and designates three EDPB Members to the ETIAS Fundamental Rights Guidance Board. (21.06.2021). – https://edpb.europa.eu/news/news/2021/edpb-adopts-final-version-recommendations-supplementary-measures-letter-eu_en (10.04.2023).

Commissioner (*Schrems I*)[18] ja kohtuasjas C-311/18, *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (*Schrems II*)[19]. Need kohtuotsused on mõjutanud üldmääruses sätestatud asjakohaste kaitsemeetmete tõlgendust.

Enne üldmääruse artikli 46 kohaste kaitsemeetmete uurimist teises peatükis vaadeldakse üldmääruse artiklis 45 toodud Euroopa Komisjoni kaitse piisavuse otsuse regulatsiooni ning selles ette nähtud kaitse taseme piisavuse hindamise aluseks olevaid asjaolusid. See on oluline, kuna Euroopa Andmekaitsenõukogu (EDPB) juhendid ja kohtupraktika viitavad kolmanda riigi kaitse piisavuse otsuse puudumisel samade põhimõtete rakendamisele asjakohaste kaitsemehhanismide kasutamisel, mis on loetletud üldmääruse artiklis 46. Oluline on need meetmed välja tuua, et teha järeldusi töö õigusliku probleemi kohta ning hinnata, kas üldmääruse artikli 46 õiguslikud meetmed koos mõjuhinnanguga tagavad isikuandmete kaitse samaväärsel tasemel väljaspool Euroopa Liitu.

Töö ülevaatlikkuse seisukohast on esile toodud asjakohaste kaitsemeetmete loetelust artiklis 46 standardsete andmekaitseklauslite kasutamine, kuna ühe kaitsemeetme näitel saab edasi anda käesoleva töö õiguslikku probleemi; lisaks on 2021. aastal Euroopa Komisjoni rakendusotsusega nr 2021/914 vastu võetud standardsed andmekaitseklauslid[20] üldmääruse artikli 46 lõike 2 punkti c alusel enim kasutatav kaitsemehhanism isikuandmete edastamisel väljapoole EL-i.[21] Käesolevas töös puudutatakse kolmandat kategooriat, üldmääruse artiklis 49 toodud erandite alusel edastamist vaid marginaalselt, tuues välja nende põhisisu ja näidates ära erandite alusel andmete edastamise suurima probleemi seoses üldmääruse eesmärgiga tagada isikuandmete samaväärne kaitse tase kõikjal, kuhu andmed liiguvad.

Kolmandas peatükis hinnatakse võimalusi, mis võiksid ületada eelmises peatükis välja toodud kitsaskohti seoses andmete edastamisega kolmandate riikide andmetöötlejatele. Selles peatükis analüüsitakse, kuidas oleks võimalik lihtsustada kaitsemeetmete rakendamise protsessi eelkõige mõjuhinnangu läbiviimise osas, kuivõrd võimalik on õigusliku ühtsuse saavutamine erinevates riikides turvalise andmeedastuse tagamise eesmärgil, samuti andmete lokaliseerimine

[18] EKo C-362/14, *Maximillian Schrems versus Data Protection Commissioner*, ECLI:EU:C:2015:650.

[19] EKo C-311/18, *Data Protection Commissioner versus Facebook Ireland Limited, Maximillian Schrems*, ECLI:EU:C:2020:559.

[20] 4. juuni 2021. aasta Euroopa Komisjoni rakendusotsus 2021/914 kolmandatesse riikidesse isikuandmete edastamise lepingu tüüptingimuste kohta vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) 2016/679. - ELT L 199/31, lk 31-61.

[21] International Association of Privacy Professionals and Ernst & Young, Annual Privacy Governance Report 2019. – https://iapp.org/resources/article/iapp-ey-annual-governance-report-2019/ (12.12.2022).

isikuandmete kaitsmise mehhanismina ning põgusalt peatutakse ka EL-i ja USA arengutel seoses uue andmekaitseraamistiku väljatöötamise ja enne selle jõustumist ettenähtavate probleemidega.

Eestis on vähe teadusuuringuid seoses isikuandmete edastamisega kolmandate riikide andmetöötlejatele, ent selleks on palju võimalusi. Seetõttu pakub see valdkond palju võimalusi uurimistöödeks, et aidata kaasa paremale arusaamisele sellest, kuidas tagada isikuandmete kaitse piiriüleselt ning laiendada andmekaitsealast teadlikkust. Lisaks on andmeedastus kolmandatesse riikidesse pälvinud Euroopa Andmekaitsenõukogu (EDPB) tähelepanu seoses Venemaaa Föderatsiooni sõjalise ründega Ukraina vastu, arvates Venemaa välja Euroopa Nõukogust ning hoiatades isikuandmete edastamise eest Venemaale lähtuvalt üldmääruse V peatüki nõuetest.[22]

Magistritöö eesmärgi saavutamiseks kasutatakse kombineeritult ajaloolist, kvalitatiivset ja ka võrdlevat uurimismeetodit. Normatiivsete allikate osas pööratakse tähelepanu eelkõige üldmääruse ja direktiivi 95/46/EÜ sätetele ja mõningal määral ka EL õigusaktidele, mis seonduvad andmekaitseõigusega EL õigusruumis. Üldmääruse ja 1995. aasta direktiivi 95/46/EÜ kui peamiste õigusaktide kõrval on käesoleva töö temaatika mõjutatud Euroopa Kohtu otsustest *Schrems I* ja *Schrems II*, milles sätteid uuritakse lisaks. Mitmed kohtupraktika ja direktiivi 95/46/EÜ põhimõtted on üle kandunud üldmäärusesse ja jäänud kehtima ning need kajastuvad ka töös viidatud EDPB juhistes.

Töös on kasutatud mitmeid mittenormatiivseid allikaid, sealhulgas üldmääruse kommentaare, õigusalaste väljaannete artikleid ja muid teaduslikke väljaandeid, seisukohti, EL institutsioonide teatisi, andmekaitse valdkonnaga tegelevate isikute avalikke avaldusi, töödokumente, pressiteateid ja poliitikateateid. Üldmääruse sätete tõlgendamisel on oluline roll Euroopa Komisjoni, Euroopa Andmekaitseinspektori ja eelkõige EDPB juhistel. Enne EDPB juhiseid kehtisid direktiivi 95/46/EÜ artikli 29 alusel loodud töörühma A29WP suunised. Sellise andmekogumise ja -töötlemise käigus saadud materjali analüüs, sh temaatikat uurivate õigusteadlaste arvamused, aitavad kaasa töö eesmärgi saavutamisele nii õigusaktide sõnastuse ja eesmärgi väljatoomisel kui ka rakendamise ja problemaatika analüüsil.

Magistritööd kõige enam iseloomustavad märksõnad on andmekaitse, isikuandmed, privaatsus, andmetöötlus, kolmandad riigid.

[22] European Data Protection Board. Statement 02/2022 on personal data transfers to the Russian Federation. (12.07.2022). – https://edpb.europa.eu/system/files/2022-07/edpb_statement_20220712_transferstorussia_en.pdf (10.04.2023).

1. Andmekaitse regulatsioon ja kontseptsioon Euroopa õiguses

1.1. Andmekaitse kui põhiõigus Euroopas

Isikuandmete töötlemisel ja kolmandate riikide andmetöötlejatele edastamisel on oluline mõista Euroopa Liidu andmekaitse regulatsiooni ja selle kontseptsiooni lähtuvalt andmekaitsest kui põhiõigusest. Enne, kui süvenetakse kolmandate riikide andmetöötlejatele andmete edastamise erisustesse, tuleb esmalt määratleda andmekaitse regulatsiooni sisu Euroopa Liidus. Isikuandmete kaitse sisuliseks lähtekohaks peetakse ELTL-ist ja hartast tulenevalt eeskätt isiku õigust privaatsusele ja eraelu kaitsele. Oluline on seejuures, et isikuandmete kaitsmiseks kehtestatud õigusaktid ei keskendu mitte lihtsalt andmete kaitsele, vaid just nimelt inimeste privaatsusele ja eraelu puutumatusele. Vaatleme järgnevalt neid kahte andmekaitsega tihedalt seotud põhiõigust ning selgitame, kuidas need on seotud Euroopa Liidu andmekaitse regulatsioonidega.

Õigus privaatsusele on universaalne põhiõigus, mida tunnustatakse peaaegu igas maailma riigis ning see on kaitstud ja sätestatud erinevates õigusaktides, sh riigi põhiseaduses.[23] Ka eraelu puutumatust tunnustatakse universaalse inimõigusena paljudes maailma riikides, samas kui andmekaitset mitte – vähemalt mitte veel.[24] Õigus eraelu puutumatusele ja eraelule on sätestatud II maailmasõja järgselt ÜRO inimõiguste ülddeklaratsiooni[25] artiklis 12, mille kohaselt ei tohi meelevaldselt sekkuda kellegi eraellu, perekonda, kodu ega kirjavahetusse. Sisulisemalt tunnustati eraelu puutumatust Euroopa inimõiguste konventsiooni[26] artiklis 8 ning Euroopa põhiõiguste harta artiklis 7, mille kohaselt on igaühel õigus sellele, et austataks tema era- ja perekonnaelu ja kodu ning sõnumite saladust.

Harta artikkel 8 tagab selgesõnaliselt õiguse isikuandmete kaitsele, nagu märgib üldmääruse esimene põhjenduspunkt, rõhutades, et isikuandmete töötlemise kaitse on füüsiliste isikute põhiõigus. Harta artikkel 8 lõige 2 näeb ette, et isikuandmeid tuleb töödelda asjakohaselt ja

[23] Kolmandatest riikidest on näiteks paljudes USA osariikides privaatsuse kaitse sätestatud nende põhiseadustes. Põhiseadusega kaitsevad ka Brasiilia, Lõuna-Aafrika Vabariik, Lõuna-Korea õigust privaatsusele. Vt lähemalt: Solove, D.J. Understanding privacy. – Harvard University Press, 05/2008, lk 3.

[24] European Data Protection Supervisor. Privacy – a fundamental right. – https://edps.europa.eu/data-protection/data-protection_en#Cross_border (26.02.2023).

[25] 10. detsembri 1948. aasta ÜRO inimõiguste ülddeklaratsioon (Peaassamblee resolutsioon 217A). – A/RES/217.

[26] Inimõiguste ja põhivabaduste kaitse konventsioon. – RT II 2010, 14, 5.

kindlaksmääratud eesmärkidel ja asjaomase isiku nõusolekul või muul õigusaktides sätestatud alusel ning et igal inimesel on õigus andmetele juurde pääseda mis on tema kohta kogutud ja õigus nõuda nende parandamist. Samad põhimõtted, õigused ja nõuded on põhjalikumalt välja töötatud üldmääruse III peatükis.

Lissaboni lepingu jõustumine 2009. aastal andis põhiõiguste hartale samasuguse õigusliku väärtuse kui EL-i aluslepingutele, luues tugevama aluse tõhusamale ja terviklikumale EL-i andmekaitse raamistikule.[27] Seega on harta siduv EL-i institutsioonidele, asutustele ja liikmesriikidele. Lisaks nõuab ELTL artikkel 16 lõige 2 EL-i poolt isikuandmete töötlemiseks kehtestatud andmekaitseeskirjade sätestamist. Euroopa Liit on ainulaadne selles osas, et see nõuab oma aluslepingutes sellise kohustuse kehtestamist.[28]

Eesti siseriiklikus õiguses on andmekaitsega tihedalt seotud Eesti Vabariigi põhiseaduse[29] (PS) §-s 26 nimetatud eraelu puutumatuse põhimõte, mille alusel on igaühel õigus perekonna- ja eraelu puutumatusele. PS § 26 sõnastamisel on selgeks eeskujuks olnud Euroopa Inimõiguste konventsiooni artikli 8 lõige 1, kuna põhiseadus sisaldab sama põhimõtet. Isikliku ja perekonnaelu, kirjavahetuse saladuse, au ja reputatsiooni kaitse on sätestatud ka kodaniku ja poliitiliste õiguste rahvusvahelise pakti artiklis 17.[30]

Privaatsus pole pelgalt individuaalõigus, vaid ka sotsiaalne väärtus ning seda saab mõista eri õigus- ja kultuuriruumides mitmeti. Näiteks USA-s on ajalooliselt peetud privaatsust vabaduse elemendiks, õiguseks olla vaba riigipoolsetest sekkumistest.[31] Euroopas on andmekaitse põhiõigus eraelu puutumatuse element, kuid näiteks USA õiguses ei mõisteta andmekaitset põhiõigusena.[32]

Andmekaitse seisukohast tähendab õigus privaatsusele ja õigus eraelu puutumatusele olla sõltumatu ja kontrollida sealjuures enda kohta käivat teavet. Õigusest eraelu puutumatusele tuleneb andmekaitse õiguse mõiste. Mõlemad õigused on olulised põhiväärtuste ja -õiguste säilitamisel ja

[27] Lissaboni leping. – ELT 2007/C 306/1.
[28] European Parliament. Understanding EU data protection policy. Summary. – https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/698898/EPRS_BRI(2022)698898_EN.pdf (10.04.2023).
[29] Eesti Vabariigi põhiseadus. – RT I, 15.05.2015, 2.
[30] Lõhmus, U. Eesti Vabariigi põhiseadus. Komm vlj. 2012. – https://pohiseadus.ee/sisu/3497/paragrahv_26 (27.02.2023).
[31] European Data Protection Supervisor. Data Protection. – https://edps.europa.eu/data-protection/data-protection_en (25.11.2022).
[32] Houser, K.A., Voss, W.G. lk 297.

edendamisel. Andmekaitsel on eesmärk tagada isikuandmete õiglane töötlemine (nt kogumine, kasutamine, säilitamine) nii avalikus kui ka erasektoris.[33]

EL-i liikmesriikide pühendumus isikuandmete kaitsele ei kajastu mitte ainult EL-i õigusaktides. Euroopa Nõukogu konventsioon nr 108[34] on esimene siduv rahvusvaheline leping, mis käsitleb isikuandmete kaitset. Sellele kirjutasid alla kõik Euroopa Nõukogu liikmed (sealhulgas kõik EL-i liikmesriigid) ning Argentina, Cabo Verde, Mauritius, Mehhiko, Maroko, Senegal, Tuneesia ja Uruguay[35] ning seda ajakohastati 2018. aasta oktoobris.[36]

27. aprillil 2016 võttis Euroopa Liit vastu uue andmekaitsealase õigusraamistiku - Euroopa Parlamendi ja Nõukogu üldmääruse 2016/679.[37] Üldmäärus on Euroopa õiguse kujundaja, mis on kehtestatud põhiõiguste kaitseks, ning see on esmane õigusakt[38], mis reguleerib nii andmekaitset kui ka andmekaitse põhiõigust EL-is. Selle rakendamine oli ühelt poolt hädavajalik samm üksikisikute andmetega seotud põhiõiguste tugevdamiseks digiajastul ja teiselt poolt äritegevuse soodustamiseks, määrates kindlaks normid, mida äriühingud ja avalik-õiguslikud asutused peavad digitaalsel ühtsel turul järgima.[39]

Kui isikuandmete töötlemine rikub põhiõigusi, näiteks õigust eraelu puutumatusele, aga ka õigust vabale enesemääramisele või mõnele muule põhiõigusele, on tegemist tõsise rikkumisega. Isikuandmete töötlemine peab üldmääruse põhjenduspunktide kohaselt olema läbipaistev, õiguspärane ja proportsionaalne ning tagama inimeste õiguse oma isikuandmete kaitsele. Kui isikuandmete töötlemisel on rikutud põhiõigusi, on isikul üldmääruse alusel õigus nõuda oma

[33] European Data Protection Supervisor. Data Protection. – https://edps.europa.eu/data-protection/data-protection_en#Cross_border (26.02.2023).
[34] 28. jaanuari 1981. aasta isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon. – RT II 2001, 1, 3.
[35] Konventsiooni nr 108 osalisriigid: Council of Europe. Parties to Convention 108. - https://www.coe.int/en/web/data-protection/national-information (27.03.2023).
[36] European Parliament. Understanding EU data protection policy. Historical developments. – https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/698898/EPRS_BRI(2022)698898_EN.pdf (10.04.2023).
[37] European Commission. Data protection in the EU. – https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en (21.11.2022).
[38] On leitud, et üldmäärus rikub oma olemuselt EL-i aluslepinguid, kuna see on põhimõttelises vastuolus EL-i põhiseadusliku korraldusega, mis on moodustatud kooskõlas asutamislepingutega. Nimelt on üldmäärus „Euroopa seadus", kuid seadused on Euroopa lepingutega keelatud. Üldmäärus „Euroopa raamseadus", kuid Euroopa seadused on Euroopa lepingutega keelatud, kuna nende kehtestamine Euroopa konstitutsiooni või konstitutsioonilise lepinguga kukkus läbi. Vt lähemalt: Rosentau, M. The General Data Protection Regulation and its Violation of EU Treaties. Juridica International, 27/2018, lk 36-37.
[39] Euroopa Komisjon. Andmekaitse EL-is. - https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_et (21.11.2022)

õiguste kaitset. Andmekaitsealaste rikkumiste tagajärjed võivad rikkujale olla märkimisväärsed: üldmääruse nõuete mittetäitmine võib põhjustada suuri rahalisi sanktsioone ettevõtetele ja andmetöötlejatele ning halvendada nende mainet. Seetõttu on oluline, et ettevõtted ja andmetöötlejad järgiksid hoolikalt andmekaitsealaseid õigusnorme ning tagaksid, et isikuandmete töötlemine toimub alati vastavalt kehtivatele õigusaktidele, kaitstes seeläbi inimeste põhiõigust andmekaitsele.

Eeltoodut kokku võttes võib öelda, et füüsiliste isikute kaitse isikuandmete töötlemisel on Euroopa õigusruumis põhiõigus, mis on kujunenud pika aja vältel ning mis on oma tähtsuselt võrdne privaatsuse ja eraelu puutumatusega. Andmekaitse kui põhiõiguse eesmärk on väärtustada inimese õigust privaatsusele ja eraelule, see on sätestatud EL aluslepingutes, üldmääruses, EL kohtupraktikas kui ka õiguslikult siduvas rahvusvahelises Euroopa Nõukogu konventsioonis nr 108. Andmekaitseõigus rõhutab, et isikuandmeid tuleb töödelda seaduslikult, õiglaselt ja läbipaistvalt ning et inimestel peab olema kontroll oma andmete üle. Järgnevalt keskendume konkreetsemalt andmekaitse regulatsioonile Euroopa Liidus ja Eestis.

1.2. Andmekaitseõiguse raamistik Euroopa Liidus

1.2.1. Euroopa Liidu andmekaitseõiguse ajalooline taust

Euroopa Liidus on aastakümneid järgitud kõrgeid andmekaitseõiguse standardeid. Üldmääruse ajalooline taust rõhutab Euroopa Liidu pühendumust andmekaitse ja privaatsuse kaitsmisele, kaitstes samal ajal ka ettevõtete huve ning võimaldades neil tegutseda Euroopa Liidus turvaliselt ja õiguslikult.

Andmekaitse valdkonna arengud algasid Euroopa Liidu liikmesriikide siseselt 1970. aastal, kui Saksamaa Hesseni liidumaa kehtestas Euroopas esimesena seaduse, mis käsitleb konkreetselt isikuandmete kaitset. Rootsi kehtestas esimesed riiklikud andmekaitsealased õigusaktid 1973. aastal, millele järgnesid Saksamaa 1977. aastal ja Prantsusmaa 1978. aastal. Need seadused võeti kasutusele II maailmasõja järgselt vastusena Saksamaal kehtestatud jälitusrežiimidele ja selle käigus ka inimeste isikuandmete suures koguses kogumisele ilma igasuguse õigusliku aluseta tänapäevases mõistes, mistõttu olid need seaduses Prantsusmaal ja Rootsis tugeva

privaatsuskultuuri väljenduseks enne EL-i ühtse andmekaitseraamistiku väljatöötamist. 1975. aasta mais võttis Euroopa Parlament vastu resolutsiooni üksikisikute õiguste kohta andmekaitsele, milles märgiti, et nende õiguste kaitse on liikmesriikide kohustus.[40]

Isikuandmete kaitse põhimõtted rahvusvahelises regulatsioonis ulatuvad tagasi 20. sajandi lõppu, kui isikuandmete töötlemiseks kehtestas 1980. aastal Majanduskoostöö ja Arengu Organisatsioon (OECD), kuhu kuuluvad Ameerika Ühendriigid (USA) ja enamik Euroopa Liidu liikmesriike, "Nõukogu soovitused seoses eraelu puutumatuse kaitset ja isikute piiriülest liikumist reguleerivate suunistega", mida värskendati 2013. aastal.[41] Teine üldmäärusele eelnenud direktiiv oli 1995. aasta Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta, mis põhines OECD eraelu puutumatuse kaitse üldpõhimõtetel. EL-i andmekaitsealaste õigusaktide ja 1995. aasta direktiivi 95/46/EÜ kehtivusest alates on rahvusvahelise andmeedastuse suhtes kohaldatud rangeid nõudeid, mille eesmärk on tagada, et kaitse leviks koos andmetega.[42] See näitab, et õiguskord, mis kehtestatakse isikuandmete kaitsmiseks, on suunatud eelkõige inimeste kaitsele, mitte nende andmete kaitsele.

EL-i andmekaitsealaste õigusaktide algusest ehk 1995. aasta direktiivi 95/46/EÜ vastuvõtmisest, mis on üles ehitatud OECD 1980. aasta eraelu puutumatuse ja isikuandmete piiriüleste voogude kaitse suuniste ja Euroopa Nõukogu 1981. aasta konventsiooni üksikisikute kaitse kohta isikuandmete automaatsel töötlemisel, on Euroopa Liidus andmeedastusreeglid andmekaitseraamistiku oluline osa. Konventsioon nr 108 on seadnud ranged nõuded isikuandmete edastamisele EL-ist kolmandatele riikidele, et vältida EL andmekaitsestandarditest kõrvalehoidmist, kui andmed edastatakse madalamate kaitsestandarditega jurisdiktsioonidesse. Sellest ajast alates on direktiivi 95/46/EÜ rahvusvaheliselt tunnustatud kui vahendit, mis kehtestab rangeimad andmekaitsestandardid, ning selle piiriülese andmevoo reeglid on saanud piiriülese andmevoo etaloniks teistes jurisdiktsioonides.[43]

---

[40] European Parliament. Understanding EU data protection policy. Historical developments. (2023). - https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/698898/EPRS_BRI(2022)698898_EN.pdf (10.04.2023).

[41] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data. (11.07.2013). - https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 (25.11.2022).

[42] OECD. Report on the cross-border enforcement of Privacy Laws. 10/2006. - The Organisation for Economic Co-operation and Development, lk 22.

[43] Svantesson, D.J.B. The extraterritoriality of EU data privacy law - its theoretical justification and its practical effect on US businesses. – Stanford Journal of International Law, Nr 1 (2014), lk 62–63.

Kokkuvõtteks saab öelda, et Euroopa Liit on aastakümneid juurutanud rangeid andmekaitseõiguse standardeid, mis rõhutavad nende pühendumust andmekaitse ja privaatsuse kaitsele. Isikuandmete kaitse õiguslik regulatsioon algas 1980. aastal OECD soovituste ja 1995. aasta Euroopa Parlamendi ja nõukogu direktiivi 95/46/EÜ-ga, sisaldades põhimõtet, et kaitse leviks koos andmetega. Euroopa Liidus on toimunud arenguid ka liikmesriikide siseselt, kus esimesed riiklikud andmekaitsealased õigusaktid võeti kasutusele pärast II maailmasõja järgset jälitusrežiimi.

1.2.2. Üldmääruse kohaldamisala ja rakendamine

Üldmäärust kohaldatakse alates 25. maist 2018 ning selle eksterritoriaalne mõju[44] laieneb andmetöötlusel ettevõtetele, üksikisikutele ja avalik-õiguslikele asutustele, sealhulgas neile, kellel ei ole Euroopa Liidus asutatud asukohta, kuid kes üldmääruse artikli 4 punkti 1 ja 2 mõistes töötlevad[45] isikuandmeid[46] Euroopa Liidus asuvate füüsiliste isikute (andmesubjektide) suhtes ja töötlemine on üldmääruse artikli 3 kohaselt seotud neile kaupade või teenuste pakkumisega kas tasu eest või tasuta või andmesubjekti käitumise jälgimisega ulatuses, milles see toimub Euroopa Liidus. Üldmäärus asendas eelnimetatud Euroopa andmekaitse direktiivi 95/46/EÜ ning selle eesmärk on tugevdada Euroopa kodanike isikuandmete kaitset ja ühtlustada andmekaitse reegleid kogu EL-is. Selle raamistiku kohaselt on ettevõtetel ja organisatsioonidel, mis koguvad ja töötlevad EL-i kodanike isikuandmeid, kohustus järgida teatavaid reegleid ja protseduure, et tagada nende andmete turvalisus ja privaatsus. Üldmäärus kehtestab ka uued nõuded seoses isikuandmete töötlemisega, näiteks andmesubjekti õigused, turvameetmed, teavituskohustus andmekaitsereeglite

[44] Üldmääruse põhjenduspunktide 22 ja 24 ning artikkel 3 kohaselt võib üldmäärus kohalduda nii vastutavale kui volitatud töötlejale, kui töötleja tegevuskoht asub EL-is ning seda sõltumatult töötleja asukohast. Vt: European Data Protection Board. Guidelines 3/2018 on the territorial scope of the GDPR (Article 3). (12.11.2019). - https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf, lk 5, (10.04.2023).

[45] Töötlemise mõiste on defineeritud üldmääruse artikkel 4 punktis 2 ning hõlmab isikuandmete või nende kogumitega tehtavaid automatiseeritud või automatiseerimata toiminguid nagu kogumine, dokumenteerimine, korrastamine, struktureerimine, säilitamine, kohandamine ja muutmine, päringute tegemine, lugemine, kasutamine, edastamise, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine, ühitamine või ühendamine, piiramine, kustutamine või hävitamine.

[46] Isikuandmete mõiste on defineeritud üldmääruse artikkel 4 punktis 1 ning selleks on igasugune teave tuvastatud või tuvastatava füüsilise isiku kohta.

rikkumise korral ning suuremad trahvid rikkumiste eest.[47] Üldmäärus loob raamistiku ettevõtete ja riigiasutuste isikuandmete töötlemiseks, sealhulgas isikuandmete edastamiseks kolmandatele riikidele. Kuna tehnoloogilised arengud seavad aina enam andmekaitsega seotud põhiõigusi proovile, vähendades üksikisiku kontrolli oma andmete üle ja suurendades teisalt privaatsusriske, oli üldmääruse jõustumine kogu Euroopa Liidus oluline samm andmekaitse kui põhiõiguse kaitseks.

Euroopa Liidu institutsioonidele kehtib Nõukogu määrus nr 2018/1725[48], mis reguleerib koos üldmääruse sätetega isikuandmete kaitset Euroopa Liidu institutsioonide ja organite poolt töödeldavate isikuandmete suhtes. Nimetatud määrus hõlmab isikuandmete töötlemist Euroopa Liidu institutsioonide ja organite poolt kõikides valdkondades ning nõuab andmekaitsega seotud kohustuste täitmist ja andmesubjektide õiguste tagamist. Määrus kehtib kõigile Euroopa Liidu institutsioonidele ja organitele ning nendega seotud isikuandmete töötlejatele ja volitatud töötlejatele. Lisaks kehtib EL-is direktiiv 2016/680/EÜ[49], mida kohaldatakse ainult õiguskaitseasutustele. Käesoleva töö raames keskendutakse üldmäärusele, jättes kõrvale EL institutsioonide ja õiguskaitseasutuste spetsiifilisema regulatsiooni nimetatud õigusaktide alusel.

Üldmäärus on suunatud EL liikmesriikidele, et ühtlustada andmekaitse järelevalveasutuste tegevusi ning tagada tegevuste parem koordineeritus. Üldmäärus on adresseeritud ka liidule endale Euroopa Andmekaitsenõukogu ja Euroopa Andmekaitseinspektori büroo loomise ning Euroopa Komisjonile ja Euroopa Kohtule pandud täiendavate kohustuste kaudu. Veelgi enam, üldmäärus on kohaldatav piiriüleselt, hõlmates kogu liitu. Lisaks laieneb selle haare ka väljaspool EL-i asuvatele teenusepakkujatele: kui nende teenus on suunatud EL-i andmesubjektidele, peavad ka nemad täitma kõiki üldmäärusega ette nähtud kohustusi.[50]

---

[47] Euroopa Andmekaitsenõukogu. Suunised 1/2019 määruse (EL) 2016/679 kohaste toimimisjuhendite ja järelevalvet teostavate asutuste kohta versioon 2.0. (04.06.2019). - https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_et.pdf (10.04.2023).

[48] 23. oktoobri 2018. aasta Euroopa Parlamendi ja Nõukogu määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ. – ELT L 295/39, lk 39-98.

[49] 27. aprilli 2016. aasta Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK. – ELT L 119/89, 4.5.2016, lk 89-131.

[50] Rosentau, M. The General Data Protection Regulation and its Violation of EU Treaties. Juridica International, 27/2018, lk 36-37.

Kogu EL-is täielikult kohaldatav üldmäärus on maailma kõige põhjalikum ja progressiivseim andmekaitsealane õiguaskt, mida ajakohastati digitaalajastu tagajärgedega tegelemiseks.[51] Nii võivad näiteks Filipiinide kodanikule kohalduda Eestis viibides üldmääruse sätted vastavalt selle kohaldamisala määratlusele, mis on toodud üldmääruse artiklis 3. Üldmäärus kohaldub samuti äriühingutele, mis ei asu EL-is, kuid mis pakuvad kaupu EL-is elavatele isikutele või jälgivad nende liikumist (üldmääruse põhjenduspunkt 24).

Peamine erinevus üldmääruse ja selle kahe eelkäija[52] vahel on see, et OECD eraelu puutumatuse kaitset käsitlevates soovitustes sisalduvad varasemad andmekaitsepõhimõtted olid EL-i riikide jaoks vabatahtlikud. Direktiiv 95/46/EÜ nõudis liikmesriikidelt selle rakendamiseks siseriiklikke õigusakte, üldmäärus on aga Euroopa tasandil täielikult jõustatav (kuigi see sisaldab ka õigusaktide rakendamist liikmesriikide ja mõnikord ka piirkondlikul tasandil). Samuti võisid EL-i liikmesriigid direktiivi 95/46/EÜ kolmanda peatüki alusel määrata trahve oma äranägemise järgi, ilma nende trahvide alam- või ülemmäärata. Üldmääruse artikkel 83 lõike 5 kohaselt võivad trahvid kõige tõsisemate rikkumiste eest ulatuda kuni 20 miljoni euroni või 4 protsendini eelneva majandusaasta ülemaailmsest aastasest kogukäibest, olenevalt sellest, kumb on suurem.[53] On selge, et kaasaegse andmevoo keerukust ja uute tehnoloogiate (nt pilvandmetöötlus) arengut ei osatud 1995. aasta direktiivi 95/46/EÜ koostamisel ka ette näha, kuna nimetatud direktiivi rahvusvaheliste edastuste raamistik loodi teise ajastu jaoks.[54]

Eelnevast selgub, et üldmäärusel on oluline roll tänapäeva ühiskonnas, kuna selle eksterritoriaalne kohaldamine on praeguseks kasvavas trendis kaasa toonud suuri haldustrahve nii liikmesriikide kui kolmandate riikide ettevõtetele. Ettevõtete teadlikkus isikuandmete töötlemisel on seetõttu

[51] European Data Protection Supervisor. Data Protection. – https://edps.europa.eu/data-protection/data-protection_en (25.11.2022).

[52] Kuigi Euroopa Nõukogu Konventsioon nr 108 on alguse saanud juba 1981. Aastal, ei loeta seda üldmääruse eelkäijaks, kuna seda loetakse siduvaks ratifitseerinud riikidele, mitte ei määratleta selle kehtivust EL-I järgi. Vt: Euroopa andmekaitseõiguse käsiraamat. – Euroopa Liidu Põhiõiguste Amet ja Euroopa Nõukogu. Luxembourg: Euroopa Liidu Väljaannete Talitus, 2020, lk 29.

[53] Daigle, B. and Khan, M. The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities.– Journal of International Commerce and Economics, 06/2020, lk 5.

[54] Article 29 Data Protection Working Party Press release. The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data (02.12.2009). – https://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2009/pr_01_12_09_en.pdf (06.03.2023).

äärmiselt oluline. Üldmääruse olulisus andmekaitse tugevdamisel on aina olulisem, kuna digiajastul on andmete liikumine üha ulatuslikum.

Kokkuvõtvalt on üldmäärust peetud maailma kõige põhjalikumaks andmekaitsealaseks regulatsiooniks, mida kohaldatakse nii liidusiseselt kui ka väljaspool EL-i asuvatele andmetöötlejatele, kes pakuvad kaupu või jälgivad üksikisikute käitumist EL-is. EL andmekaitsestandardid on ranged ning nende piiriülese andmevoo reeglid on saanud eeskujuks teistes jurisdiktsioonides. Üldmäärus erineb oma eelkäijatest, kuna see on EL-i tasandil täielikult jõustatav ning selle rakendamisel on ekstraterritoriaalne mõju, mis on toonud ettevõtjatele kaasa märkimisväärsed trahvid. Üldmääruse olulisus andmekaitse tugevdamisel digiajastul on üha ilmsem ning ettevõtted peavad olema teadlikud oma kohustustest isikuandmete töötlemisel.

Eestis reguleerivad isikuandmete kaitset nii isikuandmete kaitse seadus[55] (IKS) kui ka üldmäärus. Üldmäärus otsekohalduva õigusaktina jõustus Eestis 2018. aasta 25. mail ja on mõeldud üheselt reguleerima andmekaitseõigust EL liikmesriikides ning on seetõttu kõrgema õigusjõuga ning selle sätted on kohustuslikud kõikidele liikmesriikidele. IKS jõustus 2019. aasta jaanuaris ning § 1 kohaselt täpsustab ja täiendab mõningaid üldmääruse sätteid, mille üldmäärus on jätnud liikmesriikide otsustada. Üldmäärus ning direktiiv 2016/680/EÜ on EL-i õigusaktid, mida kohaldatakse kõigis liikmesriikides, sh Eestis, samas kui IKS kehtib ja reguleerib isikuandmete töötlemist Eestis. Üldmääruse ja IKS-iga tutvudes on selge, et need kaks õigusakti sarnanevad oma põhimõtete ja nõuete poolest. Nii on mõlema eesmärk kaitsta isikuandmeid ja tagada, et neid töödeldakse õiglaselt ja seaduslikult. Üldmääruse mõju on üldisem ja ulatuslikum, kuna see kehtib kogu EL-is ning sisaldab palju rangemaid nõudeid andmete kaitseks ja töötlemiseks.

1.3. Üldmääruse territoriaalne kohaldamine isikuandmete edastamisel kolmandate riikide andmetöötlejatele

Nagu mainitud, võib üldmääruse artikli 3 alusel ulatuda selle kohaldamisala kaugemale EL-i territooriumist. Üldmäärust kohaldatakse artikkel 3 lõike 1 järgi liidus asuva vastutava töötleja või volitatud töötleja tegevuskoha tegevuse kontekstis toimuva isikuandmete töötlemise suhtes ning sõltumata sellest, kas töödeldakse liidus või väljaspool liitu. Sama artikli lõige 2 täiendab, et

[55] Isikuandmete kaitse seadus. – RT I, 04.01.2019, 11.

üldmääruse reeglid rakenduvad ka andmetöötlejale väljaspool liitu, kui töötlemine on seotud liidus asuvatele andmesubjektidele kaupade või teenuste pakkumisega kas tasu eest või tasuta või andmesubjekti käitumise jälgimisega ulatuses, milles see toimub Euroopa Liidus. Territoriaalse kohaldamisala järgimisel oluline silmas pidada, ega kolmanda riigi, kuhu isikuandmeid edastatakse, õiguskord ei kahjusta ega vähenda üldmäärusega ette nähtud isikuandmete kaitse taset.

Isikuandmete edastamisel kolmandate riikide andmetöötlejatele jääb andmete suhtes kehtima üldmäärus vastavalt territoriaalse kohaldamisala sättele üldmääruse artiklis 3, ent selline edastamine võib kaasa tuua suurenenud riske, millele juhib tähelepanu üldmääruse artikkel 44. Selle kohaselt kehtivad V peatükis sätestatud tingimused isikuandmete edastamise suhtes kolmandale riigile või rahvusvahelisele organisatsioonile. Sama artikkel reguleerib V peatüki üldeesmärki – tagada isikuandmete edastamisel kolmandatele riikidele üldmäärusega tagatud füüsiliste isikute kaitse tase.

Arvestades ettevõtluse globaalset arengut ja võimalusi, mida kasutatakse oma kulude haldamiseks, võib tegevuskoha täpne määratlus olla mõnes olukorras keerukas. Näiteks kohtuasjas C-230/14, *Weltimmo s.r.o. versus Nemzeti Adatvédelmi és Információszabadság Hatóság* leidis kohus, et tegevuskoha mõistet tuleb tõlgendada nii asukoha stabiilsuse kui ka tegutsemise tegelikkuse järgi liikmesriigis, võttes arvesse majandustegevuse ja teenuste osutamise konkreetset laadi konkreetses asjas, juhtides eraldi tähelepnu selle kohalduvuse osas ettevõtjate suhtes, kes tegelevad üksnes interneti teel teenuste osutamisega. Kohus juhtis tähelepanu, et tagada tuleks eraelu puutumatuse tõhus ja täielik kaitse ning vältida igasugust siseriiklikest eeskirjadest kõrvalehoidmist ning seega võib stabiilseks asukohaks piisata ainult ühe esindaja olemasolust, kui see tegutseb piisavalt stabiilselt, kasutades abivahendeid, mis on vajalikud asjaomaste konkreetsete teenuste osutamiseks, millega ta kõnealuses liikmesriigis tegeleb.[56] Kuigi tegevuskoha määratlust on Euroopa andmekaitseõiguses tõlgendatud pigem laialt, on kohtuasjas C-191/15, *Verein für Konsumenteninformation versus Amazon EU Sàrl* leitud, et tegevuskoha olemasolu ei saa eeldada pelgalt selle järgi, et ettevõtte veebisait on kättesaadav EL riigis.[57]

Liidus asuvate andmesubjektide mõiste üldmääruse artiklis 3 väljendab *expressis verbis* nende asumist, mitte elukohta, kodakondsust või muud määratlust, mis ühildub üldmääruse

[56] EKo C-230/14, *Weltimmo s.r.o. versus Nemzeti Adatvédelmi és Információszabadság Hatóság*. ECLI:EU:C:2015:639, punktid 29-30.
[57] EKo C-191/15, *Verein für Konsumenteninformation versus Amazon EU Sàrl*. ECLI:EU:C:2016:612, punkt 76.

põhjenduspunktis 14 toodud põhimõttega kaitsta üldmäärusega füüsilisi isikuid olenemata nende kodakondsusest või elukohast.

Oluline nüanss artikli 3 lõige 2 punktis a on ka see, et see ei viita kaupade müümise või teenuste osutamise faktile, vaid üksnes kaupade või teenuste pakkumisele. Probleemseks võib osutuda selle tõlgendus küsimuses, kas eelmainitud veebisaidi kättesaadavus EL liikmesriikides tähendab kaupade või teenuste pakkumist, et täidetud oleks territoriaalse kohaldamisala tingimus. Selle mõistmiseks on üldmääruse põhjenduspunkt 23 andnud mõned juhised: nimelt, et tagada võimalikult lai kaitse füüsilistele isikutele, kellel on õigus üldmääruse alusel väljaspool liitu asuva töötleja poolt liidus olevate andmesubjektide isikuandmete töötlemise suhtes, tuleks määrata kindlaks, kas on ilmne, et vastutav töötleja kavatseb pakkuda teenuseid ühe või mitme liidu liikmesriigi andmesubjektidele. Kuna üksnes juurdepääs vastutava või volitatud töötleja või vahendaja veebisaidile liidus, e-posti aadressile või muudele kontaktandmetele või vastutava töötleja asukohariigiks olevas kolmandas riigis üldiselt kasutatava keele kasutus ei ole piisav sellise kavatsuse kindlaks tegemiseks, võivad sellised tegurid nagu ühes või mitmes liikmesriigis üldiselt kasutatava keele või vääringu kasutus ning võimalus tellida kaupu ja teenuseid selles teises keeles ja/või liidus olevate klientide või kasutajate nimetamine muuta ilmseks asjaolu, et vastutav töötleja kavatseb pakkuda liidus sellistele andmesubjektidele kaupu või teenuseid. Toodud üldmääruse põhjenduspunkti 23 sõnastusest selgub, et oluline on vastutava töötleja kavatsus, mille osas Euroopa Andmekaitsenõukogu on leidnud, et selline kavatsus peab olema tahtlik ja mitte juhuslik.[58]

Artikli 3 lõike 2 punktiga b laiendatakse üldmääruse kohaldatavust Euroopa Liidus viibivate andmesubjektide isikuandmete töötlemisele vastutava töötleja või volitatud töötleja poolt, kes ei asu EL-is, kui töötlemistoimingud on seotud andmesubjektide tegevuse jälgimisega. Üldmäärus pakub mõningaid juhiseid selle seose tõlgendamiseks, märkides põhjenduspunktis 24, et selleks, et teha kindlaks, kas töötlemistoimingut saab pidada andmesubjektide käitumise jälgimiseks, tuleks kindlaks teha, kas füüsilisi isikuid jälgitakse internetis, sh isikuandmete töötlemise meetoditega, mille abil koostada füüsilise isiku profiile, eelkõige teda puudutavate otsuste tegemiseks või tema isiklike eelistuste, käitumise ja hoiakute analüüsimiseks või ennustamiseks. EDPB hinnangul tuleks arvesse võtta lisaks internetis jälgimise mõistele ka jälgimine muud tüüpi võrkude või

[58] European Data Protection Board. Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), 12.11.2019. - https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf, lk 15, (10.04.2023).

tehnoloogiate kaudu, mis hõlmavad isikuandmete töötlemist, näiteks kantavate ja muude nutiseadmete kaudu. EDPB on toonud välja valiku sellistest toimingutest, mis kvalifitseeruvad tegevuse jälgimise hulka, näiteks käitumuslik reklaam, geo-lokaliseerimistegevused eelkõige turunduseesmärkidel, veebi jälgimine küpsiste või muude jälgimistehnikate (nt sõrmejälgede võtmise) abil, isikupärastatud tervise-analüütika teenused võrgus, videokaamerate abil jälgimist, turu-uuringud ja muud individuaalsetel profiilidel põhinevad käitumisuuringud ning isiku tervisliku seisundi jälgimine või regulaarne aruandlus.[59]

Samas võib selline loetelu toimingutest jääda üsna üldiseks, kuna näiteks veebi jälgimine küpsiste abil võib hõlmata praktikas enda alla väga laia ulatust tegevusi, mille puhul alati ei saa järeldada koheselt väljaspool EL-i andetöötluse kvalifitseerimist üldmääruse alla, vaid tuleb kogumis hinnata erinevaid aspekte mitte niivõrd läbi jälgimise aspekti, vaid töötlemise sisu tervikuna. Teatav ebakindlus kohaldatavate eeskirjade suhtes võib seada aga ohtu ettevõtete ja üksikisikute õiguse teada, millised õigusnormid ning millistes olukordades neile kehtivad.

Võib spekuleerida, millises osas ja kui täpselt saab üldmääruse territoriaalse kohaldamise osas tõlgendada artiklit 3 koostoimes V peatüki artikliga 44, arvestades andmetöötlust liikmesriikide ja liiduväliste töötlejate vahel, kuna üldmääruse eesmärk on kaitsta isikute põhiõigusi, ent tänapäeva digitaalset arengut silmas pidades on sellise kaitse tagamine ja teisalt ka ülemäära laia mõjuulatuse piiramine kahtlemata keerukas.

Kokkuvõtlikult võib öelda, et üldmääruse territoriaalne kohaldamisala ei piirdu EL-i territooriumiga ja see kehtib ka andmetöötlejatele, kes ei ole asutatud EL-is, kuid on suunatud EL-is asuvatele üksikisikutele oma kaupade või teenuste pakkumisega või jälgivad nende käitumist EL-is. Andmete edastamine kolmandate riikide andmetöötlejatele võib aga andmekaitsele kaasa tuua täiendavaid riske ning selleks on vaja võtta täiendavaid meetmeid, nagu on sätestatud üldmääruse V peatükis. Kui andmetöötleja edastab isikuandmeid kolmandas riigis asuvale andmetöötlejale, peab andmeedastaja järgima nii üldmäärust kui ka siseriiklikult kehtivaid õigusakte, millest võib tekkida olukord, kus erinevate õigusaktide nõuded on teineteisega vastuolus. See on üks probleemidest, mida käesolevas töös uuritakse lähemalt teises peatükis.

[59] European Data Protection Board. Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), 12.11.2019. - https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf, lk 19, (10.04.2023).

1.4. Peamised mõisted seoses isikuandmete edastamisega kolmandate riikide andmetöötlejatele

Selleks, et käsitleda küsimusi seoses isikuandmete töötlemise ja edastamisega, peatutakse siinkohal vaid töös läbivalt kasutatud põhimõistetel nagu isikuandmed, töötlemine, sh isikuandmete edastamine. Nende mõistete sisu selgitamine aitab paremini mõista töö mastaapi. Vajadusel esitatakse vastavate teemakäsitluste juures ka teisi definitsioone.

Isikuandmete mõiste on üldmääruse mõistmisel ja ka käesoleva töö kontekstis kesksel kohal, kuna termin piiritleb ühtlasi õigusakti reguleerimisala. Isikuandmete mõiste on defineeritud üldmääruse artikli 4 punktis 1 ning selleks on igasugune teave tuvastatud või tuvastatava füüsilise isiku kohta. Näidete varal on samas punktis kirjeldatud, et tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige sellise identifitseerimistunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või selle füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal. Seega, kui teave kuulub isikuandmete määratluse alla ning üldmääruse materiaalsed ja territoriaalsed sätted on täidetud, kehtivad selle kindlad nõuded.

Isikuandmete töötlemise mõiste on defineeritud üsna laia sõnastusega üldmääruse artikli 4 punktis 2. Oluline on märkida, et isikuandmete töötlemine tähendab sisuliselt kõiki isikuandmetega tehtavaid toiminguid, nii hõlmab see viidatud sätte kohaselt isikuandmete või nende kogumitega tehtavaid automatiseeritud või automatiseerimata toiminguid nagu kogumine, dokumenteerimine, korrastamine, struktureerimine, säilitamine, kohandamine ja muutmine, päringute tegemine, lugemine, kasutamine, edastamise, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine, ühitamine või ühendamine, piiramine, kustutamine või hävitamine.

Eelnevast selgub, et isikuandmete edastamine nii riigi- kui liidusiseselt ja ka väljaspool EL-i on töötlemistoiming, millele rakenduvad üldmääruses töötlemise kohta käivad sätted. Selliseid töötlemistoiminguid võib läbi viia füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes tegutseb vastutava töötleja või volitatud töötlejana.

Andmeedastust ja -analüüsi on igapäevaselt inimeste ümber palju rohkem, kui seda sageli teadvustatakse. Nii võib IP-aadresse ja küpsiseid (*cookies*) teatud asjaoludel pidada

isikuandmeteks.[60] IP-aadressi saab kasutada isiku tuvastamiseks, eriti kui see on kombineeritud muude andmetega, nagu asukoht või võrgutegevus. Samamoodi võivad küpsised sisaldada teavet, mida saab kasutada isiku tuvastamiseks, näiteks tema eelistused või sirvimisajalugu.[61] Rahvusvaheline turu-uuringute ettevõte International Data Corporation prognoosib, et 2025. aastaks ulatub globaalne andmeloome tänasest kolmveerandi võrra suuremate andmemahtudeni, kusjuures suur osa neist andmetest on loodud internetiseadmete ja sotsiaalmeedia kaudu.[62] Andmetöötlus, sh ka andmetele ligipääsu andmine (mis on töötlemistoiming üldmääruse artikli 4 punkt 2 tähenduses) näiteks Google Analyticsi vahendile internetikasutajate käitumise ja profiili loomisel, on lahutamatuks osaks tavapärastest äriprotsessidest.[63] Siiski ei pruugi internetikasutaja teadvustada, kuidas tema tegevus arvutis võib olla ühendatud läbi IP aadressi ja küpsiste kokku üheks profiiliks ning mõjutada teda tulevikus ka teda puudutavate otsuste tegemisel. Nii võivad olla kindlustusfirmale tervisekindlustuse taotluste hindamise aluseks näiteks nutikellast kogutud terviseandmed, mis võib põhjustada erineva kindlustusmakse määramist kahe sarnase tervisliku taustaga inimese jaoks. Tänapäeva tehnoloogia võimaldab kasutada kogutud andmeid otsuste tegemiseks juba praegu, mistõttu on oluline, et andmekaitsealases määratluses oleks üheselt mõistetud isikuandmetena käsitletavate andmete tähendus, et vältida privaatsusprobleeme ja selle ootamatuid tagajärgi.

Üldmääruses puudub isikuandmete kolmandale riigile või rahvusvahelisele organisatsioonile edastamise mõiste. EDPB on kindlaks määranud kolm kriteeriumi, mis kumuleerituna viitavad sellisele üleandmisele:

1) vastutav või volitatud töötleja (andmete edastaja) suhtes kohaldatakse töötlemise puhul üldmäärust;
2) andmeedastaja edastab või teeb isikuandmed kättesaadavaks teisele andmetöötlejale (vastutavale töötlejale, kaasvastutavale töötlejale või volitatud töötlejale);

[60] 2022. aasta uuringus üldmääruse eksterritoriaalsusega seotud regulatiivsete mõjude kohta globaalses andmemajanduses on analüüsitud mh küpsiste (*cookies*) kui isikuandmete kasutamist andmeanalüütikas, samuti on toodud välja veebisaitide kolmandatest isikutest andmetöötlejate suur arv. Vt: Peukert, C. jt. Regulatory spillovers and data governance: Evidence from the GDPR. – Marketing Science, 41(4), 2022, lk 747, 749, 755.

[61] Sanchez-Rola, I. jt. Can i opt out yet? GDPR and the Global Illusion of Cookie Control. – In Proceedings of the 2019 ACM Asia conference on computer and communications security. 07/2019, lk 341.

[62] Rydning, J., Reinsel, D., Gantz, J. The digitization of the world from edge to core. – Framingham: International Data Corporation. 11/2018, lk 3.

[63] Vt Google Analytics´i kohta täpsemalt näiteks: Chai, W. Google Analytics. Tech Target, Business Analytics. (04/2021). - https://www.techtarget.com/searchbusinessanalytics/definition/Google-Analytics, (10.04.2023). Google´i turuosa suurenemisele viitab 2022. aasta uuring, vt: Peukert, C. jt., lk 747.

3) andmetöötleja asub kolmandas riigis, olenemata sellest, kas tema suhtes kohaldatakse artikli 3 kohaselt üldmäärust või mitte, või on tegemist rahvusvahelise organisatsiooniga.[64]

Kui nimetatud kolm EDPB poolt määratud kriteeriumi on täidetud, toimub andmete edastamine ja kohaldatakse üldmääruse V peatükki, mille eesmärk on tagada isikuandmete jätkuv kaitse pärast nende edastamist kolmandale riigile või rahvusvahelisele organisatsioonile. See tähendab, et andmeedastus võib toimuda ainult teatud tingimustel, näiteks Euroopa Komisjoni piisavuse kohta tehtud otsuse kontekstis (üldmääruse artikkel 45) või asjakohaste kaitsemeetmete rakendamisel (üldmääruse artikkel 46). Ja vastupidi, kui kolm kriteeriumi ei ole täidetud, siis üleandmist ei toimu ja üldmääruse V peatükk ei rakendu.[65]

Isikuandmete edastamine kolmandate riikide andmetöötlejatele toimub üldmääruse artiklite 44-50 alusel. Üldreegel on see, et andmeid võib edastada juhul, kui on rakendatud nõuetekohased kaitsemeetmed ning on olemas õiguslik alus vastavalt üldmääruse artiklile 6 või 9 (näiteks andmesubjekt on andnud edastamiseks nõusoleku konkreetsel eesmärgil, töötlemine on vajalik lepingu täitmiseks jms). Pikemalt käsitletakse isikuandmete edastamist töö järgnevates peatükkides.

1.5. Kaitsemeetmete eesmärk isikuandmete kaitsel

Andmeedastus on üks viise, kuidas isikuandmeid kogutakse ja jagatakse. Võib öelda, et andmed on maailmamajanduse oluline liikumapanev jõud, mis mängib kogu majanduses ja paljudes äristrateegiates keskset rolli. Lähtudes eelnevast ja tuginedes üldmääruse V peatükile saab väita, et mitte kõikide riikide vaheline isikuandmete vahetus ei ole vaba, vaid teatud juhud on reguleeritud andmeedastuspiirangutega, mille tingimused on välja toodud üldmääruse V peatükis, eelkõige artiklis 46, ning mida tuleb tõlgendada koostoimes kohtupraktika ja EDPB juhistega. Käesolevas peatükis tuuakse välja üldmääruse kaitsemeetmete regulatsiooni eesmärgid ning ka nendega seotud problemaatika.

[64] European Data Protection Board. Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR. (14.02.2023). – https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_en, lk 3. (11.03.2023).
[65] *Ibidem*, lk 3.

Andmete turvalisele töötlemisele (s.t. ka edastamisele) on viidatud üldmääruse II peatükis isikuandete töötlemise põhimõtete juures (artikkel 5 lõige 1 punkt f) ja IV peatüki artikli 32 lõikes 2 eesmärgiga kaitsta isikuandmete juhuslikku või ebaseaduslikku hävitamist, kaotsiminekut, muutmist ja loata avalikustamist või neile juurdepääsu. Viidates andmeedastuse piirangutele, on nii direktiivis 95/46/EÜ, üldmääruses kui ka konventsioonis nr 108 silmas peetud isikuandmete edastamispiiranguid andmete edastamisel EL-väliste riikide andmetöötlejatele. Isikuandmete liikumist EL-i piires üldmäärus selliselt ei keela.

Selleks, et tagada isikuandmete kaitse põhimõtte rakendamine ka väljaspool EL-i, keelab üldmäärus vaikimisi vastutavatel ja volitatud töötlejatel isikuandmete edastamise väljapoole EL riike. Andmete edastamine kolmandate riikide andmetöötlejale on üldmääruse artikli 44 kohaselt lubatud juhul, kui vastuvõttev riik tagab isikuandmetele piisava kaitsetaseme. Üldine V peatüki eesmärk on tagada, et isikuandmete edastamisel kolmandate riikide andmetöötlejatele või rahvusvahelistele organisatsioonidele ei kahjustataks üldmäärusega tagatud kaitse taset.[66] Selline põhimõte on kooskõlas Euroopa Parlamendi ja Nõukogu sätestatud rahvusvahelise andmeedastuse eesmärgiga. Üldmääruse põhjenduspunktid 101 ja 104 rõhutavad isikuandmete edastamise olulisust kolmandate riikide andmetöötlejatele kaubanduse ja koostöö eesmärgil, rõhutades, et samal ajal tuleb tagada piisav andmekaitse tase, mis vastab EL-is tagatava kaitse tasemele, ning arvestatakse põhiõiguste olulisust. Eesmärki tagada isikuandmete kaitse nende edastamisel kolmandate riikide andmetöötlejatele kandis endas ka üldmääruse direktiivi 95/46/EÜ artikkel 25 lõige 1, mistõttu ei peatuta siinkohal pikemalt nimetatud direktiivi põhimõtetel.

Lisaks üldmäärusele näeb konventsiooni nr 108 artikkel 12 ette, et üks selle osaline ei tohi keelata isikuandmete automatiseeritud töötlemisel selle piiriülest voogu, mis läheb teise osalise territooriumile. Nimetatud artikkel kehtestab seega andmete vaba liikumise põhimõtte konventsiooniosaliste vahel ja läheneb andmeedastuse piirangule läbi andmete edastamise vabaduse. Kaudselt käsitletakse ka isikuandmete edastamist vastuvõtjatele[67], kes ei kuulu konventsiooniosalise jurisdiktsiooni alla – konventsiooni artikli 12 lõikes 3 on sätestatud, et osalisel on õigus piirata andmete edastamist, kui edastatakse tema territooriumilt lepinguosalise

[66] *Ibidem*, lk 5.

[67] Andmete vastuvõtja tähendab käesolevas töös kolmandas riigis asuvat vastutavat või volitatud andmetöötlejat, kellele edastab isikuandmeid EL-i andmetöötleja. Õiguskirjanduses kasutatakse ka mõistet andmeimportija ning andmete edastaja kohta andmeeksportija mõistet.

riigi territooriumile teise lepinguosalise territooriumi vahendusel, et vältida selliseid üleandmisi, mille tulemuseks on andmeid edastava riigi õigusaktidest kõrvalehoidmine.

Konventsiooni nr 108 laiendatud versioon aastast 2018 – konventsioon nr 108+ artikkel 14 kinnitab isikuandmete vaba liikumise põhimõtet ühelt konventsiooni-osaliselt teisele konventsiooni-osalisele (vastuvõtjale, kes allub teise osalisriigi jurisdiktsioonile), sätestades, et kui vastuvõtja allub sellise riigi või rahvusvahelise organisatsiooni jurisdiktsioonile, mis ei ole käesoleva konventsiooni osaline, võib isikuandmete edastamine toimuda ainult siis, kui on tagatud käesoleva konventsiooni sätetel põhinev asjakohane kaitsetase.[68] Sellise tingimuse eesmärk tagada, et konventsiooni osalisriigi pakutava kaitse taset ei kahjustata pärast andmete riigist lahkumist. Kõrvalehoidmise vastane eesmärk tuleneb ka üldmääruse artikli 44 viimasest lausest, mille järgi kohaldatakse kõiki sätteid andmete edastamise kohta väljapoole EL-i selleks, et määrusega tagatud füüsiliste isikute kaitse taset ei kahjustataks.

Seega on välja joonistunud kaks andmeedastuse piirangute eesmärki – esiteks tagada kaitse tase sõltumatult sellest, kuhu andmed liiguvad ning teiseks – kõigile andmeahelas osalevatele andmetöötlejatele kohalduvate piirangute läbi välistada, et andmetöötlejal tekiks huvi viia andmed liidust välja eesmärgiga neid seal vabalt töödelda.

Eeltoodut silmas pidades võib järeldada, et andmete edastamispiirangud üldmääruse artiklis 46 on sätestatud nii direktiivi 95/46/EÜ alusel kui selle asendanud üldmääruse kohaselt, et tagada isikuandmete kaitse tase kolmandates riikides vastavalt EL-i andmekaitsealaste õigusaktidega kehtestatud põhimõtetele olukorras, kus riigil puudub Euroopa Komisjoni kaitse piisavuse otsus.

Ka Euroopa Komisjon väljendas oma teatises Euroopa Parlamendile ja Nõukogule 2017. aastal, et rahvusvahelise andmeedastuse peamiseks eesmärgiks on tagada, et kui eurooplaste isikuandmeid edastatakse väljapoole Euroopa Liitu, läheb isikuandmete kaitse andmetega kaasa. Lisaks märkis komisjon: „Privaatsuse tagamine on stabiilsete, turvaliste ja konkurentsivõimeliste globaalsete kaubavoogude eeltingimus. Privaatsusega ei saa kaubelda.“[69] Seega on andmetöötleja, kes kogub andmeid esmalt EL-is asuvatelt andmesubjektidelt ja edastab need seejärel kolmanda riigi vastutavale või volitatud töötlejale, kohustatud tagama andmete edastamisel kaasneva kaitse

[68] Council of Europe. Convention 108+: Convention for the Protection of Individuals with Regard to the Processing of Personal Data. 2018. - https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (24.03.2023).

[69] Euroopa Komisjoni teatis Euroopa Parlamendile ja Nõukogule. Isikuandmete vahetamine ja kaitsmine globaliseerunud maailmas. – 2017 COM/2017/07 final, 10.01.2017, punkt 2.2. ja 3.

andmetega. [70] Seda põhimõtet võib pidada ilmselt kõige olulisemaks eesmärgiks, miks igasugune andmeedastus ei ole vaba ja piiramatu.

Olgugi, et eesmärk andmekaitse taseme osas näib olevat selge, võib selle praktikas järgimisel tekkida probleeme. Andmete kolmandate riikide andmetöötlejatele edastamisel on nõutav mõlemal poolel kaks erinevat andmetöötlejat. Sellise edastamise õiguslikud aspektid hõlmavad mõningaid keerukusi – nimelt andmeedastaja on kohustatud järgima EL-i andmekaitsealaste õigusaktide sätteid, kuna talle kohaldub andmeid kogudes ja töödeldes üldmäärus. Kuid andmeid vastuvõtva andmetöötleja suhtes kohaldatava õiguse üle võivad tekkida vaidlused, kuna lisaks isikuandmete saamisega kohalduvatele nõuetele tuleb järgida tal ka siseriiklikku õigust, mis ei pruugi olla kooskõlas EL õigusega ja võetud lepinguline kohustus tagada andmeedastajaga kokkulepitud kaitsemeetmeid muutuks sellisel juhul võimatuks.[71] Samale probleemile on käesolevas töös viidatud territoriaalse kohaldamisala käsitluse juures ning ka edaspidi.

Liikudes õigusaktidest kohtupraktika juurde, on Euroopa Kohus andmete edastamispiirangute eesmärke sõnastatud ka kohtupraktikas. *Schrems I* punktis 73 märkis Euroopa Kohus, et EL-i põhiõiguste hartat silmas pidades ja otsuse ajal kehtinud direktiiviga 95/46/EÜ tagatud kõrgetasemelisest kaitsest saaks kergesti mööda hiilida isikuandmete edastamisega kolmandate riikide andmetöötlejatele nendes riikides töötlemise eesmärgil, kui andmetöötluse reeglid kehtiksid vaid EL-is.

Schrems II kohtuasja kohtujuristi[72] ettepaneku punkt 117 väljendab nii üldmääruse artiklite 45 ja 46 eesmärki – kindlustada isikuandmete kõrgetasemelise kaitse järjepidevus andmete edastamise korral väljapoole liitu.[73] Ka üldmääruse artikli 44 eesmärk on vältida liidu õigusest tulenevatest kaitsestandarditest mööda hiilimist seeläbi, et isikuandmed edastatakse kolmandasse riiki selleks,

[70] European Data Protection Board. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Version 2.0, 18.06.2021. https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf, lk 3, (10.04.2023).

[71] Bu-Pasha, S. Cross-border issues under EU data protection law with regards to personal data protection. Information & Communications Technology Law, 2017, 26(3), lk 214-215.

[72] Kohtujurist (ingl *advocate general*) on kohtunik, kes abistab Euroopa Liidu Kohut selle ülesannete täitmisel. Kohtujurist vastutab täiesti erapooletult ja sõltumatult arvamuse esitamise eest talle määratud kohtuasjade kohta. Selgitused: Advocate general of the CJEU, (07.07.2020). Eurofound. - https://www.eurofound.europa.eu/observatories/eurwork/industrial-relations-dictionary/advocate-general-of-the-cjeu (05.02.2023).

[73] EK C-311/18, *Data Protection Commissioner versus Facebook Ireland Limited, Maximillian Schrems*, kohtujurist Saugmandsgaard Øe, H. ettepanek, punkt 117.

et neid seal töödelda.[74] Seda eesmärki silmas pidades ei ole vahet, millisel õiguslikul alusel andeedastus toimub, kuna hartaga tagatud põhiõiguste kaitse nõudeid ei eristata lähtudes sellest, millisel õiguslikul alusel konkreetne edastamine toimub. Andmete edastamise õiguslikust alusest sõltuvalt erineb seevastu aga viis, kuidas kõrgetasemelise kaitse järjepidevus tagatakse.[75]

Viidatud välistused tekitavad küsimuse, kas isikuandmete edastamine ilma kaitse piisavuse otsuseta riikidesse, s.t. üldmääruse artikli 46 kaitsemeetmete rakendamisel, sõlmides andmeedastuseks poolte vahel andmeedastuslepingu, on piisav ja suudab kanda üldmääruses ette nähtud andmete kaitse eesmärki. Kui kaitsemeetmeid ei ole võimalik järgida, on vastutav andmetöötleja kohustatud andmete edastamise peatama või lõpetama lepingu, mis võimaldas andmete edastamist kolmandasse riiki (*Schrems II* punkt 3 ja 135). Praktikas on keeruline saavutada olukorda, kus andmeedastaja analüüsiks ennetava meetmena läbi kõikide andmete sihtriikide seadusandlused, et olla kindel, et andmeid vastuvõtvale andmetöötlejale edastatud andmete kaitse on ka siseriikliku õigusega kooskõlas. Sellises olukorras võib aga näha ühte põhilist probleemi, miks andmekaitse kõrge tase, mida üldmäärusega soovitakse hoida riikide üleselt, ei pruugi olla praktikas tagatud.

Kokku võttes eelnevat, on andmeedastuse piirangute peamiseks eesmärgiks nii üldmääruse, selle eelkäija, direktiivi 95/46/EÜ kui ka konventsiooni nr 108 ja 108+ kohaselt tagada, et kui eurooplaste isikuandmeid edastatakse väljapoole EL-i, liigub isikuandmete kaitse andmetega kaasa ning teiseks, kõigile andmeahelas osalevatele andmetöötlejatele kohalduvate piirangute läbi välistada, et andmetöötlejal tekiks huvi viia andmed liidust välja eesmärgiga neid seal vabalt töödelda. Lisaks eelnevale võib näha andmekaitse-eeskirjade kehtestamisel ka soovi ja vajadust kaitsta isikuandmeid välisriikide ametiasutuste sekkumise eest. Siiski võib kaitse-eesmärkide täitmine olla praktikas keeruline – andmetetöötleja kolmandas riigis, kes on andmeedastajaga koostöös kohustatud täitma üldmääruse sätteid, ei saa jätta täitmata siseriikliku õigusega pandud kohustusi. Lepingu ja üldmäärusega sätestatud kohustuste ning sihtkohaks oleva riigi õigusest tulenevate nõuete vaheline kollisioon muudab küsitavaks andmete kõrgetasemelise kaitse pärast andmete EL-ist lahkumist.

[74] Vt ka EKo C-362/14, *Schrems*, punkt 73.
[75] EK C-311/18, *Data Protection Commissioner versus Facebook Ireland Limited, Maximillian Schrems*, kohtujurist Saugmandsgaard Øe, H. ettepanek, punktid 117-118.

2. Kaitsemeetmete tähendus ja nende rakendamisega kaasnev problemaatika

2.1. Kaitsestandardi määratlus ja õigusselgus üldmääruses

Üldmäärus tunnistab ka kõrgetasemelise andmekaitse tagamise tähtsust isikuandmete edastamisel kolmandate riikide andmetöötlejatele (üldmääruse artiklid 44–50). Isikuandmete edastamisel kolmandate riikide andmetöötlejatele liigituvad riigid EL-i väliselt esmajoones selle järgi, kas riik on saanud Euroopa Komisjonilt andmekaitse taseme piisavuse otsuse üldmääruse artikkel 45 järgi või mitte.[76]

Üldmääruse V peatükis isikuandmete edastamiseks kolmandatele riikidele ja rahvusvahelistele organisatsioonidele on loodud kolmeastmeline struktuur andmete kaitse loetelus.[77] Ettevõtete-vahelise andmeedastuse korral EL-ist kolmanda riigi andmetöötlejale on üldmääruse V peatüki isikuandmete turvalise edastamise alusteks kolm võimalikku viisi toodud järjestuses:

I. Edastamine Euroopa Komisjoni otsuse alusel, kui komisjon on leidnud, et riik või organisatsioon tagab isikuandmete piisava kaitse (üldmääruse artikkel 45).
II. Edastamine asjakohaste kaitsemeetmete kohaldamisel (üldmääruse artikkel 46, s.t. standardsete andmekaitseklauslite kasutamine, siduvate kontsernisiseste eeskirjade kasutamine (üldmääruse artikkel 47), komisjoni poolt kontrollimenetluse kohaselt vastu võetud standardsete andmekaitseklauslite alusel, järelevalveasutuse poolt vastu võetud ja komisjoni poolt kontrollimenetluse kohaselt heaks kiidetud standardsete andmekaitseklauslitega, toimimisjuhendiga, sertifitseerimismehhanismiga ning *ad hoc* lepinguklauslitega).
III. Erandite rakendamine konkreetses olukorras (üldmääruse artikkel 49).

Üldpõhimõtetele üldmääruse artiklis 44 järgneb esmalt üldreegel artiklis 45 selle kohta, et isikuandmete edastamine kolmandale riigile või rahvusvahelisele organisatsioonile võib toimuda ainult Euroopa Komisjoni otsuse alusel kolmanda riigi piisava kaitse taseme kohta. Üldmääruse

[76] Andmekaitse inspektisoon. Andmete edastamine välisriiki. (21.06.2021) - https://www.aki.ee/et/teenused-poordumisvormid/andmete-edastamine-valisriiki (30.03.2023).
[77] Kuner, C jt. The EU General Data Protection Regulation: A Commentary/Update of Selected Articles. – Update of Selected Articles, 04.05.2021, lk 159.

artikli 46 kohaselt ei pea sellisel juhul töötlemistoiminguks täiendavaid tingimusi (nt eriluba taotlema) rakendama. Kui isikuandmete edastamine toimub riikidesse väljaspool Euroopa Liitu, tuleb seega esmalt kindlaks teha, millisele andmekaitsetasemele riik vastab ja vastavalt sellele järgida nõudeid.

Kui selline piisavuse otsus, nagu on kirjeldatud üldmääruse artiklis 45, puudub, võib üldmääruse artikli 46 alusel vastutav töötleja või volitatud töötleja edastada isikuandmeid kolmanda riigi andmetöötlejale üksnes juhul, kui vastutav töötleja või volitatud töötleja on sätestanud asjakohased kaitsemeetmed nagu eelpool loetletud punktis 2. Üldmääruse artikkel 49 lõige 1 sätestab, et piisavuse otsuse puudumisel või asjakohaste kaitsemeetmete puudumisel, sh üldmääruse artiklis 47 sätestatud siduvate kontsernisiseste eeskirjade puudumise korral, võib andmeedastus toimuda sättes loetletud erandite alusel. Seega on erandite kasutamise eeltingimuseks asjaolu, et edastataval riigil puudub üldmääruse artikli 45 kohane otsus ja artikli 46 tingimused ei ole rakendatavad, olles rakendatavate meetmete osas järjekorras kolmandal kohal ning seda ainult piiratud juhtumitel.

Järgnevalt tuuakse välja, kuidas, s.t. milliseid termineid kasutades, on üldmääruses kirjeldatud eel-loetletud kolme peamist edastamise viisi, et tuua välja mõistete selgus õiguse rakendajale – andmete edastajale. Selleks on võrdlusena eestikeelsele üldmäärusele kasutatud inglisekeelset üldmääruse teksti, kuna nendes esinevad terminite kasutusel eestikeelses versioonis mõned erisused ning terminite erinevuste korral on aluseks võetud inglisekeelne originaaltekst.[78]

Üldmääruse kaitsemeetmete väljatöötamisel on olnud roll *Schrems I* kohtuotsusel ning *Schrems II* kohtuotsus on mõjutanud kaitsemeetmete tõlgendamist, siis avatakse käesolevaga ka mõned aspektid kohtulahenditest, mis on mõjutanud kaitsestandardi tõlgendamist. Edastamise tingimuste sõnastuse uurimine aitab käesoleva töö raames välja tuua problemaatikat kaitsemeetmete õigusliku tõlgendamise ja rakendamise osas. Üldmääruse V peatüki üldise kaitsestandardi kirjeldamise järel on teise peatüki peamine eesmärk keskenduda artikli 46 asjakohaste kaitsemeetmetega seotud küsimustele selle rakendamise ja samaväärse kaitse taseme saavutamisele, ent kaitsestandardi mõistmine üldiselt, kohtupraktika ja kontseptsiooni mõistmine aitab paremini esile tuua töö temaatikat.

[78] Eestikeelne üldmääruse tekst on tõlgitud selle esialgsest tekstist. Kuna tõlke tulemusel ei ole kõik terminid tõlgitavad ja tõlgitud samade vastetega, esineb inglisekeelses üldmääruse tekstis nende täpne vaste. Seega on võrdluse aluseks kohane võtta ja arvestada ka inglisekeelse üldmääruse tekstiga. Vt ka: Antonova, J. Euroopa andmekaitsereformist läbi keeleprisma. - Õiguskeel 1/2015.

Üldmääruse V peatükk kasutab vähemalt nelja erinevat väljendit, et kirjeldada rahvusvahelisel andmeedastusel, s.t. isikuandmete edastamisel kolmandate riikide või rahvusvaheliste organisatsioonide andmetöötlejatele, nõutavat kaitsestandardit. Kõige sagedamini kordub piisava kaitsetaseme nõue (ingl k. *adequate level of protection*), mida kasutatakse üldmääruse artiklis 45 ja millele viitavad üldmääruse põhjenduspunktid nr 102-104, 107, 168-170. Üldmääruse V peatüki teistes sätetes on ka sellised mõisted nagu asjakohased kaitsemeetmed (ingl k. *appropriate safeguards)*, mida on kasutatud V peatüki artiklis 46 toodud kaitsemeetmete kirjeldamiseks (lisaks sisaldub asjakohaste kaitsemeetmete termin ka üldmääruse põhjenduspunktides 102, 107, 108, 110 ja artikli 13 lõike 1 punktis f, artikli 14 lõike 1 punktis f, artikli 15 lõikes 2, 40, 41 lõiget 4, artikli 42 lõikes 2, 46, ja 50; muude, edastamisega mitteseotud sätete kontekstis ka üldmääruse põhjenduspunktides 50, 52, 56, 62, 71, 74, 78, 156 ja 157 ning artikli 6 lõike 4 punktis e, artikli 9 lõige 2 punktis b, artiklites 10, 58 lõige 4, 87 ja 89), sobiv kaitsetase (ingl k. *appropriate level of protection),* mis on esitatud üldmääruse inglisekeelse versiooni põhjenduspunktis 102; ning sobivad kaitsemeetmed (ingl k. *suitable safeguards),* mida on kasutatud üldmääruse V peatüki artiklis 49 toodud erandite kohaldamisel (lisaks ka üldmääruse põhjenduspunktides 113 ja artikkel 13 lõike 1 punktis f; artikkel 14 lõike 1 punktis f; artikkel 30 lõike 1 punktis e, artikkel 30 lõike 2 punktis c; lisaks muude, edastamisega mitteseotud sätete kontekstis ka inglisekeelse üldmääruse teksti põhjenduspunktides 52 ja 71).

Huvitav on ka asjaolu, et üldmääruse artiklis 44, mis käsitleb edastamise üldpõhimõtteid, ei mainita mõistet „piisav kaitsetase" (*adequate level of protection*), vaid selle asemel kasutatakse piisava kaitsetaseme mõistet vaid isikuandmete edastamisel, mis põhineb komisjoni kaitse piisavuse otsusel üldmääruse artiklis 45.

Eelnevast selgub, et üldmääruses on kasutatud isikuandmete rahvusvaheliseks edastamiseks nõutavate kaitsemeetmete kirjeldamiseks erinevaid mõisteid olenevalt edastamise meetmest. Selline erinevate mõistete kasutamine erinevates V peatüki artiklites võib tekitada segadust andmetöötlejale nende mõistete eristamise osas, samuti küsimust, milles seisneb toodud terminite erinevus.

Vaadeldes kohtupraktikast tulenevat sõnastust üldmääruse V peatüki kaitsestandardi kirjeldamiseks, siis *Schrems I* otsusest 2015. aastal on tulenenud mõningane sõnastus üldmääruse V peatüki kaitsemeetmete sõnastamisel. Kaitse piisavuse otsus üldmääruses kordab nimelt *Schrems I* otsust, et need peavad vastama sisulise samaväärsuse standardile ja teisest küljest rõhutab see

üldpõhimõtet, mis reguleerib kõiki rahvusvahelisi andmeedastusi, mis aga ei kujuta endast eraldiseisvat alust andmete edastamise jaoks.[79] *Schrems II* kohtuotsuses, mis jõustus üldmääruse kehtivuse ajal, on kohus tuvastanud, et igat tüüpi ülekannete puhul tuleks saavutada sisuliselt samaväärne kaitsestandard (*Schrems II* punktid 94, 96-97, 105). Sellisele põhimõttele vastab ka üldmääruse inglisekeelne põhjenduspunkt 104. Kuigi üldmääruse V peatükk ei kasuta „sisuliselt samaväärse kaitse" või „samaväärse kaitsestandardi" terminit, on seda terminit kasutatud kaitse piisavuse otsuse ja andmekaitse tüüptingimuste alusel toimuva andmeedastuse tõlgendamisel nii kohtuotsustes (*Schrems I* punktid 73 ja 96; *Schrems II* punktid 105, 162) kui EDPB andmetöötluse juhistes[80].

Z. Gulczyńska sõnul on Euroopa Kohus sooritanud samaväärse kaitsetaseme, piisava kaitsetaseme ja asjakohaste kaitsemeetmete võrdsustamisel keerulist õigusvõimlemist, mis on tekitanud uusi küsimusi ja kahtlusi ning eelkõige seab see kahtluse alla EL-i õiguse tõlgendamise, mille kohaselt EL-i seadusandja on tegutsenud mõistlikkuse põhimõttel, luues eeskirju ning tagades sellega järjepidevuse ja täielikkuse ning vältides dubleerimist. Selline tõlgendus nõuab muu hulgas eeldamist, et (ühe instrumendi piires) ei ole erinevatel terminitel sama tähendust ja vastupidi, ühel terminil ei saa olla kahte erinevat tähendust.[81] Käesoleva töö autor nõustub sellega, et üldmääruse V peatüki kaitsemeetmete kohta käivas regulatsioonis orienteerumine, õigusliku tõlgenduse ja erinevate terminite mõistmine võib andmetöötlejale olla väga koormav, seda enam, et andmetöötluse reeglite tõlgendamine ei ole üldiselt ettevõtja peamine eesmärk, vaid pigem kohustus. Samuti leiab töö autor, et erinevate terminite kasutamine ühtse kaitsestandardi kirjeldamiseks tekitab pigem segadust kui õigusselgust.

Seoses keerukate andmeedastuse reeglite järgimisega nii nende sõnastuse kui sisu tõlgendamisel, on 1995. aasta direktiivis 95/46/EÜ sätestatud andmeedastuseeskirju kritiseeritud ning oletatavalt on ettevõtted neid ka eiranud, kuigi reeglite mittejärgimist ei ole statistiliselt kuigi lihtne tuvastada. Euroopa Komisjon tunnistas andmekaitseasutuste võetud jõustamismeetmete nõrkust 2003. aastal,

[79] Gulczyńska, Z. A certain standard of protection for international transfers of personal data under the GDPR. - International Data Privacy Law, 11(4), 11/2021, lk 364.
[80] European Data Protection Board. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Version 2.0, (18.06.2021). – https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf, (10.04.2023).
[81] Gulczyńska, Z. A certain standard of protection for international transfers of personal data under the GDPR. - International Data Privacy Law, 11(4), 11/2021, lk 361.

andes märku paljudest volitamata ja ebaseaduslikest andmeülekannetest sihtkohtadesse, mis ei taga andmete piisavat kaitset. Kuigi otseste tõendite kogumine direktiivile 95/46/EÜ mittevastavuse kohta oli raske, tulenes mittevastavus mõningatest kaudsetest tõenditest: andmeedastuste maht oli suurenenud nimetatud direktiivi jõustumise järgselt ja paljud neist edastustest tuli seega ilmselt läbi viia muul viisil kui andmeedastusreeglite rakendamisel. Nõuetele mittevastavus võis tuleneda ka andmeid edastavate ettevõtete vähesest teadlikkusest. Nii nagu kasutajad ei pruukinud olla teadlikud andmeedastustest, mida nad "käivitasid", ei pruukinud klientide andmeid töötlevad ettevõtted olla teadlikud nendest tulenevatest juriidilistest kohustustest andmeedastuste osas.[82] Kuigi mõningaid 1995. aasta direktiiviga 95/46/EÜ seotud probleeme on lahendatud üldmääruse asendumise, kohtupraktika ja Euroopa institutsioonide juhistega, võivad sarnased küsimused tänapäeval jätkuda, kuna ettevõtted peavad leidma võimalusi tagada andmete piisav kaitse, ent mis on sageli aja- ja rahamahukas protsess ning nõuab eriteadmisi.

Eelnevat arvestades võib öelda, et üldmääruse V peatükk seab andmete kaitse osas kõrge taseme, ent ka vajaliku eesmärgi: isikuandmete edastamine kolmandate riikide andmetöötlejatele ei tohi kahjustada üldmäärusega tagatud füüsiliste isikute kaitse taset (üldmääruse artikkel 44). Ka Euroopa Kohtu Screms II otsuse punktis 93 rõhutatakse vajadust tagada kolmandasse riiki edastatavate isikuandmete üldmäärusega tagatud kaitsetaseme järjepidevus.

Probleemkohaks kaitsestandardi mõistmisel üldmääruses on välja toodud terminite võrdluse põhjal selle erinev sõnastus. Nimelt taotleb üldmäärus koostoimes kohtulahendi *Schrems I* sõnastusega nn ühtse kaitsestandardi ideed, kuid seda ei toeta üldmääruses kasutatud erinev sõnastus. Nagu eelnevast selgub, kasutab kehtiv üldmäärus V peatükis vähemalt nelja erinevat väljendit. Neid termineid on kasutatud eesmärgiga tuua välja erinevad meetmed andmete kaitse tagamisel andmeedastusel, ent erinev sõnastus tekitab ühtse kaitsestandardi tunnetuse asemel killustatust. Tõlgendades õigustermineid lähtuvalt põhimõttest, et ühel ja samal terminil ei saa olla erinevat tähendust ning erinevatel terminitel ühte ja sama sisu, tuleks järeldada, et üldmääruse erinevate terminitega on taotletud üldmääruse sõnastuses erinevaid eesmärke, mis aga ei lähe kokku üldise eesmärgiga tagada samaväärne standard sõltumata rakendatavatest meetmetest. See võib muuta

[82] Euroopa Komisjoni raport. 15.05.2003. First report on the implementation of the Data Protection Directive (95/46/EC). – https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52003DC0265&from=EN, lk 9, 11-13, 16, (07.02.2023).

õiguse rakendamise andmetöötlejatele keeruliseks ning nõuab meetmete tõlgendamiseks eriteadmisi.

Õiguse tõlgendamise osas tuleks lähtuda põhimõttest, et kui sätte sõnastus on selge ja täpne, siis selle kontekstuaalne või teleoloogiline tõlgendus ei tohi seada kahtluse alla selle sätte sõnasõnalist tähendust, kuna see oleks vastuolus õiguskindluse põhimõttega.[83] *Schrems II* otsuse ja üldmääruse V peatüki nõudeid ja elemente on aga praktikas raske võrrelda, kuna *Schrems II* otsus ei andnud sellist selgust, mis oleks suunanud üksikisiku õiguslikku käitumist. Selline selgus oleks autori hinnangul aga vajalik, kuna üldmääruse sätete rikkumine võib endaga kaasa tuua suuri rahalisi kohustusi. Üldmääruse artikli 83 lõike 5 punkti c kohaselt võib rikkumine isikuandmete edastamisel kolmandas riigis asuvale vastuvõtjale või rahvusvahelisele organisatsioonile (artiklite 44–49 alusel) kaasa tuua sama lõike kohaselt haldustrahvi, mis ulatub kuni 20 miljonini või kuni 4% tema eelneva majandusaasta ülemaailmsest aastasest kogukäibest, olenevalt sellest, kumb summa on suurem.[84]

Kokku võttes eelnevat saab välja tuua, et üldmääruse V peatüki kaitsestandardi sõnastus võib olla segadusttekitav, kuna üldmääruse V peatüki tingimustes on kasutatud erinevaid väljendeid andmekaitse taseme kirjeldamiseks. Selline lähenemine ei taga töö autori hinnangul õigusselgust üldmääruse tõlgendamisel ja rakendamisel. Vaatleme järgnevalt põgusalt üldmääruse V peatüki esimeses järjekorras oleva edastamise võimaluse, kaitse piisavuse otsuse tähendust ja rolli asjakohaste meetmete ja ka üldmääruse eesmärkide täitmise mõistmiseks.

[83] Lenaerts, K, Gutiérrez-Fons, J.A. To say what the law of the EU is: methods of interpretation and the European Court of Justice. Academy of European Law. Distinguished Lectures of the Academy. 2013/9, lk 6.

[84] Vastavalt üldmääruse põhjenduspunktile 151 ei võimalda Eesti õigussüsteem määrata trahve üldmääruses sätestatu kohaselt. Eestis määrab trahvi järelevalveasutus väärteomenetluse raames. Kinnitatud seaduseelnõu kohaselt võimaldab väärteomenetluse seadustik alates 1. novembrist 2023 määrata Eestis trahve üldmääruses sätestatud ulatuses. Vt: Karistusseadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seadus (Euroopa Liidu õigusest tulenevad rahatrahvid) 94 SE, 22.02.2023. – Riigikogu. https://www.riigikogu.ee/tegevus/eelnoud/eelnou/1bfa1944-2de6-449d-a788-887bc84cfd0f/Karistusseadustiku%20muutmise%20ja%20sellega%20seonduvalt%20teiste%20seaduste%20muutmise%20seadus%20(Euroopa%20Liidu%20%C3%B5igusest%20tulenevad%20rahatrahvid) (20.04.2023).

2.2. Kaitse piisavuse otsus ja selle mõju asjakohaste kaitsemeetmetele kohaldamisele

Üldmääruse artikli 46 alusel toimuva andmeedastuse kaitsetaseme piisavuse hindamiseks kolmandas riigis kinnitas Euroopa Kohus kohtuasjas *Schrems II* punktides 85-94, et organisatsioonid peavad esmalt läbi viima andmeedastuse mõjuhinnangu, et tagada vastavalt üldmääruse artikli 46 lõike 1 kohane kohustus, et andmesubjektide kohtulikult kaitstavad õigused ja tõhusad õiguskaitsevahendid on kättesaadavad. Selline mõjuhinnang peab otsuse kohaselt hõlmama üksikjuhtumipõhiselt nii üldmääruse artikli 46 kaitsemeetmete, näiteks standardsete andmekaitseklauslite tingimuste kui ka andmete vastuvõtja asukohariigi seadusandluse arvesse võtmist.

Andmeedastuse mõjuhinnangu andmise olulised tegurid hõlmavad suures osas samu tegureid, mida Euroopa Komisjon võtab arvesse piisavuse otsuse tegemisel, nagu on sätestatud üldmääruse artikli 45 lõikes 2. Seetõttu vaatleme põgusalt üldmääruse artikli 45 kaitse piisavuse otsust ainult osas, mis aitab mõista selle sisulist mõju asjakohaste kaitsemeetmete kohaldamisele.

Kaitse piisavuse otsus üldmääruse artiklis 45 peegeldab isikuandmete kolmandate riikide andmetöötlejatele edastamise raamistikus kõige selgemalt EL-i kohustust ja eesmärki kaitsta liikmesriikides asuvate isikute eraelu puutumatust ja andmekaitseõigusi, kui nende isikuandmeid edastatakse väljapoole EL-i, kuna kolmanda riigi või organisatsiooni kaitse piisavuse kindlaks tegemiseks hindab Euroopa Komisjon üldmääruse artikli 45 lõike 2 kohaselt mitmeid elemente, sealhulgas õigusriigi põhimõtteid, inimõiguste ja põhivabaduste austamist, riigi julgeolekut, karistusõigust ja riigiasutuste juurdepääsu isikuandmetele, turvameetmete ja eeskirjade rakendamist, kohtupraktikat ning andmesubjektide tõhusate ja kohtulikult kaitstavate õiguste olemasolu, sõltumatu järelevalveasutuse olemasolu ja koostöö tegemine liikmesriikide järelevalveasutustega ning rahvusvahelisi kohustusi või muid kohustusi õiguslikult siduvatest konventsioonidest või õigusaktidest või kolmanda riigi või rahvusvahelise organisatsiooni osalemist mitmepoolsetes või piirkondlikes süsteemides, eelkõige seoses isikuandmete kaitsega.

Üldmääruse artiklis 45 lõige 2 toodud loetelu isikuandmete kaitse taseme piisavuse hindamise asjaoludest on pikk ning märksa detailsem kui see oli direktiivi 95/46/EÜ artiklis 25, mille järgi võeti andmekaitse taseme hindamise aluseks kolmandates riikides "(...) kõiki andmete edastamise toimingute või andmete edastamise toimingute kogumi asjaolusid; tähelepanu pööratakse eelkõige andmete laadile, kavandatud töötlemistoimingu või töötlemistoimingute eesmärgile ja kestusele,

päritoluriigile ja lõppsihtriigile, kõnealuses kolmandas riigis kehtivatele nii üldistele kui ka konkreetse sektori õigusnormidele ja kõnealuses riigis järgitavatele ametieeskirjadele ja turvameetmetele.“ Üldmääruses loetelust selgub, et kaitse piisavuse otsuse saamiseks hinnatakse nii kohaldatavate eeskirjade sisu kui ka vahendeid, mis tagavad selliste reeglite tegeliku jõustamise.

Euroopa Komisjoni veebilehel on avaldatud piisavuse otsuste saanud riikide loetelu. Euroopa Komisjon on seni tunnustanud Andorrat, Argentiinat, Kanadat (äriorganisatsioonid), Fääri saari, Guernseyd, Iisraeli, Mani saart, Jaapanit, Jerseyt, Uus-Meremaad, Korea Vabariiki, Šveitsi, Ühendkuningriiki ja Uruguayd kui piisavat kaitset pakkuvaid riike. Need piisavuse otsused, välja arvatud Ühendkuningriigi oma, ei hõlma andmevahetust õiguskaitsesektoris, mida reguleerib eelmises peatükis mainitud õiguskaitsedirektiivi 2016/680 artikkel 36.[85] Piisavuse otsuse alusel toimub andmeedastus kolmandasse riiki analoogselt EL-i sisese isikuandmete edastusega ning selleks ei pea ettevõtjad rakendama täiendavaid kaitsemeetmeid.[86] Nagu selgub, ei ole enamik maailma riike Euroopa Komisjoni otsuse alusel piisava andmekaitse tasemega riigina tunnustatud ning seega ei ole enamikule kolmandate riikide andmete vastuvõtjale isikuandmete edastamine andmeedastaja jaoks kõige lihtsama meetme – kaitse piisavuse otsuse alusel võimalik.

Eelnevat kokku võttes saab öelda, et isikuandmete kaitse piisavuse otsus üldmääruse artiklis 45 on oluline element isikuandmete kolmandate riikide andmetöötlejatele edastamise raamistikus ning seda kasutatakse Euroopa Liidu kodanike privaatsuse ja andmekaitseõiguste kaitseks eesmärgiga kaitsta liikmesriikides asuvate isikute eraelu puutumatust ja andmekaitseõigusi, kui nende isikuandmeid edastatakse väljapoole EL-i. Euroopa Komisjon hindab piisava kaitsetaseme tagamiseks kolmandate riikide õigusakte ja nende rakendamist, kohtupraktikat, järelevalveasutuste olemasolu ja rahvusvahelisi kohustusi. *Schrems II* kohtuotsus rõhutab, et kolmandate riikide andmetöötlejatele andmete edastamine ei tohiks kahjustada EL-is pakutavat kaitset. Kaitse tase kolmandates riikides ei pea olema identne EL-is tagatavaga, vaid sisuliselt samaväärne. Euroopa Kohtu *Schrems II* kohtuotsus tugevdab kõrget standardit, mida kohus nõuab andmete edastamisel kolmandate riikide andmetöötlejatele, ja on oluline, et kohus laiendab kaitse piisavuse standardit ka teistele andmeedastusmehhanismidele.

[85] European Commission. Adequacy decisions. How the EU determines if a non-EU country has an adequate level of data protection. - https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (21.03.2023).

[86] Andmekaitse inspektisoon. Andmete edastamine välisriiki. (21.06.2021) - https://www.aki.ee/et/teenused-poordumisvormid/andmete-edastamine-valisriiki (30.03.2023).

Nii 2015. aasta *Schrems I* kui 2020. aasta *Schrems II* kohtuotsuste mõju üldmääruse V peatüki kaitsemeetmetele märgiline. Need kohtuotsused avavad tõlgendustega mitmeid olulisi põhimõtteid, mida tuleks andmeedastusel järgida nii kaitse piisavuse otsuse osas kui teiste kaitsemeetmete rakendamisel. Seetõttu vaadeldakse kohtuotsuste mõju järgnevates alapeatükkides veidi lähemalt ning tuuakse välja nende sisaldavad olulisemad põhimõtted, mis on olulised käesoleva töö kontekstis.

2.3. Kohtupraktika mõju asjakohaste kaitsemeetmetele kohaldamisele ja üldmääruse eesmärkidele

2.3.1. Safe Harbor otsuse ja *Schrems I* kohtuotsuse mõju asjakohaste kaitsemeetmete rakendamisele

Kaitsestandardi sisuline tõlgendamine on tihedalt seotud *Schrems I* ja *Schrems II* kohtulahenditega, sest need otsused käsitlesid andmeedastusi üldmääruse alusel EL-ist USA-sse ning tõstatasid küsimuse, kas USA-s on andmekaitse tase piisavalt kõrge, et tagada EL-i kodanike isikuandmete kaitse nõuetele vastavus sisuliselt samaväärsele kaitsele EL-is tagatuga, nagu on käesolevas töös viidatud eelnevalt kaitsestandardi määratluse juures.

Direktiivi 95/46/EÜ põhjenduspunkt 56 rõhutab isikuandmete piiriülest liikumist kolmandate riikidega, pidades seda vajalikuks rahvusvahelise kaubanduse laiendamisel. Andmete vaba liikumise võimaldamiseks EL-i ja USA vahel, mis on kahe piirkonna vahelise tugeva kaubandussuhte aluseks, võttis Euroopa Komisjon vastu otsuse 2000/520/EÜ[87] (Safe Harbori otsuse). Safe Harbori otsus võeti vastu sel ajal kehtinud direktiivi 95/46/EÜ artikli 25 lõigete 5 ja 6 alusel, mille alusel on Euroopa Komisjoni volitatud alustama läbirääkimisi kolmanda riigiga, et parandada olukorda, mis tekib siis, kui Euroopa Komisjon leiab, et asjaomane kolmas riik ei taga piisavat kaitset (Safe Harbori otsuse preambul). Selle otsusega tunnistas Euroopa Komisjon, et USA kaubandusministeeriumi 21. juulil 2000 avaldatud Safe Harbor põhimõtted ja nendega

[87] Euroopa Komisjoni 26.07.2000 otsus nr 2000/520/EÜ vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ piisava kaitse kohta, mis on ette nähtud Safe Harbor põhimõtetega ja sellega seotud korduma kippuvate küsimustega, mille on välja andnud Ameerika Ühendriikide kaubandusministeerium. – ELT L 215, 25.08.2000, lk 7-47.

kaasnevad korduma kippuvad küsimused (KKK; moodustavad Safe Harbor ühe osa vastavalt Safe Harbor otsuse punktile 5) tagasid piisava kaitsetaseme isikuandmetele.[88] Safe Harbori otsus kehtis ainult nendele ettevõtetele, kes olid ise otsustanud neid põhimõtteid vabatahtlikult järgida, kuid reeglid muutusid siduvaks nendele organisatsioonidele, kes otsustasid end sertifitseerida, s.t. teatasid kaubandusministeeriumile oma kohustusest põhimõtetest kinni pidada.[89]

Safe Harbori põhimõtete eesmärk oli seega anda andmesubjektidele õigused ja kaitse, mis olid võrreldavad 1995. aasta direktiivis 95/46/EÜ sätestatud õigustega ja kaitsega. Safe Harbori otsus moodustas vahetasandi vastuoluliste regulatiivsete režiimide vahel, mille täielikku ühtlustamist ei toimu, kuid mille tulemusel järgivad USA isikuandmete vastuvõtjad EL-i andmekaitseõigusel põhinevaid standardeid seoses EL-ist saadud andmetega. Safe Harbor võimaldas USA ettevõtetel ise kinnitada, et nad on pakkunud teatud privaatsuskaitset.[90]

Schrems I kohtuasi sai alguse 2013. aasta juunis, kui Austria kodanik Maximillian Schrems esitas kaebuse Iirimaa andmekaitsekomisjonile ja palus järelevalveasutusel keelata või peatada tema isikuandmete edastamine Facebook Irelandilt USA-sse, kuna ta leidis, et USA seadused ja tava ei taganud tema territooriumil hoitavate isikuandmete piisavat kaitset seal avaliku võimu poolt teostatava jälitustegevuse eest (*Schrems I* punktid 26, 28). Iirimaa andmekaitsekomisjon jättis kaebuse läbi vaatamata kaebuse tagasi eelkõige põhjusel, et Euroopa Komisjon leidis otsuses 2000/520 (Safe Harbor), et USA tagas Safe Harbor raames edastatavate isikuandmete piisava kaitse (*Schrems I* punkt 29). M. Schrems vaidlustas Iirimaa andmekaitsekomisjoni otsuse ja Iirimaa kõrgem kohus esitas otsuse 2000/520 kehtivuse kohta eelotsuse taotluse Euroopa Liidu Kohtule (*Schrems I* punkt 1).

Schrems I punktid 28 ja 30 ja kohtujuristi ettepanek[91] viitavad korduvalt ühe ajendina *Schrems I* asjas Edward Snowdeni poolt USA luureteenistuse NSA tegevuse kohta tehtud paljastused, mille kohaselt NSA oli loonud PRISM-nimelise programmi, mille raames sai see agentuur õiguse vabalt tutvuda andmekogumitega, mis on salvestatud USA asuvates serverites, mida omavad või juhivad rida äriühinguid, kes on tegevad interneti ja tehnoloogia valdkonnas, näiteks Facebook.

[88] *Ibidem*, põhjenduspunkt 5.
[89] *Ibidem*, KKK 6.
[90] Kuner, C. Reality and illusion in EU data transfer regulation post Schrems. - German Law Journal, 2017, 18(4), lk 890.
[91] EK C-362/14, *Maximillian Schrems versus Data Protection Commissioner*, kohtujurist Y. Bot´i ettepanek, punktid 25-26, 35-36.

Euroopa Kohus tunnistas 2015. aastal Safe Harbori otsuse kehtetuks[92] vastavalt *Schrems I* kohtuotsuse punktile 107. Otsuse kohaselt peeti Safe Harborit üheks kanaliks, mis võimaldas NSA-l juurdepääsu EL-ist USA-sse edastatud andmetele (*Schrems I* punkt 87).

Schrems I kohtuasja olulisust ja mõju üldmääruse V peatüki kaitsemeetmetele näitab see, et Euroopa Kohtu tõlgendus *Schrems I* kohtuasjas piisava kaitsetaseme kohta (*Schrems I* punkt 73 ja 74) kajastub ka peale *Schrems I* otsust kehtima hakanud üldmääruse artikli 45 tekstis – kokkuvõtlikult ei pea kolmandate riikide õigus tagama üldmääruse ja EL õiguse identset kaitsetaset, vaid oluline on EL-i andmekaitsealastes õigusaktides sätestatud olulisi tingimusi täita.

Schrems I kohtuotsus, millega tunnistati ühtlasi kehtetuks EL-USA Safe Harbori turvalise andmeedastuse raamistik, mõjutas kogu EL-i andmekaitse põhimõtteid tol ajal kehtinud direktiivis 95/46/EÜ ja peale seda kehtima hakanud üldmääruses. Otsus peegeldas selgelt, et USA ettevõtted on EL-ist andmete vastuvõtjatena kohustatud järgima küll Euroopa õigusakte, ent seejuures puudub garantii, et USA luureasutused ei koguks, säilitaks ega töötleks Euroopa kodanike andmeid.[93] Sama problemaatika on jätkuvalt aktiivne ning ei puuduta ainult USA-d, vaid kõiki riike väljaspool EL-i, kelle andmekaitse tase on madalam üldmäärusega kehtestatud standardist.

2.3.2. Privacy Shield otsuse ja *Schrems II* kohtuotsuse mõju asjakohaste kaitsemeetmete rakendamisele

Pärast EL-USA andmeedastuse raamistiku Safe Harbor kehtetuks tunnistamist 2015. aastal, avaldasid EL-i ja USA ametivõimud EL-USA privaatsuskilbi Privacy Shield lepingu eelnõu 29. veebruaril 2016,[94] et võimaldada andmevoogu Atlandi-üleses andmevahetuses,[95] mis viis Privacy

[92] Euroopa Liidu Kohus. Pressiteade nr 91/20, Luxembourg, 16.07.2020. Kohtuotsus (kohtuasi C-311/18) Data Protection Commissioner vs. Maximillian Schrems ja Facebook Ireland. Euroopa Kohus tunnistab kehtetuks otsuse 2016/1250 isikuandmete kaitse piisavuse kohta ELi-USA andmekaitseraamistikus Privacy Shield, lk 1-3.
[93] EKo C-362/14, *Schrems*, punkt 86.
[94] Weiss, M. A., Archick, K. U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield. – Congressional Research Service. 19.05.2016, lk 3, 12.
[95] Euroopa Parlament. USA Riikliku Julgeolekuagentuuri järelevalveprogramm, ELi liikmesriikide jälgimisasutused ning mõju ELi kodanike põhiõigustele. P7 TA(2014)0230 9.11.2017. – ELT C 378/104.

Shieldi otsuse vastuvõtmiseni juulis 2016. aastal[96] direktiivi 95/46/EÜ kehtivuse ajal selle artikkel 25 lõike 6 alusel Euroopa Komisjoni volituste raames. Direktiivi 95/46/EÜ asendumisel üldmäärusega jäi Privacy Shield otsus jõusse üldmääruse artikli 45 lõike 9 alusel, mille kohaselt direktiivi 95/46/EÜ artikli 25 lõike 6 alusel komisjoni poolt vastu võetud otsused jäävad jõusse, kuni neid muudetakse, asendatakse või kehtetuks tunnistatakse.

Privacy Shield otsust Safe Harboriga võrreldes võib öelda, et nende ülesehitus on sarnane. Privacy Shield on isereguleeruv süsteem andmete edastamiseks USA-sse, kuid erinevalt Safe Harbor põhimõtetest sätestati selles USA ettevõtetele rangemad kohustused. Sarnaselt Safe Harbori otsusega nägi ka Privacy Shield ette kinnituste süsteemi, Privacy Shield otsuse artikli 1 lõike 3 kohaselt edastatakse isikuandmed EL-USA andmekaitseraamistiku Privacy Shield raames juhul, kui need edastatakse liidust USA asuvatele organisatsioonidele, mis kuuluvad Privacy Shieldi nimekirja, mida haldab ja mille teeb avalikkusele kättesaadavaks USA kaubandusministeerium.

Privacy Shield otsus koosneb USA kaubandusministeeriumi 7. juulil 2016 välja antud põhimõtetest ning otsuse lisades sisalduvatest avaldustest, mehhanismide kirjeldusest ja kohustustest, sealhulgas kinnitustest, et USA ametiasutuste juurdepääs andmetele riikliku julgeoleku tagamiseks ja õiguskaitse eesmärkidel kehtivad konkreetsed piirangud ja kaitsemeetmed (Privacy Shield otsuse põhjenduspunkt 88). Võrreldes Safe Harbor põhimõtetega muudeti Privacy Shield otsusega rangemaks järgmised aspektid:

- Üksikisiku kaitse tõhustamine vastavalt Privacy Shiled otsuse I lisale: Iga Euroopa kodanik, keda mõjutab USA ettevõtte privaatsusskeemi turvalisuse ebaõige kasutamine, käivitab asjakohase konfliktilahenduse mehhanismi, mida on võimalik lahendada otse ettevõttega, asjaomase EL-i liikmesriigi andmekaitseasutuse kaudu, kes seejärel esitab kaebuse USA kaubandusministeeriumile; või vahekohtumehhanismi kaudu, mida on kirjeldatud Privacy Shield otsuse I lisas.
- Järelevalve ja jõustamise tugevdamine vastavalt Privacy Shiled otsuse II lisale: Privacy Shield kehtestas II lisaga tugevama järelevalve- ja jõustamissüsteemi, kusjuures USA ametiasutused kohustuvad perioodiliselt kontrollima USA ettevõtete vastavust nõuetele ja võtma rikkumiste

[96] 12. juuli 2016. aasta Euroopa Komisjoni rakendusotsus (EL) 2016/1250 isikuandmete kaitse piisavuse kohta ELi-USA andmekaitseraamistikus Privacy Shield vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ 1. lisa – ELT L 207/1 (2016/4176) (Privacy Shield otsus).

korral jõulisemaid meetmeid, s.t. kui on tõendeid õigusaktide rikkumise kohta, eemaldatakse ettevõte Privacy Shieldi nimekirjast.

- Ombudsmani mehhanism vastavalt Privacy Shiled otsuse III lisale: Privacy Shield lõi ombudsmani mehhanismi otsuse III lisa alusel, et pakkuda ELi kodanikele sõltumatut võimalust esitada kaebusi USA valitsuse juurdepääsu kohta nende isikuandmetele. Täpsemalt nähakse lisas ette sõltumatu ombudsmani ametikoht, kes käsitleb ELi üksikisikute kaebusi USA ametiasutuste juurdepääsu kohta nende isikuandmetele. Ombudsmani nimetab ametisse USA välisminister ning ta peab olema sõltumatu ja erapooletu. Mehhanismi eesmärk on tagada EL-i kodanike jaoks Safe Harbori lepinguga võrreldes tõhusam viis kahju hüvitamiseks.

Jätkuna *Schrems I* kohtuasjale kontrollis *Schrems II* kohtuasjas Euroopa Liidu Kohus 16. juuli 2020 otsuses, Euroopa üldmääruse ja USA privaatsuskilbi Privacy Shield kehtivust. Austria aktivist Maximillian Schrems esitas selles kohtuasjas kaebuse Iirimaa andmekaitsekomisjonile, väites, et tema isikuandmeid töödeldakse ebaseaduslikult USA-s, kuna ei ole piisavat kaitset privaatsuse rikkumise eest. *Schrems II* kaebuse sisu seisnes selles, et USA privaatsuskilbi raamistik, mis võimaldas isikuandmete edastamist Euroopast USA andmetöötlejatele, ei taga üldmäärusega nõutavat kaitset.

Kohus tunnistas Privacy Shield raamistiku kehtetuks 2020. aastal[97] ja seda mitmel põhjusel. *Schrems II* otsuses on probleemidena välja toodud, et USA õiguskaitsenõuded on ülimuslikud Privacy Shieldi nõuete ees (*Schrems II* punkt 164); samuti puuduvad USA õigusaktides vajalikud piirangud ja kaitsemeetmed ametiasutuste volituste suhtes vastavalt raamistikule (*Schrems II* punktid 168-185); lisaks puuduvad EL-i andmesubjektide jaoks tõhusad õiguskaitsevahendid olukorras, kus andmesubjektid sooviksid oma õigusi maksma panna (*Schrems II* punktid 191-192).

Schrems II otsusel on oluline mõju üldmääruse tõlgendamisele. Kohtuasjas leiti, et Euroopa Komisjoni otsus Safe Harbor lepingu kohta, mis võimaldas isikuandmete edastamist USA-sse, oli kehtetu, kuna see ei taganud piisavat kaitset Euroopa Liidus kogutud isikuandmetele. *Schrems II* otsuse suuremale mõjule kõigile andmeedastusmehhanismidele on viidanud EDPB 11. novembril 2020 avaldatud järelevalvemeetmete Euroopa oluliste garantiide osas, et tulenevalt *Schrems II* otsuse punktist 105, mõjutavad Privacy Shieldi kehtetuks tunnistamise põhjused ka muid

[97] Euroopa Liidu Kohus. Pressiteade nr 91/20, Luxembourg, 16.07.2020. Kohtuotsus (kohtuasi C-311/18) Data Protection Commissioner vs. Maximillian Schrems ja Facebook Ireland. Euroopa Kohus tunnistab kehtetuks otsuse 2016/1250 isikuandmete kaitse piisavuse kohta ELi-USA andmekaitseraamistikus Privacy Shield, lk 1-3.

edastusvahendeid.[98] *Schrems II* kohtuotsus võttis seisukoha ka asjakohaste kaitsemeetmete, täpsemalt standardsete andmekaitseklauslite kehtivuse osas (*Schrems II* punkt 203), mida vaadeldakse täpsemalt käesoleva töö järgmistes osades.

Schrems II kohtuotsusega tunnistati 2020. aastal kehtetuks EL-USA andmeedastuse raamistik Privacy Shield, mis oli loodud asendama Safe Harbor otsust. Privacy Shield pidi tagama tugevamad andmekaitsemeetmed ja -kohustused, kuid Euroopa Kohus otsustas, et USA jälitustegevused ei ole vastavuses EL-i õigusega. Otsuse tulemusel jääb organisatsioonide võimaluseks leida isikuandmete EL-ist edastamiseks muud õiguslikud mehhanismid, näiteks standardsed andmekaitseklauslid üldmääruse artikli 46 alusel, kuid need nõuavad andmekaitse tagamiseks ka täiendavaid lisameetmeid. Kokkuvõtvalt mõjutas *Schrems II* otsus märkimisväärselt üldmääruse andmekaitsemeetmete sisu, andes otsuses seisukohti üldmääruse kaitse piisavuse taseme ja artikli 46 kaitsemeetmete osas.

2.3.3. Järeldused kaitse piisavuse otsuse regulatsiooni ja kohtupraktika mõju kohta vastavalt üldmääruse eesmärkidele

Üldmääruse V peatüki andmeedastuse sätted on olulised tagamaks isikuandmete edastamisel kolmandate riikide andmetöötlejatele või rahvusvahelistele organisatsioonidele üldmäärusega sätestatud kaitse tase kõikjal, kuhu andmed liiguvad[99] ning ühtlasi kõigile andmeahelas osalevatele andmetöötlejatele kohalduvate piirangute läbi välistada, et andmetöötlejal tekiks huvi viia andmed liidust välja eesmärgiga neid seal vabalt töödelda ehk vältida üldmääruse nõuetest kõrvalehoidmist (nagu on toodud *Schrems I* punktis 73). Vaatleme, kas eelpool käsitletud piisava kaitsetaseme nõue ja kohtupraktikas sätestatud põhimõtted täidavad üldmääruse eesmärki kaitsetaseme tagamise osas.

Toodud eesmärki – tagada EL-i isikuandmete kaitse samaväärne tase väljaspool EL-i – on mõjutatud, õigupoolest seatud kahtluse alla eelmistes punktides käsitletud *Schrems I* ja *Schrems II* kohtupraktikaga. Safe Harbor ja Privacy Shield olid *sui generis* lepingud, mille üle pidas EL

[98] European Data Protection Board. Recommendations 02/2020 on the European Essential Guarantees for surveillance measures. 10.11.2020. – edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf (europa.eu), punktid 5-6, (10.04.2023).

[99] European Data Protection Board. Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR. (14.02.2023). – https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_en, lk 5, (11.03.2023).

läbirääkimisi ainult USA-ga, et võimaldada andmete edastamist ettevõtetele, mis tõendavad nendes kokkulepetes sätestatud reeglite järgimist. Mõlemad Schremsi kohtuasjad, mille tulemusel nii Safe Harbor kui Privacy Shield kehtetuks tunnistati, keskendusid EL-USA vahel kehtinud andmekaitselepingutele ning ühtlasi kaitsestandardi piisava kaitse taseme põhimõttele.[100] Nimetatud kohtuasjad on mõjutanud laiemalt kogu üldmääruse V peatüki tõlgendust ning seadnud küsimuse alla kaitsemeetmete eesmärgi säilitada piisav andmekaitse tase.

Kohtuasjadest *Schrems I* ja *Schrems II* järelduv eesmärk on kahtlemata tagada isikuandmete kaitse kõrge tase. Siiski on küsitud, kas kohtu kasutatud meetodid ja vähene paindlikkus tagavad tõepoolest selle eesmärgi saavutamise. Schremsi kohtupraktika näitab, et kolmandatelt riikidelt nõutav standard on ülimalt kõrge. Z. Gulczyńska uurimuses on välja toodud, et seda standardit ei taga isegi kõik EL liikmesriigid.[101] Euroopa Inimõiguste Kohus (EIK) on leidnud, et mitme liikmesriigi, viimati Ungari[102] ja Ühendkuningriigi (kui see oli veel ELi liikmesriik)[103] rakendatud jälitusmeetmed rikuvad EIK nõudeid.

Kaebajad, kaks Ungari kodanikku, leidsid EIK kohtuasjas 37138/14 esitatud *Szabó and Vissy versus Hungary* taotluses, et Ungari rikub Euroopa inimõiguste konventsiooni artiklit 8, kuna nende suhtes võidakse väidetavatel riigi julgeoleku eesmärkidel rakendada põhjendamatuid ja ebaproportsionaalselt sekkuvaid meetmeid. EIK leidis, et Ungari seadus rikub Euroopa inimõiguste konventsiooni artiklit 8 ja mõistis Ungari valitsuse hukka, kuna kohtuliku kontrolli puudumine ja julgeolekuteenistuse massiline jälitustegevus rikuvad inimõigusi, eriti õigust eraelu puutumatusele invasiivsete jälgimisvahendite tõttu.[104] Ka otsustas EIK Ühendkuningriigi kohtuasjas ECHR nos 58170/13 *Big Brother Watch and Others versus the United Kingdom* massilise jälgimise kohta tehtud otsuses, et Ühendkuningriigi pealtkuulamise režiim rikkus õigust eraelu puutumatusele, kuna sellel puudus piisav järelevalve ja kaitsemeetmed.[105]

[100] Chander, A. Is Data Localization a Solution for Schrems II? – Journal of International Economic Law, 23(3), 2020, lk 772.
[101] Gulczyńska, Z. A certain standard of protection for international transfers of personal data under the GDPR. - International Data Privacy Law, 11(4), 11/2021, lk 366, 371-372.
[102] ECHR 37138/14, *Szabó and Vissy versus Hungary*, 12.01.2016.
[103] ECHR nos 58170/13 jt, *Big Brother Watch and Others versus the United Kingdom.* 13.09.2018.
[104] ECHR 37138/14, *Szabó and Vissy versus Hungary,* punkt 102.
[105] ECHR nos 58170/13 jt, *Big Brother Watch and Others versus the United Kingdom,* punkt 536.

Samamoodi leidis Euroopa Kohus, et ka Prantsusmaa, Belgia ja Ühendkuningriigi seadused[106] ei vasta EL-i standarditele.[107] Seetõttu on kolmandatelt riikidelt nõutav kaitse tase vähemalt mõnel juhul kõrgemgi kui liikmesriikide endi poolt järgitav. See paradoks ei ole mitte ainult ebamugavus EL-i suhetes kolmandate riikidega, mis õõnestab EL-i võimet parandada isikuandmete kaitset ülemaailmselt, vaid konventsiooni 108 kontekstis võib see tähendada liikmesriikide õiguslike kohustuste rikkumist.[108] Toodud EIK kohtuasjad näitavad Euroopa riikide põhiõiguste, õiguse eraelu puutumatusele ja privaatsusele, rikkumist. Töö autor leiab, et kui Euroopa riikide õiguskord ei taga üldmääruse artikli 45 lõike 2 punktis a esitatud nõudeid kolmandate riikide kaitse taseme piisavuse hindamise aluseks olevate asjaolude osas, ei saa selliste nõuete täitmise kohustust panna kolmandatele riikidele, esitades neile nõuded, mida EL liikmesriigid ise ei täida.

L. Determanni käsitlus USA andmekaitse regulatsiooni piisavuse osas tõi esile mõningad müüdid ja levinud kahtlused võrreldes üldmäärusega, pakkudes analüüsi USA andmekaitseõiguse kohta 2016. aasta kontekstis. Ta lükkas ümber müüdi USA andmekaitseõiguse puudulikkuse kohta, viidates paljudele föderaal- ja osariigi seadustele, mis kaitsevad isikuandmeid USA-s mitmel viisil. Determann leidis, et kuigi üldmäärus pakub mõnes valdkonnas suuremat kaitset, nagu andmesubjekti õigused ja andmerikkumistest teatamise nõuded, siis USA-s on tegelikult rangemad standardid sellistes kaitsemeetmetes nagu krüpteerimis- ja andmete lokaliseerimise nõuded. L. Determanni uurimuse kohaselt lähenevad USA ja EL andmekaitsele küll erinevalt, kuid üldiselt on mõlemad isikuandmete kaitsmisel tõhusad. Tema käsitluses on esile toodud ka arvamus, et tegelikult ei pruugi ka Euroopa riikide õigusaktid tagada täielikku vastavust üldmääruse andmekaitse standardile, nagu on mainitud eespool. Olulise osana on Determanni analüüsis välja toodud, et tegelikkuses on rahvusvaheline luurealane koostöö on muutumatult sama, viidates *Schrems I* kohtuotsuse seisukohtadele.[109] Selline käsitlus on kahtlemata huvitav ning avab uusi tahke Euroopa kaitsestandardi käsitluse osas. Seega, kuigi üldmäärus seab liiduülese õigusaktina EL riikidele andmekaitse standardid, siis fookus selle järgimise osas on EL-i välistel riikidel, samas

[106] EKo C-511/18, *La Quadrature du Net*, ECLI:EU:C:2020:791, punkt 229; EKo C–623/17, *Privacy International versus Secretary of State for Foreign and Commonwealth Affairs* jt, ECLI:EU:C:2020:790, punkt 83.
[107] Christakis, T. „Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 1). News and comments on EU law. (13.11.2020). – European Law Blog. https://europeanlawblog.eu/2020/11/13/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-1/ (13.02.2023).
[108] Gulczyńska, Z. A certain standard of protection for international transfers of personal data under the GDPR. - International Data Privacy Law, 11(4), 11/2021, lk 372.
[109] Determann, L. Adequacy of data protection in the USA: myths and facts. - International Data Privacy Law, 22.09.2016, 6 (3), lk 244-250.

kui EL liikmesriikide siseriikliku õiguse aspektid võivad olla teatavas vastuolus üldmääruse põhimõtetega. Sisuliselt on raske eelneva põhjal (eeltoodud EIK otsused selle kohta, kuidas EL liikmesriikide jälitusmeetmed rikuvad EIK nõudeid) välistada, et ka mõne Euroopa riigi siseriiklik seadusandlus ei vasta täielikult samaväärse kaitse standardile ning on vastuolus üldmääruse põhimõtetega. See omakorda tekitab vastuolu kaitsestandardi kõrgete nõudmiste osas, mida nõutakse kolmandatelt riikidelt osas, milles EL ise ei suuda nende nõuete täitmist liidus tagada.

Selle üle, kas üldmääruse andmeedastusrežiim võib potentsiaalselt piirata kaubandust ja rikkuda harta artiklis 8 toodud andmete privaatsust kui inimõigust, on arutlenud J. X. Dhont. Kontekstis, kus õigus andmekaitsele on tõstetud inimõiguseks, väärib see kahtlemata kõrgeimat kaitsestaatust ja seega ka laiemat kaiset. Samas tekitab see küsimusi, kas ka iga EL-i liikmesriik peaks samale proovile edukalt vastu? Sellele, kuidas isikuandmeid EList lahkumisel kaitsta, lihtsaid vastuseid pole. Siiski tundub raske õigustada õiguslikku režiimi, mis inimõiguste kaitse tõttu struktuuriliselt kahjustab rahvusvahelist kaubandust. Mõnevõrra dramaatiliselt öeldes: see mitte ainult ei oleks pikas perspektiivis jätkusuutlik, vaid kujutaks endast sisuliselt ohtu väärtustele, millel see põhineb, s.t. majanduslikule õitsengule ja rahule.[110]

Üldmääruse üheks eesmärgiks on ka kolmandates riikides asuvatele andmetöötlejatele kohalduvate piirangute abil välistada, et andmetöötlejal tekiks huvi viia andmed liidust välja eesmärgiga neid seal vabalt töödelda ehk vältida üldmääruse nõuetest kõrvalehoidmist. Kuivõrd on selline eesmärk täidetud kaitse piisavuse otsuse ja kohtupraktika tähenduses, vaatleme järgnevalt.

Käesolevas töö osas vaadeldi üldmäärusega kehtestatud kaitsestandardi olemust üldmääruse V peatüki kontekstis, mille osas tekitab küsimusi erinevates peatüki artiklites kasutatud erinev sõnastus sama kaitsestandardi kirjeldamiseks. Lisaks on antud põgus ülevaade üldmääruse artiklis 45 toodud tingimustest, millega tuleb arvestada ka üldmääruse artikli 46 kaitsemeetmete kohaldamisel, kui nende alusel toimub isikuandmete edastamine kolmandate riikide andmetöötlejatele. Nimelt on täiendava tingimusena üldmääruse artikkel 46 kaitsemeetmete rakendamisel vajalik läbi viia mõjuhinnang kolmanda riigi õiguskorra osas. Selline lisatingimus kaitsemeetmete rakendamisel on kujunenud standardiks läbi kohtupraktika, mille tulemusel on EDPB andnud välja soovitused andmeedastajale. Käesolevast töö osast joonistub välja probleem, et vaatamata üldmääruse kõrgele kaitsestandardile, üldmääruse artiklis 45 viidatud tingimustele,

[110] Dhont, J. X. Schrems II. The EU adequacy regime in existential crisis? – Maastricht journal of European and comparative law, 26(5), lk 598-601.

mida tuleb rakendada ka artikli 46 kaitsemeetmete kohaldamisel, ja lisaks kohtupraktikale, ei pruugi isikundmete kaitse kolmandates riikides nende meetmete rakendamisel tagada samaväärset andmete kaitset. Veelgi enam, kohtupraktika ja õiguslikud arutelud on esile toonud probleemi, et ka EL liikmesriikide endi siseriiklik õigus ei pruugi olla täielikus vastavuses eesmärgiga tagada üldmääruses sätestatud kaitse tase.

2.4. Asjakohaste kaitsemeetmete rakendamine ja selle problemaatika

2.4.1. Asjakohaste kaitsemeetmete kasutamine standardsete andmekaitseklauslite näitel isikuandmete edastamisel

Teise peatüki alguses on selgitatud, et kaitse piisavuse otsuse (üldmääruse artikkel 45) puudumisel tuleb kolmandate riikide andmetöötlejatele isikuandmete edastamisel järgmisena kaaluda üldmääruse artiklis 46 ette nähtud asjakohaste kaitsemeetmete rakendamist. Selle artikli lõike 1 kohaselt võib andmetöötleja edastada isikuandmeid kolmanda riigi andmete vastuvõtjale juhul, kui andmeedastaja on rakendanud asjakohased kaitsemeetmed, mis on loetletud artikli 46 lõikes 2 ning andmesubjektide kohtulikult kaitstavad õigused ja tõhusad õiguskaitsevahendid on kättesaadavad.

Isikuandmete edastamine kolmandate riikide andmetöötlejatele, mis ei ole saanud piisavuse otsust, kujutab endast andmeedastust mittepiisava andmekaitsetasemega riiki ning edastamisel tuleb rakendada üldmääruse artikli 46 kaitsemeetmeid. EL-i suurimad majanduspartnerid nagu näiteks USA[111] ei kuulu kaitse piisavuse otsuse saanud riikide kategooriasse, kus nende riikide andmekaitse piisavust oleks EL-i poolt tunnustatud.[112] Sisuliselt tähendab see, et kui andmetöötlejad soovivad nende riikide andmetöötlejatega EL andmesubjektide isikuandmeid jagada, tuleb neil leida õiguslikud meetmed üldmääruse artiklist 46 ja veenduda andmekaitse piisava taseme tagamises sellise andmeedastuse käigus. Nagu töö eelmises alapeatükis käsitletud, tuleb andmeedastajal jälgida, et klientide ja partnerite andmete turvalisus oleks tagatud

[111] Hamilton, D. S., Quinlan, J. P. Annual Survey of jobs, trade and investment between the United States and Europe 2020. – The Transatlantic Economy, lk 10-11, 14, 18, 47.
[112] Voss, W.G. Transatlantic Data Transfer Compliance. 2022. – BUJ Sci. & Tech. L., lk 160.

üldmäärusele vastavalt, kuna kolmanda riigi siseriiklikud õigusaktid võivad olla vastuolus EL-i andmekaitse regulatsiooniga.

Üldmääruse artikkel 46 loetleb üles kaitsemeetmed, mille rakendamisel on võimalik isikuandmete edastamine kolmandate riikide andmetöötlejatele. Need kaitsemeetmed on nimetatud käesoleva töö teise peatüki alguses. Praktikas on loetletud kaitsemeetmetest pooldanud organisatsioonid ülekaalukalt (2019. aasta uuringu käigus selgus, et ligikaudu 88% ettevõtetest, kes edastavad isikuandmeid väljapoole EL-i, tuginevad tüüptingimustele) Euroopa Komisjoni poolt vastu võetud standardsete andmekaitseklauslite (tüüptingimuste) kasutamist üldmääruse artikli 46 lõike 2 punkti c alusel.[113] Töö ülevaatlikkuse seisukohast käsitletakse asjakohaste kaitsemeetmete loetelust artiklis 46 ainult standardsete andmekaitseklauslite kasutamist, kuna ühe kaitsemeetme näitel saab edasi anda käesoleva töö õiguslikku probleemi. Lisaks on ka töös käsitletud *Schrems I* ja *Schrems II* kohtuotsuste mõju tüüptingimustele suurim.

Standardsed andmekaitseklauslid isikuandmete kolmandate riikide andmetöötlejatele edastamise kohta vastavalt Euroopa Parlamendi ja nõukogu määrusele 2016/679 võeti täiustatud versioonis vastu 4. juunil 2021 Euroopa Komisjoni rakendusotsusega nr 2021/914. Selliste kaitsemeetmete eesmärgiks on kompenseerida puudujääki, et tagada vastuvõtja kolmanda riigi suhtes piisav kaitsetase. Teisisõnu peavad lepingusätted „rahuldavalt kompenseerima üldise piisava kaitse puudumise, lisades olulised kaitseelemendid, mis igas konkreetses olukorras puuduvad".

Nagu käesolevas töös eelnevalt käsitletud, siis ainuüksi üldmääruse artikli 46 kohaste meetmete rakendamisest ei piisa. Lisaks kaitsemeetme rakendamisele on vajalik läbi viia ka andmeedastuse mõjuhinnang. Mõjuhinnang (*transfer impact assessment*) on analüüs, mille käigus hinnatakse andmete ülekandmise võimalikku mõju isikuandmete kaitsele ja eraelu puutumatusele. See hinnang peaks arvestama kõiki asjaomaseid tegureid, sealhulgas andmete tundlikkust, nende töötlemise eesmärki, vastuvõtva riigi või organisatsiooni seadusandlikku raamistikku ja muid asjakohaseid tegureid. See tähendab, et andmeedastajad peavad end kurssi viima ka välismaiste õigussüsteemidega, et saavutada teadmine andmeedastuse vastavuse osas ning tuvastada ja vähendada riske, mis võivad tekkida isikuandmete kaitse rikkumisel.

[113] International Association of Privacy Professionals and Ernst & Young. Annual Privacy Governance Report 2019, 77. - https://iapp.org/resources/article/iapp-ey-annual-governance-report-2019/ (12.12.2022).

Mõjuhinnangu läbiviimise kohustusele ei viita otsesõnu üldmäärus. Hinnangu läbiviimise vajadusele viitavad:

- Euroopa Kohtu otsus *Schrems II*. Selle kohaselt tuleb hinnata standardsete andmekaitseklauslite ehk tüüptingimuste alusel tehtavate ülekannete kaitsetaseme piisavust ja tüüptingimusi selles osas täiendada (*Schrems II* punktid 131-134), et korvata kolmanda riigi andmekaitse puudulik tase.[114]
- Samuti kohustavad mõjuhinnangut läbi viima eelviidatud Euroopa Komisjoni poolt heaks kiidetud lepingu tüüptingimused, mille kohaselt peavad kõik andmeedastusega seotud osapooled tagama, et andmeid vastuvõtvale andmetöötlejale ei kehtiks õigusaktid või tavad, mis võiksid takistada neil klauslitest tulenevaid kohustusi täitmast.
- EDPB on samas küsimuses väljastanud 2021. aastal värskendatud soovitused, mille eesmärk on käsitleda Euroopa Kohtu *Schrems II* otsuse nõudeid, et järgida nõudeid isikuandmete kolmandate riikide andmetöötlejatele edastamise tüüptingimuste kohta juhendi täiendavate edastusvahendite kohta, et tagada vastavus EL-i isikuandmete kaitse tasemele.[115]

Vaatleme lähemalt *Schrems II* kohtuotsuse käsitlust seoses standardsete andmekaitseklauslitega. Kohtupraktikast on tõusetunud ka vajadus rakendada mõjuhinnangu läbiviimine lisaks tüüptingimuste kasutamisele, seetõttu omab kohtupraktika suurimat rolli õiguslike meetmete kujunemisele antud temaatika juures.

Oluline on esmalt märkida, et *Schrems II* kohtuotsus tunnistab standardsete andmekaitseklauslite kehtivust edastusvahendina, mis võib tagada lepinguliselt sisuliselt samaväärse kaitsetaseme kolmandate riikide andmetöötlejatele edastatavatele andmetele (*Schrems II* punkt 203). Seejuures ei ole ainuüksi tüüptingimuste rakendamist peetud piisavaks vahendiks kaitse taseme saavutamiseks.

[114] 4. juunil 2021 Euroopa Komisjoni poolt välja antud tüüptingimused kajastavad üldmääruse uusi nõudeid ja võtavad arvesse Euroopa Kohtu *Schrems II* otsust, tagades kodanikele kõrgetasemelise andmekaitse. European Commission adopts new tools for safe exchanges of personal data. (04.06.2021). – European Commission https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847 (10.04.2023).

[115] European Data Protection Board. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Version 2.0, 18.06.2021. https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf, lk 3, (10.04.2023).

Euroopa Kohus leidis *Schrems II* otsuse punktis 104, et asjakohaste kaitsemeetmete kasutamiseks tuleb arvesse võtta nii liidus asuva andmetöötleja ja kolmandas riigis asuva isikuandmete vastuvõtja vahel kokku lepitud lepingutingimusi kui ka kolmanda riigi õigussüsteemiga seotud asjakohast teavet, mis puudutab selle riigi ametiasutuste võimalust edastatavatele isikuandmetele juurde pääseda. Oluline aspekt selle juures on, et *Schrems II* peab artikli 46 kaitsemeetmete rakendamisel hindamise aluseks üldmääruse artikli 45 lõikes 2 toodud mitteammendavaid kriteeriume, kuna EL-i õigusega olulise samaväärsuse standard kehtib ka asjakohaste kaitsemeetmete alusel andmete edastamise kohta (*Schrems II* punkt 96), millest on juttu käesoleva peatüki alguses. Kohus kinnitas, et kaitsetaseme määramise standardid peavad põhinema Euroopa Liidu õigusel, eriti hartaga tagatud põhiõigustel (*Schrems II* punkt 99).

Samuti leidis kohus, et kuna standardsed andmekaitseklauslid ei ole kolmandate riikide õiguskaitseasutustele siduvad, ei saa nad takistada sellistel asutustel juurdepääsu nende alusel edastatud andmetele (*Schrems II* punkt 136), mistõttu on lisaks tüüptingimustele oluline kasutada täiendavaid meetmeid lisaks neile, mis on sätestatud standardsete andmekaitseklauslite alusel (*Schrems II* punkt 134). Kohtuotsusest endast ei tulene, millised need täiendavad kaitsemeetmed peaksid olema, samuti ei tulene sõnaselgelt üldmääruse artikli 46 sõnastusest, et andmete edastamisel artikli 46 alusel toodud kaitsemeetmete rakendamisel tuleks lähtuda samadest põhimõtetest nagu lähtub Euroopa Komisjon kaitse piisavuse otsuse hindamisel artikli 45 alusel. *Schrems II* kohtuotsuse järel oli seetõttu vajadus saada täpsemaid seisukohti, milliseid kaitsemeetmeid tuleks täpsemalt lisaks rakendada.

EDPB võttis 2020. aastal, peale *Schrems II* otsust vastu soovitused selleks, et aidata andmeedastajatel (olgu need vastutavad töötlejad või volitatud töötlejad, eraõiguslikud üksused või avalik-õiguslikud asutused, kes töötlevad isikuandmeid üldmääruse kohaldamisalas) täita keerulist ülesannet hinnata kolmandaid riike ja määrata vajaduse korral asjakohased täiendavad meetmed ning pakub andmete edastajatele juhiseid, mida järgida andmeedastusel kolmandate riikide andmetöötlejatele. Juhiseid on täiendatud 2021. aastal.[116] EBPB soovitused on esitatud kuue sammuna, mida andmeedastajad peaksid üldmääruse artikli 46 kohaste kaitsemeetmete kasutamisel võtma ning seega ei kehti need mitte ainult standardsete andmekaitseklauslite

[116] European Data Protection Board. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Version 2.0, 18.06.2021. https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf (10.04.2023).

kasutamise, vaid ka muude selles artiklis mainitud edastusmehhanismide kohta. EDPB juhis täidab ühtlasi puudujäägi, mis tõusetus *Schrems II* kohtuotsusega vajadusest saada täpsemaid seisukohti lisameetmete rakendamise osas.

Järgnevalt antakse põgus vaade nendele sammudele, et avada mõõdet, millega tuleb andmeedastajal arvestada, kui ta soovib edastada isikuandmeid mittepiisava kaitse tasemega riikidesse. Lisamärkusena tuleb siiski mainida, et ei saa üheselt järeldada, et kõik kolmandad riigid, mis ei ole kaitse piisavuse otsust saanud, on seetõttu automaatselt mittepiisava tasemega, kuna kõiki riike ei ole sellest aspektist Euroopa Komisjoni poolt hinnatud.

Viidatud EDPB juhis 01/2020 soovitab esmalt andmeedastajatel kaardistada isikuandmete liikumine kolmandate riikide andmetöötlejatele, et tagada neile sisuliselt võrdne kaitsetase olenemata sellest, kus neid töödeldakse ning veenduda, et edastatavad andmed on piisavad, asjakohased ja piirduvad sellega, mis on vajalik seoses nende töötlemise eesmärkidega. Soovitus on kontrollida üldmääruse V peatüki edastustööriista, millele ülekanne tugineb, olgu selleks kaitse piisavuse otsus, üks üldmääruse artikli 46 kaitsemeetmetest või erandlik andmeedastus tulenevalt üldmääruse artiklist 49. Juhis 01/2020 EDPB-lt annab juhtnöörid, et rakendada tõhusaid lisameetmeid, mis tagavad, et edastatud isikuandmete kaitse on sisuliselt samaväärne. Kui selliseid meetmeid ei leita, ei tohi alustada isikuandmete edastamist asjaomasesse kolmandasse riiki valitud edastusvahendi alusel ning kui edastust juba teostatakse, tuleb see viivitamatult peatada või lõpetada.[117]

Edastatavate andmete kaitse taseme viimiseks EL-i olulise samaväärsuse standardini näeb EDPB juhis ette täiendavate meetmete kindlaksmääramise ja vastuvõtmise andmetöötleja poolt juhul, kui hinnangust selgub, et kolmanda riigi õigusaktid ei ole piisavalt tõhusad üldmääruse artikli 46 kohaselt. Näidetena toob EDPB välja järgmised võimalikud täiendavad kaitsemeetmed: tehnilised meetmed (krüpteerimine, pseudonüümiseerimine jt), lepingulised nõuded (nt kohustus kasutada konkreetseid tehnilisi meetmeid; läbipaistvusaruannete ja muu teabe avaldamine riigiasutuste juurdepääsu kohta; sertifikaatide saamine ja auditite läbiviimine), organisatsioonilised meetmed (nt sisepoliitika vastuvõtmine, parimate tavade ja distsiplinaarmeetmete väljatöötamine ning andmetele juurdepääsu taotluste dokumenteerimine). Lisaks on soovitus teha kõik ametlikud protseduurilised toimingud, mida täiendavate kaitsemeetme vastuvõtmine võib nõuda, olenevalt

[117] Ibidem, punkt 72, lk 26.

üldmääruse artikli 46 edastustööriistast ning vajadusel pidada nõu pädevate järelevalveasutustega. Viimaks on antud soovitus aeg-ajalt kaitsemeetmeid ning nende vastavust uuesti hinnata.[118]

Eelnevat põhjal saab öelda, et kooskõlas *Schrems II* kohtuotsuse punktiga 131 ja üldmääruse artikli 46 lõikega 1, kui Eurooa Komisjon ei ole vastu võtnud otsust andmekaitse taseme piisavuse kohta kolmandas riigis, peaks andmeedastaja EL-is võtma kasutusele meetmeid andmekaitse puudumise kompenseerimiseks kolmandas riigis. Täpsemad juhised on antud EDPB poolt pärast *Schrems II* kohtuotsuse väljakuulutamist, mis paneb andmetöötlejale kohustuseks kaitsemeetmete rakendamisel (näiteks tuginedes andmeedastusel lepingulisele meetmele, standardsetele andmekaitseklauslitele) hinnata andmete sihtkohariigi õigust sisuliselt samade kriteeriumite alusel nagu hindab Euroopa Komisjon kaitse piisavuse otsuse jaoks.

Seega, vastutava või volitatud töötleja seisukohast, kes soovib ärialases koostöös kolmanda riigi ettevõttega (riik, millel puudub kaitse piisavuse otsus) asuda teenuse toimimiseks edastama isikuandmeid kolmanda riigi andmetöötlejale, peab ta esmalt rakendama üldmääruse V peatüki artikli 46 lõike 2 punktides b-f nimetatud ühte kaitsemeedet. Kui ettevõte tugineb näiteks standardsete andmekaitseklauslite kasutamisele, ei saa ta sellega ainuüksi piirduda, kuna kohtupraktika ja EDPB välja antud juhised sätestavad, et ainuüksi tüüptingimuste kasutamisest ei piisa, vaid rakendada tuleks täiendavaid meetmeid, et veenduda kolmanda riigi andmekaitse põhimõtetes ja laiemalt ka muudes põhimõtetes, mis puudutavad põhiõigusi, avaliku võimu sekkumist jpm.

Olles käsitlenud käesolevas peatükis üldmääruse artikli 46 aluseks olevate kaitsemeetmete (töö käsitluses tüüptingimuste) rakendamisega kaasnevate täiendavate meetmete kasutamise vajadust, vaatleme kaitsemeetmete rakendamisega seonduvat problemaatikat järgmistes alapunktides, kuna vastutus andmevoogude õigusliku hindamise, haldamise ja kaitsmise seisukohast sisaldab mõningaid nõrkusi selle õiguslikust aspektist.

[118] *Ibidem*, lk 25.

2.4.2. Kaitsemeetmete rakendamise problemaatika

Kaitse piisavuse otsuse puudumisel võib andmeid EL-ist väljapoole edastada vaid juhul, kui vastutav töötleja või volitatud töötleja on kehtestanud asjakohased kaitsemeetmed üldmääruse artikli 46 loetelu põhjal ning lisaks viinud läbi mõjuhinnangu kolmanda riigi osas, kuhu plaanitakse isikuandmeid edastada. Asjakohased kaitsemeetmed võivad olla ette nähtud lepinguliste lahendustega, nagu näiteks lepingu tüüptingimustega (üldmääruse artikkel 46 lõige 2 punkt c). Selliste lepinguliste lahenduste eesmärk on tagada, et andmesaaja riigis oleks sinna edastatud andmed kaitstud samaväärselt EL-i liikmeriikidega. Eelnev analüüs näitab, et kuigi tüüptingimusi kasutatakse praktikas laialdaselt, on nende rakendamisel mitmeid raskusi. Mõjuhinnangu kui põhjaliku analüüsi ja hindamise läbiviimine on andmetöötlejale kulukas ja aeganõudev protsess ning töö autori hinnangul liiga koormav.

C. Kuner on leidnud, et komisjoni poolt üldmääruse artikli 46 lõike 2 punkti c alusel vastu võetud andmekaitse tüüptingimuste eesmärk on üksnes teha liidus asuvatele vastutavatele töötlejatele või nende volitatud töötlejatele kättesaadavaks lepingulised kaitsemeetmed, mis on ühtviisi kohaldatavad kõigis kolmandates riikides ja seda seega olenemata kaitsetasemest, mis neist riikidest igaühes tagatud on. Ta leiab, et kuna tüüptingimused ei saa juba iseenesest anda tagatisi, mis lähevad kaugemale lepingulisest kohustusest tagada liidu õigusega nõutava kaitsetaseme järgimine, võivad need olenevalt kolmandas riigis valitsevast olukorrast vajada täiendavate meetmete võtmist vastutava töötleja poolt, et tagada nõutava kaitsetaseme järgimine.[119] Kuner leiab, et sellisel kujul saavad kaitsemeetmetest üldmääruse artikli 46 tähenduses „mini-kaitse piisavuse otsused" ning selle protsessi keerukus võib panna ettevõtted, eriti väiksemad, seda teed täielikult vältima. Kuigi suured ettevõtted saavad endale lubada kulukaid juriidilisi nõuandeid, mille eesmärk on vaadata läbi välisriigi jälitusseaduse vastavus EL-i õigusele, siis väiksemad ettevõtted seda ei tee.[120]

Käesoleva töö autor nõustub eeltoodud seisukohtadega, et tüüptingimused iseenesest ei taga piisavat kaitse taset isikuandmetele kolmandas riigis määral, mis on nõutav EL-i õigusega, ning seetõttu võib EL-is asuva vastutava töötleja poolt olla vajalik võtta täiendavaid meetmeid, et tagada

[119] Kuner, C. The Schrems II judgment of the Court of Justice and the future of data transfer regulation. European Law Blog. – European Law blog, (17), 17.07.2020.
[120] *Ibidem*.

nõutava kaitsetaseme järgimine, olenevalt kolmandas riigis valitsevast olukorrast. Ent sellise hinnangu läbiviimine on suureks probleemiks ettevõtetele, eriti väiksematele, sest tüüptingimuste rakendamisele lisanduv mõjuhinnangu läbiviimine on keerukas ja võib panna andmeedastajaid seda vältima, kuna neil ei pruugi selleks piisavalt ressursse (teadmisi, raha ja aega) olla.

Samuti võib andmetöötleja ekslikult jätta tähelepanuta üldmääruse artiklis 28 lõike 1 toodud tingimuse, mille kohaselt võib vastutav töötleja kasutada ainult selliseid volitatud töötlejaid, kes annavad piisava tagatise, et nad rakendavad asjakohaseid tehnilisi ja korralduslikke meetmeid sellisel viisil, et töötlemine vastab käesoleva määruse nõuetele ja sealjuures tagatakse andmesubjekti õiguste kaitse.

Puuduvad täpsed andmed selle kohta, kui paljud andmetöötlejad jätavad kohaldamata kohtupraktikast tõusetunud kohustuse viia enne andmete edastamist kolmanda riigi osas läbi mõjuhinnang, kuid sellisele probleemile on siiski viidatud.[121] Andmetöötleja, kellel puuduvad teadmised valdkonna spetsiifikast ning kohtupraktikast tulenevatest suunitlustest, võib kohaldada lepingulises suhtes kolmanda riigi andmetöötlejale tüüptingimusi, jättes teadmatusest või ressursipuudusest rakendamata mõjuhinnangu läbiviimise protsessi, nagu selgus Euroopa Komisjoni tuletatud kaudsetest tõenditest direktiivi 95/46/EÜ kehtivusajal sätestatud andmeedastuseeskirjade puhul, kus komisjon teatas probleemist paljude volitamata ja ebaseaduslikest andmeülekannete osas sihtkohtadesse, mis ei taga andmete piisavat kaitset. [122] Nii nagu kasutajad ei pruukinud olla puudulike teadmiste või oskamatuse tõttu andmekaitse valdkonnas kursis andmeedastuse nõuetega sel ajal, ei pruugi ka tänasel päeval kõik andmetöötlejad järgida andmekaitsega kaasnevaid kohustusi andmeedastustel kolmandate riikide andmetöötlejatele.

Andmekaitse valdkond on keerukas ning nõuete täitmiseks vajalike üldmääruse sätete järgimine ja uueneva kohtupraktika ning EDPB juhiste arvestamine võib andmetöötleja jaoks olla sageli väljakutse. Andmekaitsealaste nõuete täitmiseks peavad andmetöötlejad olema kursis nii seadusandluse kui ka juhiste ja parimate tavade muutustega. Esmane ülesanne andmetöötlejale on täita üldmääruse nõudeid, mis reguleerivad isikuandmete töötlemist. Üldmäärus hõlmab lisaks

[121] Evans, M. jt. Schrems II landmark ruling: A detailed analysis. 07/2020. – Norton Rose Fulbright. https://www.nortonrosefulbright.com/en-jp/knowledge/publications/ad5f304c/schrems-ii-landmark-ruling-a-detailed-analysis (10.04.2023).

[122] Commission of the European Communities. First report on the implementation of the Data Protection Directive (95/46/EC). – COM(2003) 265 final, 15.05.2003, lk 9, 11-13, 16.

sätetele, mis puudutavad andmeedastust kolmandate riikide andmetöötlejatele, järgima ka muid üldmäärusest tulenevaid kohustusi, mille järgimine nõuab üldmääruse põhjalikku tundmist. Lisaks peavad andmetöötlejad järgima ka muid nõudeid, mis ei tulene otseselt üldmäärusest – nendeks on valdavalt kohtupraktika ja EDPB juhiste järgimine, mis annavad selgitusi ja tõlgendusi üldmääruse sätete ja täiendavate õiguslike meetmete kohta. Kohtupraktika areneb pidevalt ja EDPB avaldab sageli uusi juhiseid, seega peavad andmetöötlejad olema kursis nende muudatustega, et oma tegevust vastavalt kohandada. Sellest tulenevalt võib andmetöötleja jaoks olla andmekaitsealaste nõuete täitmine ressursimahukas ja koormav ülesanne. Nõuete täitmiseks on vaja sageli kasutada spetsialiste või teenusepakkujaid, mis suurendab andmetöötleja kulutusi.

2.4.3. Kolmanda riigi siseriiklikult kohalduva õiguse probleem

Täiendav probleem, mis tekib andmete edastamisel väljaspool EL-i asuvale vastuvõtjale ja mida on käsitletud käesolevas töös eelnevalt, on siseriiklikult kohalduva õiguse probleem. Kolmandate riikide andmetöötlejatele, kellele edastatakse EL territooriumi andmesubjektide isikuandmeid, kohalduvad siseriiklikud õigusaktid, mis võivad nõuda andmetöötlejatelt andmete avaldamist näiteks õiguskaitseasutustele. Sellised õigusaktidest tulenevad kohustused on reeglina ülimuslikud mis tahes lepingu suhtes, mille andmete edastaja ja vastuvõtja on sõlminud. Andmetöötlusleping ei ole siduv õiguskaitseasutustele kolmandas riigis, kes võivad soovida saada ligipääsu EL-ist saadud andmetele. Sellest omakorda tekib küsimus, et kui andmete kaitse pole tüüptingimuste ja mõjuhinnanguga tagatud samaväärselt EL-i standardiseeritud tasemega, siis kas pingutus siseriikliku õiguse hindamisel tagab üldse eesmärki.

Kui isikuandmeid töödeldakse EL-i territooriumil, ei kaitse neid mitte ainult üldmääruse reeglid, vaid ka muud reeglid nii EL-i kui ka liikmesriikide tasandil, millele on viidatud eespool käesolevas töös. Oluline on mõista, et kui isikuandmeid edastatakse või tehakse neile juurdepääs väljaspool EL-i territooriumit asuvatele üksustele, ei kohaldu enam EL-is sätestatud kõikehõlmav õigusraamistik. Seetõttu tuleb tagada kolmandate riikide andmetöötlejatele edastatud isikuandmete kaitse muul viisil, näiteks edastades need vastavalt üldmääruse artiklis 45 viidatud Euroopa Komisjoni piisavuse otsuse kontekstis või pakkudes asjakohaseid kaitsemeetmeid vastavalt üldmääruse artiklis 46 loetletud edastusvahenditele, millele tuginedes tuleb hinnata, kas on vaja

rakendada täiendavaid meetmeid, et edastatavate andmete kaitse tase oleks samaväärne EL-i standardiga.[123]

Andmetöötlejale kolmandas riigis, kes töötleb EL andmesubjektide isikuandmeid, kohalduvad üldmääruse sätted vastavalt selle artiklile 3. Lisaks üldmääruse sätetele peab andmete töötleja järgima ka oma siseriiklikku õigust. Kui kolmandas riigis kehtivad eeskirjad valitsuse juurdepääsu kohta isikuandmetele, mis ületavad demokraatlikus ühiskonnas vajaliku ja proportsionaalse piiri, et kaitsta ühte olulistest eesmärkidest, nagu on tunnustatud ka liidu või liikmesriikide õiguses, võib tekkida andmete vastuvõtjal õiguslik vastuolu erinevate õigusaktide järgimise osas.

Schrems II kohtuasjas rõhutatakse, et lepingulised andmekaitse tüüptingimused ei saa olla siduvad kolmandate riikide ametiasutustele, kuna viimased ei ole lepingu osapooled ja seega ei saa nad takistada sellistel asutustel juurdepääsu nende alusel edastatud andmetele, mistõttu on lisaks kaitsemeetmetele oluline kasutada täiendavaid kaitsemeetmeid lisaks neile, mis on sätestatud standardsete andmekaitseklauslite alusel.[124]

Kokkuvõtlikult võib öelda, et andmete edastamine väljaspool EL-i asuvale vastuvõtjale on põhjalik protsess, mis nõuab hoolikat kaalumist ning sobivate kaitsemeetmete rakendamist. Rahvusvahelist andmeedastust käsitlevaid sätteid väljendatakse tihti range formaalsusega, kuid nende täitmine ei pruugi tagada andmesubjektide privaatsust ja kaitset. Selliste eeskirjade rakendamine nõuab andmetöötlejatelt sageli pikaajalisi ja kulukaid tegevusi, kuid selle mõju ei pruugi anda sobivaid tulemusi andmesubjektide kaitse tagamisel.

2.4.4. Kaitsemeetmete piisavus andmekaitse taseme tagamisel kohtupraktika valguses

Nii nagu Safe Harbor ja Privacy Shield läbisid andmeedastuse meetmena Euroopa Kohtu kontrolli oma üldiselt sobivuselt kaitsma isikuandmeid EL-USA vahelises andmevahetuses, tõusetub küsimus, kas samasuguse kahtluse alla võib seada ka teisi kaitsemehhanisme. Kuigi Euroopa Kohus on analüüsinud tüüptingimuste tõhusust ja jõudnud järeldusele, et nende rakendamiseks

[123] European Data Protection Board. Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR. (14.02.2023). – https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_en, lk 5. (11.03.2023).
[124] EKo C-311/18, *Data Protection Commissioner,* punktid 134, 136; EK C-311/18, *Data Protection Commissioner versus Facebook Ireland Limited, Maximillian Schrems*, kohtujurist Saugmandsgaard Øe, H. ettepanek, punkt 126.

tuleks lisada täiendavaid meetmeid olukordades, kus kaitse piisavuse tase võib erineda sellest, mida EL-is tagatakse, ei veena see USA näite põhjal täielikult, et tüüptingimuste rakendamine tagaks andmete parema turvalisuse ja kaitse võrreldes kehtetuks tunnistatud andmekaitselepingutega.

Kohtujurist Saugmandsgaard Øe esitatud arvamus ja *Schrems II* otsuse punktis 203 on tüüptingimustele tuginevaid organisatsioone aidanud, leides, et Euroopa Komisjoni otsus 2010/87/EL tõepoolest kehtiv, kuigi kohtujuristi ettepanku rõhuasetus oli mitte niivõrd tüüptingimustel, vaid lisaks rakendatavatel kaitsemeetmetel, et kompenseerida kaitse taseme puudumine kolmandas riigis.[125] Nagu eelnevalt välja toodud, on lisameetmena mõjuhinnangu läbiviimine mahukas protsess. Näiteks 2019. aasta Euroopa Komisjoni hinnang Jaapanile õiguskorrale isikuandmete kaitse piisavuse osas on umbes 70-leheküljeline dokument, milles on antud hinnang Jaapani õiguskorrale üldmääruse artikli 45 lõike 2 tähenduses.[126] Sellises mahus õigusliku analüüsi koostamine näitlikustab autori arvates ka mõjuhinnangu läbiviimise mahkukust ja keerulisust.

Kuigi nii andmeedastajatel kui ka liikmesriikide andmekaitseasutustel on õigus andmete edastamine peatada, kui nad leiavad, et rahvusvaheline edastamine kahjustab EL-is tagatud kaitse taset, siis praktikas peaks see tähendama, et selline vastavuse puudumine on teada andmeedastajale või järelevalveasutusele, mida ei pruugi siiski kunagi juhtuda.[127] Lisaks, isegi kui see teave nendeni jõuaks, ei kaitse edastamise peatamine juba edastatud andmete osas. Kokkuvõtteks võib öelda, et kohtujurist Saugmandsgaard Øe sõnul sõltub komisjoni otsuse kehtivus vastutava töötleja kohustusest või, kui vastutav töötleja seda ei tee, pädeva andmekaitseasutuse kohustusel peatada või keelata üleandmine, kui klausleid ei ole võimalik täita.

Euroopa Kohus leidis, et avaliku võimu – näiteks õiguskaitseorganite – üldine juurdepääs andmetele seab ohtu harta artiklis 7 sätestatud õiguse eraelule, kuid ei maininud, kas selline juurdepääs rikub ka õiguse olemust harta artikli 8 alusel. Õigused andmekaitsele ja privaatsusele on omavahel tihedalt seotud ning luureteenistuste jälgimine hõlmab enesestmõistetavalt

[125] *Ibidem*, punktid 124-126.

[126] 23. jaanuari 2019. aasta Euroopa Komisjoni rakendusotsus (EL) 2019/419, isikuteabe kaitse seaduse raames Jaapani pakutava isikuandmete kaitse piisavuse kohta vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) 2016/679 (teatavaks tehtud numbri K(2019) 304 all) (EMPs kohaldatav tekst). – ELT L 76/1, lk 1-58.

[127] Andmeedastuse peatamise kohta vt: EK C-311/18, *Data Protection Commissioner versus Facebook Ireland Limited, Maximillian Schrems*, kohtujurist Saugmandsgaard Øe, H. ettepanek, punktid 129-160 ja mujal ettepanekus läbivalt.

isikuandmete töötlemist.[128] On leitud, et asjaolu, et Euroopa Kohus ei maini andmekaitseõiguse olemust, võib seega peegeldada tema pikaajalist segadust andmekaitseõiguse ja eraelu puutumatuse eristamise osas.[129]

Kokkuvõtvalt on Euroopa Kohtu lahendite näitel tõstatatud küsimus, kas samasuguse kahtluse alla nagu seati EL-USA andmeedastuslepingud, võib seada ka teisi kaitsemehhanisme, nagu standardsed andmekaitseklauslid, mis on õiguslik alus andmeedastusteks kolmandate riikidega. *Schrems I* ja *Schrems II* otsuste valguses tõusetub küsimus, kas tüüptingimused suudavad tagada isikuandmete turvalisuse tasemel, mis vastab Euroopa Liidu üldmääruses sätestatud kaitse tasemele. Kuigi Euroopa Kohus on analüüsinud nende tõhusust ja jõudnud järeldusele, et nende rakendamiseks tuleks lisada täiendavaid meetmeid, ei veena ka lisameetmete kasutamine täielikult, et üldmääruse artikli 46 kaitsemeetmete rakendamine andmevahetuses kolmandate riikide andmetöötlejatega tagaks andmete turvalisuse ja kaitse samaväärsel tasemel EL-is tagatuga.

2.5. Isikuandmete kaitse edastamisel erandite alusel

Eelnevas alapeatükis käsitleti isikuandmete kolmandate riikide andmetöötlejatele edastamise kaitsemeetmete problemaatikat üldmääruse V peatükis. Siiski saab isikuandmete edastamisel tekkida olukord, kus kaitsemeetmeid ei saa rakendada. Sisuliselt on võimalik kaaluda kaitsetut varianti isikuandmete edastamiseks – isikuandmete edastamist üldmääruse artiklis 49 nimetatud erandite alusel. Antud lahendust saab kasutada vaid erandlikes ja piiritletud olukordades. Vaatleme põgusalt käesolevas töös selle tähendust läbi üldmääruses sätestatud kaitsestandardi tähenduse.

Üldmääruse artikkel 49 lõige 1 sätestab, et teiste üldmääruse V peatüki meetmete ammendumisel, s.t. piisavuse otsuse või asjakohaste kaitsemeetmete puudumisel võib andmeedastus toimuda sättes loetletud erandite alusel teatud tingimustel. Siiski, üldmääruse artikkel 49, nagu selle nimetuski ütleb, on kasutatav vaid erandjuhtudel. Erandid paiknevad struktuuriliselt võimaliku edastusmehhanismina üldmääruse V peatükis pärast piisavuse otsust ja asjakohaste kaitsemeetmete rakendamise kohta käivaid sätteid. EDPB leiab oma juhistes, et erandeid tuleb tõlgendada nii, et

[128] Kuner, C. Reality and illusion in EU data transfer regulation post Schrems. – German Law Journal, 2017, 18(4), lk 892.
[129] Lynskey, O. The foundations of EU data protection law. – Oxford University Press, 2015, lk 270–272: Docksey, C. Four fundamental rights: finding the balance. – International Data Privacy Law, 2016/6(3), lk 195, 198.

see ei läheks vastuollu erandite olemusega kui erandid reeglist, mille kohaselt ei tohi isikuandmeid edastada kolmandasse riiki, välja arvatud juhul, kui riik tagab piisava andmekaitse taseme või kui on kehtestatud asjakohased kaitsemeetmed. Erandid ei saa praktikas muutuda reegliks, vaid neid tuleb piirata konkreetsete olukordadega.[130]

Erandid on mõeldud seega katma olukordi, kus andmete edastamise sihtriigis puudub piisav kaitse tase, kuid andmesubjekti riskid on suhteliselt väikesed või muud huvid (avalikud või andmesubjekti huvid) kaaluvad üles andmesubjekti õiguse eraelu puutumatusele. Erandeid tuleb tõlgendada kitsalt ja need ei saa üldiselt pakkuda pikaajalist raamistikku andmete korduvale või struktuursele edastamisele.[131]

Peamine problemaatika seoses eranditega andmete kaitstuse osas, millele viitab ka mainitud EDPB juhis, on see, et erandid ei taga, et andmesubjektid saavad pärast andmete kolmandate riikide andmetöötlejatele edastamist jätkuvalt samaväärset kaitset, mis neile kohaldub EL-is ning erandite alusel toimuv andmeedastus ei paku piisavat kaitset üldmääruse artikli 45 tähenduses, samuti ei ole sellisel andmeedastusel nõutud asjakohaseid kaitsemeetmeid, nagu on sätestatud üldmääruse artikli 46 alusel.[132] Seega tuleb rõhutada, et erandite kasutamine ei taga mingit kaitset andmeedastusele kolmandate riikide andmetöötlejatele ning nende alusel ei ole võimalik kaitsta andmete jälgimise eest õiguskaitseasutuste poolt, nagu Schremsi kohtuasjades arutati.

EDPB märkis, et isegi kui muud erandid ei piirdu sõnaselgelt juhuslike ülekannetega, tuleb neid tõlgendada viisil, mis säilitab nende erandi artiklites 44–47 sätestatud üldreeglitest. See tähendab, et nendele „erandlikele" põhjustele tuginemist tuleb piirata konkreetsete olukordadega; sh juhul, kui andmesubjekt on andnud nõusoleku isikuandmete edastamiseks erandite alusel, kuna isik võib oma nõusoleku igal ajal tagasi võtta.[133]

See töö ei keskendu erandite rakendamisele ega analüüsile, kuivõrd see ei aita avada problemaatikat, mis on seotud isikuandmete edastamise ja kaitsemeetmete rakendamisega

[130] European Data Protection Board. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Version 2.0, (18.06.2021). https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf, lk 14, (10.04.2023).
[131] Kuner, C. Reality and illusion in EU data transfer regulation post Schrems, lk 910.
[132] European Data Protection Board. Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679. (25.05.2018). – https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en, lk 3, (10.04.2023).
[133] *Ibidem*, lk 4, 8.

tavapärases äritegevuses. Erandite olemasolu on oluline ainult kontekstis, et tunnistada nende olemasolu, ning samal ajal tuleb märkida, et need ei ole nö tavapärane andmeedastusmehhanism. EDPB juhised täiendavad üldmääruse artiklit 49, rõhutades, et erandite alusel andmete edastamine kolmandate riikide isikuandmete töötlejale ei saa olla tavapärane andmeedastus, kuna erandite rakendamine on mittejuhuslik ja ühekordne.[134] Lisaks annab erandite (üldmääruse artikkel 49) osas tehtud ülevaade tunnistust sellest, et need meetmed ei sobi laiaulatuslikuks andmeedastuseks ning ei kaitse andmeedastuse käigus isikuandmeid ühelgi üldmääruse põhimõtete ja eesmärkides kantud viisil.

Kokkuvõtvalt võib öelda, et isikuandmete edastamisel võib tekkida olukordi, kus kaitsemeetmeid ei saa rakendada ning seetõttu tuleb kasutada erandeid. Üldmääruse artikkel 49 sätestab, et erandeid saab kasutada teatud tingimustel ning neid tuleb tõlgendada kitsalt, piirates nende kasutamist konkreetsete olukordadega. Erandid on mõeldud katma olukordi, kus sihtriigis puudub piisav kaitse tase, kuid andmesubjekti riskid on suhteliselt väikesed või muud huvid kaaluvad üles andmesubjekti õiguse eraelu puutumatusele. Erandite kasutamine ei taga aga kaitset andmeedastusele kolmandate riikide andmetöötlejatele ning nende alusel ei ole võimalik kaitsta andmete jälgimise eest õiguskaitseasutuste poolt. Seetõttu tuleb erandite kasutamist piirata konkreetsete olukordadega ning neid tuleb tõlgendada viisil, mis säilitab erandi artiklites 44–47 sätestatud üldreeglitest.

[134] *Ibidem*.

3. Ettepanekud kaitsemeetmete tõhustamiseks isikuandmete edastamisel kolmandate riikide andmetöötlejatele

3.1. Võimalused EL andmetöötleja koormuse vähendamiseks kolmandate riikide õiguskorra hindamisel

Kolmanda peatüki eesmärk on analüüsida võimalusi, kuidas EL-i andmesubjektide isikuandmed oleksid paremini kaitstud olukorras, kus isikuandmed edastatakse kolmandate riikide andmetöötlejatele, mis pole saanud Euroopa Komisjonilt kaitse piisavuse otsust. Nagu käesolevast tööst selgub, tuleb sellise andmeedastuste puhul järgida üldmääruse artiklis 46 sätestatud meetmeid kooskõlas kohtupraktika ja EDPB antud juhistega. Eelnevalt on vaadeldud artikli 46 kaitsemeetmeid standardsete andmekaitseklauslite (tüüptingimuste) põhjal ning leitud, et tüüptingimuste rakendamine nõuab EL andmetöötlejalt nii üldmääruse kui EDPB juhiste järgimist ning lisaks tüüptingimuste rakendamisele ja selle sisu kooskõlastamisele andmete vastuvõtjaga kolmandas riigis, tuleb andmeedastajal läbi viia kolmanda riigi osas mõjuhinnang, mis on oma põhimõtetelt sarnane Euroopa Komisjoni poolt läbi viidava kaitse piisavuse otsuse aluseks olevale hindamisele üldmääruse artikli 45 lõikes 2 toodud asjaolude alusel.

Kaitsemeetmete ja mõjuhinnangu rakendamise juures on probleemiks, et andmetöötleja, kes rakendab kõiki meetmeid sellise andmeedastuse jaoks, ei saa siiski lõpuni tagada, et isikuandmete edastamisel kolmanda riigi õigusruumis on nende andmete kaitse tagatud samaväärselt EL kaitsestandardiga, peamiselt seetõttu, et kolmandates riikide andmekaitse õigusraamistik ei pruugi olla samatähenduslik nagu seda on kujundatud Euroopas mitme aastakümne vältel.

Lähtuvalt samaväärse kaitse taseme tagamise põhimõttest isikuandmete edastamisel EL-ist kolmandate riikide andmetöötlejatele ja nagu töös eelnevalt viidatud, on kohtuasjas *Schrems II* välja toodud, et vastutavad või volitatud töötlejad, kes tegutsevad andmeedastajatena, vastutavad iga juhtumi puhul eraldi ja vajaduse korral koostöös kolmanda riigi andmetöötlejaga selle eest, kui kolmanda riigi õigus või tava on vastuolus üldmääruse artikli 46 ülekandevahendites sisalduvate asjakohaste kaitsemeetmetega. Sellistel juhtudel jääb andmeedastajatele võimalus rakendada täiendavaid meetmeid, et täita lüngad isikuandmete õiguslikus kaitses ja viia andmeedastus EL-i

õigusega nõutavale tasemele. EDPB hinnangul on see põhimõte kooskõlas üldmääruse artikli 5 lõike 2 aruandekohustuse (ehk vastutuse) põhimõttega, mis nõuab, et vastutavad töötlejad vastutaksid üldmääruses toodud isikuandmete töötlemise põhimõtete täitmise eest ja suudaks neid ka tõendada.[135] Ka kohus on kinnitanud vastutuse põhimõtet seoses rahvusvaheliste andmeedastustega ning märkinud *Schrems II* otsuses, et tüüptingimuste alusel andmeid edastavad vastutavad andmetöötlejad peavad kontrollima, kas sihtriigiks oleva kolmanda riigi õigus tagab piisava kaitse EL õiguse alusel ja et nad on kohustatud enne iga edastamist kontrollima, kas asjaomases kolmandas riigis järgitakse EL-i õigusega nõutavat kaitsetaset; samuti selleks, et hinnata, kas tüüptingimuste pakutav kaitsetase vastab osapoolte „olemusliku samaväärsuse" nõudele, peaks arvesse võtma nii klausleid endid kui ka selle kolmanda riigi õigussüsteemi asjakohaseid aspekte, kuhu andmeid edastati ja ka neid aspekte, mis on sätestatud üldmääruse artikli 45 lõikes 2 sisalduvas mittetäielikus loendis. (*Schrems II* punktid 99-100, 134 ja 142).

EDPB juhis andmeedastajatele (olgu need vastutavad töötlejad või volitatud töötlejad, eraõiguslikud isikud või avalik-õiguslikud asutused, kes töötlevad isikuandmeid üldmääruse kohaldamisala raames), mille keerukaks ülesandeks on hinnata kolmandate riikide osas vajadusel asjakohased täiendavad meetmed, on pikk ja paneb suure kohustuste koorma ja vastutuse andmeedastajale sobiva andmeedastusmehhanismi valimisel, selle hindamisel, täiendavate meetmete rakendamisel. Tegemist ei ole pelgalt tehniliste kaitsemeetmete rakendamise soovitustega andmete turvaliseks edastamiseks, vaid eeldab mahuka õigusliku analüüsi läbiviimist ja lisaks sellele ka teatud aja tagant korralist (ümber)hindamist.[136]

Schrems II otsus artikkel 46 asjakohaste kaitsemeetmete ja sellele lisaks täiendava mõjuhinnangu läbiviimisel on oma olemuselt küllaltki jäiga tõlgendamisruumiga. Otsust lugedes saab selgeks, et mõjuhinnang kolmanda riigi kaitse tasemele peaks põhinema üksnes andmete vastuvõtja õigussüsteemile, arvestamata konkreetselt edastatavate isikuandmete olemust ja eesmärki. Antud olukorras tekib küsimus proportsionaalsusest, kui vastutus antakse andmetöötlejale hinnata kolmanda riigi õiguskorra sobivust. Nimelt, kui andmeedastus hõlmab andmesubjektide IP-aadresside edastamist andmetöötlejale koostöö eesmärgil, on andmetöötleja kohustus tagada

[135] European Data Protection Board. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Version 2.0, (18.06.2021). – https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf, lk 3, (10.04.2023).
[136] *Ibidem*.

kaitsemeetmete rakendamine ja hindamine sama laiaulatuslikult kui andmete edastamine suuremale hulgale inimestele või ulatuslikuma ja detailsema sisuga andmete korral. Töö autor leiab, et proportsionaalsuse põhimõtet tuleks arvestada ka sellistes olukordades.

Näiteks kohtujuristi ettepanekus *Schrems II* kohtuasja kohta soovitati, et hindamine nõuaks välisriigi õigussüsteemi arvesse võtmist konkreetse edastamise tunnuste, sealhulgas isikuandmete olemuse kontekstis, võttes arvesse töötlemise eesmärki ning seda, kuidas ja miks riigiasutused isikuandmetele juurde pääsevad.[137] Kohtujuristi sellise arvamuse tagajärjeks võiks olla, et andmete edastus, mille puhul kõikide täiendavate tingimuste mittejärgimisest tulenev kahju andmesubjektile oleks olematu ning mõnel juhul võiks olla võimalik andmete edastamine kolmandate riikide andmetöötlejatele ilma täiendavate tingimuste jälgimiseta või vähemate kaitsemeetmete rakendamisega.

Seda kohtujuristi arvamust Euroopa Kohtu *Schrems II* asjas ei korratud ja seega jäävad kaitsemeetmed kohtuotsuse põhjal üsna jäigaks, sõltumata sellest, kas kolmandale riigile edastatakse näiteks EL-i andmesubjektide IP aadressid või suure hulga andmesubjektide isiklike andmetega, nt kliendibaas, mis sisaldab nime, aadressi, telefoninumbrit, sünniaega, e-posti aadressi, passi numbrit, pangakaartide numbrid koos kaartide aegumise infoga- [138] Ka üldmäärus ei näe ette kõrvalekaldeid täiendavate meetmete rakendamisel sõltuvalt sellest, kui tundlikke andmeid kolmandate riikide töötlejale edastatakse.

Andmeedastuse mehhanismide hindamine ja täiendavate kaitsemeetmete rakendamine võib olla aeganõudev ja ressursimahukas protsess. Võrdluseks võib tuua, et Euroopa Komisjon võib kulutada mitu aastat, et hinnata piisavust kolmandate riikide kaitsemeetmete osas. Näiteks Jaapaniga alustati läbirääkimisi 2018. aasta juulis[139] ning kaitse piisavuse otsus saadi 2019. aasta

[137] EK C-311/18, *Data Protection Commissioner versus Facebook Ireland Limited, Maximillian Schrems*, kohtujurist Saugmandsgaard Øe, H. ettepanek, punkt 135.

[138] Sellised andmed läksid kaduma Marriotti hotelliketi andmelekke käigus umbes 500 miljoni kliendi kohta. Vt: Perlroth, N., Tsang, A., Satariano, A. Marriott hacking exposes data of up to 500 million guests. 11/2018. – The New York Times. https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html (10.04.2023).

[139] European Commission. International data flows: Commission launches the adoption of its adequacy decision on Japan. (05.09.2018). – https://ec.europa.eu/commission/presscorner/detail/en/IP_18_5433 (27.09.2019).

jaanuaris.[140] Korea puhul alustati läbirääkimisi juba 2017. aastal[141] ning kaitse piisavuse otsus Euroopa Komisjonilt saadi alles 2021. aasta juulis.[142] Ajaline mõõde selliste otsuste hindamise läbiviimiseks näitab otsuse läbiviimise keerukust ja põhjalikkust, mida on nõutud üldmääruse artikli 45 lõikega 2.

Seega peaks andmetöötleja, kes soovib edastada Euroopa andmesubjektide isikuandmeid näiteks Hiina ettevõttele, rakendama samaväärset hindamist Euroopa Komisjoni läbiviidavale otsusele, mis nõuab eriteadmisi, ajakulu, tööjõudu ja rahalisi vahendeid ning küsimusi tekitab, kas nii mahuka mõjuhinnangu läbiviimine andmeedastuste korral kolmanda riigi andmetöötlejale on mõeldud praktiliselt rakendamiseks või pigem õigusliku olukorra katmiseks.

Kaitse piisavuse otsuse taotlemine võib olla niisiis väga ajamahukas protsess. See nõuab põhjalikku hindamist, et tagada kolmanda riigi kaitse tase isikuandmete töötlemisel, ning võib võtta mitmeid aastaid. Lisaks sellele võivad kolmandate riikide õigusaktid ja muud asjaolud muutuda aja jooksul, mis tähendab, et kaitse piisavuse otsus vajab pidevat jälgimist ja (ümber)hindamist, nagu eelnevalt viidatud. Ei ole mõeldav, et andmeedastaja viiks läbi kolmandate riikide õiguskorra põhjaliku hindamise, et olla veendunud, et sellesse riiki andmete edastamine mõnda üldmääruse artikli 46 meedet kasutades on piisavalt turvaline. Nagu töös varasemalt on viidatud, meenutakse see piisavusotsuse tegemist ettevõtjalt.[143]

Tuleviku vaates võiks kaaluda tööriistade loomist, mis aitaksid hinnata kolmandate riikide õiguskorda ja andmekaitsemeetmeid. Sellised abivahendid võiksid olla automatiseeritud ja nende kasutamine võimaldaks tõsta töö efektiivsust ning vähendada võimalikku inimlikku viga. Kolmandate riikide andmekaitse taseme hindamine hõlmab vastavalt töös välja toodud meetmetele, mille kohta on EDPB andnud suunised, peamiselt riigi õiguskorra hindmaist. Iga andmeedastuse puhul peab seega iga andmetöötleja hindama asjaolusid, mis võiksid olla üldteada ning kättesaadavad, et hõlbustada andmevahetust. Samuti, kui mõne riigi õiguskord välistab väga

[140] 23. jaanuari 2019. aasta Euroopa Komisjoni rakendusotsus (EL) 2019/419, isikuteabe kaitse seaduse raames Jaapani pakutava isikuandmete kaitse piisavuse kohta vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) 2016/679 (teatavaks tehtud numbri K(2019) 304 all) (EMPs kohaldatav tekst). – ELT L 76/1, lk 1-58.

[141] Euroopa Komisjoni teatis Euroopa Parlamendile ja Nõukogule. Isikuandmete vahetamine ja kaitsmine globaliseerunud maailmas. – 2017 COM/2017/07 final, 10.01.2017, punktid 2.2. ja 3.

[142] Data protection: European Commission launches the process towards adoption of the adequacy decision for the Republic of Korea. 16.06.2021. – European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964 (11.04.2023).

[143] Kuner, C. The Schrems II judgment of the Court of Justice and the future of data transfer regulation. European Law Blog. – European Law blog, (17), 17.07.2020.

oluliselt võimaluse üldmääruse kaitsestandardiga kohanemiseks, võiks autori arvates selline pidevalt ajakohastatud info olla avalikult usaldusväärsest allikast, näiteks Euroopa mõne institutsiooni toel, andmeedastajale vabalt kättesaadav, et vältida kahju tekkimist isikuandmete edastamisega madala kaitsega jurisdiktsioonidesse ja tagada üldmääruse nõuete parem järgimine.

Kindlasti võiks kaaluda ka Euroopa tasemel teadlikkuse tõstmist vastutavatele töötlejatele, kes töötlevad andmeid rahvusvahelises keskkonnas. Arvestades, et käesoleval ajal kasutavad ka väikeettevõtjad hulgaliselt koostööpartnereid kolmandates riikides, on teadlikkuse üldine tõstmine autori hinnangul väga vajalik. Informatsiooni jagamine andmetöötlejatele peaks hõlmama teadmisi rahvusvahelistest andmekaitsestandarditest, õiguslikest nõuetest ning kolmandate riikide õiguskorra hindamisest. See aitaks tõsta vastutavate töötlejate teadlikkust ning tagada nende võimekust täita oma ülesandeid nõuetekohaselt.

3.2. Andmekaitse taseme õiguslik ühtlustamine

Andmeedastust käsitlevate sätete eesmärk Euroopas on tagada, et eurooplaste isikuandmete edastamisel EL välistesse riikidesse liiguks ka kaitse koos andmetega. Kui erinevates riikides oleks tagatud samaväärne kaitse, õiguslik standard ja arusaam isikuandmete kaitsest, ei oleks vajalik lisaks andmeedastuslepingute sõlmimisele rakendada meetmeid kaitse samaväärse taseme hindamises osas selliselt, nagu need põhimõtted kehtivast üldmäärusest, kohtupraktikast ja EDPB juhistest tulenevad. Õiguslikku ühtlustamist on aja jooksul püütud tagada erinevate võimaluste kasutamise teel.

Näiteks 2005. aasta Montreux' deklaratsioon oli rahvusvahelise andmekaitse- ja privaatsusvolinike konverentsi tulemuseks, mis rõhutas inimeste õigust privaatsusele ja isikuandmete kaitsele ning tunnustas vajadust teha koostööd rahvusvahelisel tasandil nende eesmärkide saavutamiseks. Deklaratsioonis rõhutati ka vajadust kaitsta isikuandmeid üleilmse andmevahetuse ja kasvava tehnoloogilise arengu kontekstis, samuti väljendati muret terrorismivastaste meetmete ja isikuandmete kaitse tasakaalu pärast. Montreux' deklaratsioon kutsus riike üles võtma vastu tõhusaid andmekaitsealaseid regulatsioone, looma rahvusvahelisi standardeid andmekaitse ja

privaatsuse tagamiseks ning arendama koostööd erinevate riikide andmekaitse- ja privaatsusvolinike vahel.[144]

Ka 2009. aastal avaldatud dokumendis "The Future of Privacy Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data", mille koostas (direktiivi 95/46/EÜ artikli 29 alusel loodud töörühma) A29WP 29 töögrupp, anti ülevaade andmekaitse õigusaktide olukorrast Euroopas ja tehti ettepanekuid nende edasiseks arendamiseks ning selles rõhutati vajadust tagada tõhus andmekaitse ning edendada andmete kogumise ja kasutamise eetilisi standardeid. Samuti tehti selles mitmeid konkreetseid ettepanekuid, kuidas andmekaitse õigusakte edasi arendada ja tugevdada, et tagada inimeste õiguste tugev kaitse globaalses kontekstis.[145]

OECD poolt eraelu puutumatuse kaitse ja isikuandmete piiriüleste voogude suuniste vastuvõtmine andis samuti olulisi suuniseid nii esmakordsel vastuvõtmisel 1980. aastal[146] ning uuendustega 2013. aastal.[147] Suuniste eesmärk oli ühtlustada riiklikke eraelu puutumatust käsitlevaid õigusakte ja austada inimõigusi ning hoida rahvusvahelistes andmevoogudes ühtlast taset. Privaatsust läbi õiguse eraelu puutumatuse on käsitletud töö esimeses peatükis seoses Euroopa inimõiguste konventsiooni artikliga 8, mille kohaselt on igaühel õigus sellele, et austataks tema era- ja perekonnaelu ja kodu ning sõnumite saladust.

Õiguslikult siduv rahvusvaheline mitmepoolne isikuandmete kaitse leping on käesoleval ajal Euroopa Nõukogu konventsiooni nr 108, mille osalised on kõik EL liikmesriigid ja tähelepanuväärsena paljud riigid väljaspool Euroopat.[148] Konventsiooni osalisriigid ei ole piiritletud Euroopa Liidu alaga ning ka konventsiooni kohaldamisala on laiem üldmääruse kohaldamisalast, hõlmates ka isikuandmete töötlemist õiguskaitse- ja kohtuasutuste poolt ning

[144] Montreux Declaration. The protection of personal data and privacy in a globalized world: a universal right respecting diversities. - https://edps.europa.eu/sites/edp/files/publication/05-09-16_montreux_declaration_en.pdf (27.03.2023).

[145] Article 29 Data Protection Working Party. Working Party on Police and Justice. The Future of Privacy - Joint Contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. 01.12.2009. - https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf, lk 2, 4, 11, (27.03.2023)

[146] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (11.07.2013). - https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 (25.11.2022).

[147] *Ibidem*.

[148] Council of Europe. Parties to Convention 108.- https://www.coe.int/en/web/data-protection/national-information (27.03.2023).

andes võimaluse piirata konventsioonist tulenevaid õigusi muude konkureerivate huvide, näiteks riigi julgeoleku ja avaliku julgeoleku nimel. Konventsioonis sätestatud põhimõtteid tugevdati selle ajakohastamise käigus 2018. aastal[149] ning selle uuendatud verisoon artikkel 14 kinnitab isikuandmete vaba liikumise põhimõtet ühelt konventsiooni-osaliselt teisele (ehk kahe andmetöötleja vahel, kes alluvad eri riikide jurisdiktsioonile), sätestades, et kui andmete vastuvõtja allub sellise riigi või rahvusvahelise organisatsiooni jurisdiktsioonile, mis ei ole käesoleva konventsiooni osaline, võib isikuandmete edastamine toimuda ainult siis, kui on tagatud käesoleva konventsiooni sätetel põhinev asjakohane kaitsetase. Sellise tingimuse eesmärk kattub töö teises peatükis välja toodud andmeedastuse piirangute põhieesmärgiga, et isikuandmete kaitse taset ei kahjustataks pärast andmete riigist lahkumist ning selline tingimus laieneb kõikidele konventsiooni nr 108 osalistele, sh EL-i mittekuuluvatele riikidele (nt Albaania, Türgi, Ukraina, Island, Moldova, Monaco, Norra, Šveits jt)[150].

Konventsioonis 108+ artikli 15 alusel tunnustatakse ka järelevalvet teostavate asutuste keskset rolli konventsiooni sätete järgimise tagamisel, mis on kindlasti lisaks eeltoodud eesmärkide sätestamisele oluline viis õigusliku ühtlustamise saavutamise tähenduses. Konventsioon rõhutab selle artikliga vajadust järelevalveasutuste tõhusate meetmete kasutamise kohta, ning tunnustab õigust teha otsuseid konventsiooni rikkumiste kohta ja määrata halduskaristusi.[151] Ka üldmäärus peab oluliseks riikide seotust rahvusvaheliste lepingutega – üldmääruse artikli 45 lõike 2 punkti c kohaselt võtab Euroopa Komisjon kolmanda riigi kaitse taseme piisavuse hindamisel muu hulgas arvesse kolmanda riigi rahvusvahelisi kohustusi või muid kohustusi, mis tulenevad õiguslikult siduvatest konventsioonidest või õigusaktidest. Lisaks rõhutab üldmääruse põhjenduspunkt 105, et komisjon peaks arvestama eelkõige kolmanda riigi ühinemist Konventsiooniga nr 108, mille tähtsust on rõhutanud ka Euroopa Andmekaitsenõukogu (EDPB) arvamuses 5/2023.[152]

[149] Council of Europe. Convention 108+: Convention for the Protection of Individuals with Regard to the Processing of Personal Data. 2018. - https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (24.03.2023).

[150] Council of Europe. Parties to Convention 108.- https://www.coe.int/en/web/data-protection/national-information (27.03.2023).

[151] Council of Europe. Convention 108+: Convention for the Protection of Individuals with Regard to the Processing of Personal Data, lk 10.

[152] European Data Protection Board. Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework. (28.02.2023). - https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf (10.04.2023)

Hoolimata sellest, et konventsioon nr 108 hõlmab nii EL-i liikmesriike kui ka väljaspool seda asuvaid riike, on globaalset andmekaitseõiguse ühtlustamist peetud siiani ebatõenäoliseks. Pigem on võimalust nähtud mõne andmekaitsealase põhimõiste, näiteks „isikuandmete“ ühtlustamise saavutamise osas.[153] Andmekaitsealase ühtsuse saavutamine ja ühetaoline tõlgendamine aitaks tagada, et EL-i andmekaitseõigust kohaldatakse ja mõistetakse ühte moodi, ent ei kohusta üldmääruse nõudeid siiski kõigile riikidele ühesugusteks muutma. Sellisel juhul oleks ühtse kaitsestandardi mõistmine rahvusvahelisel tasemel oluliselt lihtsam ning andmeedastuse riskid kolmandate riikides osas oluliselt madalamad.

K. Houser ja W. Voss on leidnud, et õiguslik ühtlustamine tundub just poliitilise keskkonna tõttu ebatõenäoline.[154] Selle taga võib näha riikide erinevaid poliitilisi, majanduslikke ja sotsiaalseid huve, mis mõjutavad nende lähenemist andmekaitsele. Nii on EL rakendanud rangemaid andmekaitsestandardeid, et kaitsta andmesubjektide privaatsust, samas kui osad riigid võivad soovida kergemaid standardeid, et edendada ettevõtlust läbi vabade andmevoogude.

Samuti võivad andmekaitsealased õigusaktid ja standardid olla seotud laiemate poliitiliste küsimustega, nagu näiteks rahvusvaheline kaubandus, julgeolek ja terrorismivastane võitlus. Selliste küsimuste puhul võivad riigid soovida säilitada oma suveräänsust ja otsustusvõimet, mis võib viia erinevate andmekaitsealaste standardite ja õigusaktide vastuvõtmiseni.

Kindlasti võib andmekaitsealaste regulatsioonide ja standardite vastuvõtmine olla poliitiliselt keeruline protsess, kuna sellega kaasneb tihti kulukas tehnoloogiline ja bürokraatlik muudatuste läbiviimine. Riigid võivad olla vastu standardite loomisele, mis nõuavad suuri kulutusi, eriti kui neil puudub ressursside ja tehnoloogia infrastruktuur, et neid rakendada. Näiteks on praeguseks laialdaselt tunnustatud, et andmete privaatsusõigus USA-s on EL-is pakutavast kaitsest oluliselt erinev, kuna USA ja EL lähenevad eraelu puutumatusele erinevalt. USA-s kasutatakse valdkondlikku lähenemisviisi, mis tugineb seadusandluse, regulatsiooni ja iseregulatsiooni kombinatsioonile. USA privaatsusseadused on kitsad ja sektoripõhised, mis tähendab, et põhikirjad näevad ette, millist teavet seadus hõlmab, EL-is on andmekaitsealased õigusaktid palju laiemalt kohaldatavad.[155]

[153] Goddard, M. The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. International Journal of Market Research, 2017, 59(6), pp.704-705.
[154] Houser, K.A., Voss, W.G., lk 288-289.
[155] Schwartz, P.M., Peifer, K.N. Transatlantic data privacy law. – Georgetown Law Journal, 106, 2017, lk 117-178.

Tuues näiteid väljaspool Euroopa riike toimuvatest andmekaitse arengutest sooviga otsida õigusliku ühtlustamise võimalusi, siis näiteks California 2018. aasta tarbijate privaatsusseaduse (CCPA) jõustumine 2020. aastal tähistas USA ühe osariigi esimest kõikehõlmavat privaatsusseadust. Sellele järgnes nii föderaal- kui ka osariigi tasandil eraelu puutumatusega seotud seadusandluse väljatöötamise protsess, kuigi paljud neist seaduseelnõudest ei saanud seaduseks. Sellest hoolimata on viis teist osariiki – Colorado, Virginia, Utah, Connecticut ja Iowa, vastu võtnud oma osariigi privaatsusseaduse. Veelgi enam, föderaalne seaduseelnõu, mida tuntakse USA andmete privaatsus- ja kaitseseadusena (ADPPA), on läbimas USA kongressi läbivaatust. ADPPA jõustumisel muutuksid kehtetuks enamik osariigi ja kohalikest seadustest.[156] Selline õiguslik ühtlustamise USA andmekaitseõiguses annab oluliselt parema lähtekoha ja võimaluse, et EL-ist isikuandmete edastamine kolmandasse riiki oleks vähem komplitseeritum ning tagaks ka kindlamad väljavaated Privacy Shield asemele uue andmekaitseraamistiku kinnitamiseks.

Andmekaitse ja privaatsuse ülemaailmsel mõistmisel on oluline roll mitte ainult vastavate sätete olemasolul, vaid ka erinevate riikide taval ja väärtustel ning kultuurilistel hoiakutel, kuna need peegelduvad lõppseosena ka põhiväärtustes ja õigusaktides. Võrreldes näiteks kahte peamist andmekaitse regulatsiooni, USA-s kehtivat Health Insurance Portability and Accountability Act (HIPAA) ja üldmääruse ulatust, eesmärki ja peamisi sätteid, on leitud, et mõlema määruse eesmärk on kaitsta inimeste privaatsust ja isikuandmeid, kuid nende lähenemisviisides on olulisi erinevusi, kus üldmäärus pakub tugevamaid privaatsuskaitseid ja seab organisatsioonidele, mis töötlevad isikuandmeid, rangeimad nõuded. Ehkki regulatsioonid erinevad olulistes aspektides, jagavad nad ühist pühendumust kaitsta inimeste privaatsust ja võivad pakkuda olulist juhendamist organisatsioonidele, kes soovivad rahvusvaheliselt privaatsusnorme järgida.[157] Seega on oluline mõista erinevaid andmekaitse regulatsioone ja nende erinevusi, et tagada tugevamad privaatsus- ja kaitsestandardid kogu maailmas ning arendada välja tõhusad õigusraamistikud, mis võimaldavad organisatsioonidel vastutustundlikult töödelda inimeste isikuandmeid.

Kuigi andmekaitsealaste õigusaktide ja standardite ühtlustamine on keeruline ja lähiaastate vaates ebatõenäoline protsess, võib olla see võimalik andmekaitsealaste õigusaktides sätestatud põhimõtete kohaldamisel pikemas perspektiivis, et andmekaitsealaseid eesmärke ja piiranguid

[156] OneTrust DataGuidance. US Privacy Laws. Comply with US Privacy Laws. - https://www.dataguidance.com/comparisons/usa-privacy-laws, (10.04.2023).
[157] Tovino, S.A. The HIPAA privacy rule and the EU GDPR: illustrative comparisons. – Seton Hall Law Review. UNLV Williams S. Boyd School of Law, 2017/47.

mõistetaks põhimõttelises käsitluses ühte moodi, ilma et peaks selleks muutma kõikide riikide õigust samasuguseks üldmäärusega.

Andmekaitsealase õigusaktide ja standardite ühtlustamiseks on vaja koostööd ja dialoogi erinevate riikide ja rahvusvaheliste organisatsioonide vahel, et leppida kokku ühtsed põhimõtted ja standardid, mis tagavad isikuandmete tõhusa kaitse kõigis riikides. Andmekaitse eesmärkidest ja piirangutest ühetaoline arusaamine hõlbustaks nii õiguslikku kui sotsiaalset isikuandmete väärtustamist ühetaoliselt ning selle suurem eesmärk oleks, et andmeedastuse käigus ei oleks tarvis hinnata kolmandate riikide õiguskorda ja seeläbi minimeerida riske isikuandmete kaitsel ning hõlbustada andmetöötlejate tööprotsesse. Õiguslik ühtlustamine eeldab koostööd ja dialoogi erinevate riikide ja rahvusvaheliste organisatsioonide vahel, tervitatav oleks seejuures rahvusvaheline koostöö julgustamaks riike ülemaailmset andmekaitsestandardit vastu võtma. Seda oleks võimalik saavutada diplomaatiliste kanalite, rahvusvaheliste organisatsioonide ja vastavate riiklike ja EL institutsioonide koostöö abil.

Oluline on võtta arvesse ka tehnoloogilisi arenguid ja nende mõju andmekaitsele ning kaasata eksperte erinevatest valdkondadest, et leida optimaalseid lahendusi õigusliku ühtlustamise protsessis. Samuti on oluline tagada, et riiklikud õigusaktid ja standardid vastaksid rahvusvahelistele nõuetele ning et riigid suudaksid tagada nende rakendamise ja järgimise. Lisaks on vaja tagada läbipaistvus ja vastutusega seotud küsimused. Kõik need meetmed aitaksid kaasa isikuandmete tõhusamale kaitsele ja ühtlustatud andmekaitse standarditele erinevates riikides.

Kokkuvõtteks võib öelda, et privaatsus on oluline teema kogu maailmas ning piiriülese teabeedastuse tulemusena peavad ettevõtted järgima erinevaid rahvusvahelisi nõudeid ja standardeid. Praeguseks on õiguslikku ühtlustamist Euroopas püütud erinevates vormides tagada aastakümneid, seda näiteks eeltoodud Montreaux deklaratsiooni, konventsiooni nr 108 ja selle täiendatud versiooniga, andmekaitse töögrupi, põhiõiguste harta jt meetmete kaudu. Konventsioon 108 ja selle täiendus omavad praktilisi väljavaateid ülemaailmse andmekaitselepinguna ühtse standardi väljatöötamiseks.

Andmekaitsealaste õigusaktide ja standardite ühtlustamine on keeruline ja lähiaastate vaates ebatõenäoline protsess, kuna sellised standardid võivad siseriiklikult olla seotud laiemate poliitiliste küsimustega. Samuti võib muudatuste läbiviimine ja andmekaitsealase õiguse ühtlustamine olla kulukas ja tehniliselt keerukas protsess. Siiski on see võimalik pikemas perspektiivis, kuid eeldab koostööd ja dialoogi erinevate riikide ja rahvusvaheliste

organisatsioonide vahel. Autori hinnangul ei pea selliseks õiguslikuks ühtlustamiseks looma uut institutsiooni ega vormi, vaid piisaks olemasoleva välja töötatud kava edasiarendusest konventsiooni nr 108 näitel, millega ka praegu on liitunud mitmed riigid väljaspool EL-i, nagu töös viidatud. Sellise konventsiooni siduvaks muutumise eelduseks peaks olema andmekaitsestandardi sisuline vastavus ning selline lähenemine annaks andmetöötlejale kindlust andmete edastamisel kolmandate riikide andmetöötlejatele.

3.3. Andmete lokaliseerimine andmete kaitse tagamise meetmena

Pärast Privacy Shieldi otsuse kehtetuks tunnistamist *Schrems II* otsusega, mis puudutas andmeedastust EL-i ja USA vahel, on pakutud Euroopast kolmandate riikide andmetöötlejatele andmeedastuse probleemi lahendusena välja andmete lokaliseerimise lahendus, mis tähendaks, et isikuandmete kaitse tagamise eesmärgil ei edastata neid EL-ist kolmandatesse riikidesse. Ka Maximillian Schrems ise pakkus päev pärast *Schrems II* kohtuotsuse väljakuulutamist välja sarnase lahenduse ettevõtetele, kes edastavad andmeid USA-sse väljaspool Euroopat – jätta andmed Euroopa Liitu.[158]

Nii hakati pärast Snowdeni paljastusi takistama andmete edastamist ebausaldusväärsetesse jurisdiktsioonidesse, mille andmekaitsestandardid on nõrgemad[159] ning see ajendas andmete lokaliseerimise nõudeid pidama vahendiks, mis kaitseb isikuandmeid välismaiste luureagentuuride kätte sattumise eest.

On pakutud välja mitmeid lahendusi Euroopa ettevõtete andmete salvestamiseks EL-is asuvates serverites.[160] Lisaks on väljendatud õiguskirjanduses äärmuslikumat lahendust, mis hõlmab andmete edastamist sellise krüpteerimise astmega, et seda ei saaks keegi vastuvõtjariigis lugeda, isegi mitte adressaat. [161] Kuna tänapäeval koguvad ja haldavad andmeid praktiliselt kõik ettevõtted,

[158] Vt postitus IAPP LinkedIn lehel: The Schrems II Decision: The Day After. International Association of Privacy Professionals IAPP. – LinkedIn. https://www.linkedin.com/posts/iapp---international-association-of-privacy-professionals_the-schrems-ii-decision-the-day-after-activity-6689891497254420480-wy00 (10.04.2023).

[159] Hill, J. The growth of data localization post-Snowden: Analysis and recommendations for U.S. policymakers and business leaders. In The Hague Institute for Global Justice, Conference on the Future of Cyber Governance, 05/2014, lk 4.

[160] Kuner, C. Reality and illusion in EU data transfer regulation post Schrems, lk 913.

[161] Christakis, T. „Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 1). News and comments on EU law. (13.11.2020). – European Law Blog.

võivad andmete asukoha ja sellest tulenevate probleemide haldamine mõjutada tõsiselt Euroopa ettevõtteid ning ka küsimus andmete hoidmisest EL-is või väljaspool liitu olla praktiliselt iga ettevõtja jaoks küsimus.

USA seadusandlus võimaldab oma ametiasutustel juurdepääsu Euroopa isikuandmetele läbi õigusakti Clarifying Lawful Overseas Use of Data Act (Cloud Act).[162] Cloud Act on USA föderaalne seadus, mis jõustus 2018. aasta märtsis. Cloud Act'i kohaselt on selle peamine eesmärk võimaldada USA ametiasutustel juurdepääsu elektroonilistele tõenditele, mis asuvad väljaspool USA-d, sealhulgas EL-is. Sellega loodi uus õiguslik raamistik, mida tuleks arvestada isikuandmete töötlemisel. Cloud Act annab nimelt USA ametiasutustele laiendatud õigused saada juurdepääs andmetele, mis on salvestatud väljaspool USA-d, sh Euroopas. Varem oli see võimalik ainult juhul, kui USA-l oli vastav riiklik leping, nagu näiteks vastastikuse õigusabi leping. Cloud Act muudab asjaolusid oluliselt, sest see annab USA ametiasutustele võimaluse taotleda andmeid otse teenusepakkujatelt, kes säilitavad andmeid väljaspool USA-d. Lisaks võimaldab Cloud Act teenusepakkujatel jagada andmeid USA ametiasutustega ilma, et nad oleksid sunnitud teavitama sellest asjaomase riigi valitsust.[163]

Eelnev tähendab, et Euroopa isikuandmed võivad olla ohus ka Euroopas, sest Cloud Act võimaldab USA ametiasutustel neile juurde pääseda, isegi kui andmed on säilitatud väljaspool USA-d ja vastavat riiklikku lepingut ei ole. Sellisele probleemile viitab ka M. Rutherford, viidates, et Cloud Act tõstatab keerukaid ja mitmetahulisi andmetele juurdepääsu ja privaatsusega seotud probleeme, mis nõuavad hoolikat kaalumist ja analüüsi, et maandada võimalikke riske ja maksimeerida potentsiaalset kasu. Cloud Act võib kahjustada üksikisikute ja ettevõtete privaatsust ja andmekaitseõigusi, võimaldades USA valitsusel juurdepääsu USA-s asuvate tehnoloogiaettevõtete salvestatud andmetele, isegi kui neid andmeid hoitakse väljaspool USA-d. Cloud Act loob olulise nihke võimu dünaamikas, andes USA valitsuse täidesaatvale võimule suurema kontrolli piiriülese juurdepääsu üle andmetele ja piirates teiste riikide võimalusi kehtestada oma andmeprivaatsusstandardid. Samuti tõstatab see küsimusi riikliku suveräänsuse ja rahvusvahelise õiguse vahelise seose kohta, kuna see annab USA valitsusele õiguse pääseda juurde väljaspool

https://europeanlawblog.eu/2020/11/13/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-1/ (13.02.2023).

[162] Clarifying Lawful Overseas Use of Data Act, H.R.1625 (Cloud Act). – 115th Congress. https://www.congress.gov/bill/115th-congress/house-bill/1625/text.

[163] Cloud Act. Frequently Asked Questions. – US Departement of Justice. https://www.justice.gov/criminal-oia/page/file/1153466/download (20.04.2023).

USA-d salvestatud andmetele, mis võib rikkuda teiste riikide suveräänsust. Artikkel rõhutab pilveseadusega seotud läbipaistvuse ja vastutuse puudumist, kuna see võeti vastu ilma piisava aruteluta või arvestamata selle võimalikku mõju eraelu puutumatusele, andmekaitsele ja rahvusvahelistele suhetele.[164] Seega on Cloud Actil oluline mõju isikuandmete kaitsele ka Euroopas ning andmekaitseõigusele üldisemalt.

Positiivne külg ettevõtjale andmete lokaliseerimise juures oleks see, et esiteks ei peaks andmeedastaja tegelema, kaitsemeetmete valiku, analüüsi, kaitsemeetmete rakendamise ja hilisema monitoorimisega ning see aitaks kokku hoida aega ja raha; arvatavalt mõtleksid ettevõtjad vähem aga sellele, et lokaliseerimise kasu oleks turvalisemalt hoitud andmed. Pigem räägiks lokaliseerimise kasuks asjaajamise mugavus ja kui võimalik, siis ka madalamad kulud.

Paraku on leitud, et andmete lokaliseerimise kahjuks räägib majandustegevuse piiramisele riikide vahel just kulude kasv.[165] Andmete lokaliseerimine mitmes jurisdiktsioonis tegutsevate ettevõttete jaoks tähendaks oma infrastruktuuri lokaliseerimist mitmes eri õigusruumis, mis on tõenäoliselt samuti kulukas protsess ja mõnel juhul ka ilmselt teostamatu, muutes andmete värskendamise ja küberjulgeoleku protsessid ainult keerulisemaks.[166]

Töö autori jaoks ei kõla veenva argumendina andmete kaitse eesmärgist lähtuvalt hoida kõiki andmetöötlusteenuseid eranditult EL-is ja usutavasti pole see tihti võimalikki – paljud Euroopa ärialased suhted, sh andmevahetus, baseeruvad koostööl ja andmevahetusel kolmandate riikidega. Seega võib andmete lokaliseerimise kasutamine eesmärgiga vältida andmete edastamist kolmandate riikide andmetöötlejatele olla abiks vaid üksikjuhtudel, kuid ei saa olla suuremahuline lahendus. Sellegipoolest on andmete lokaliseerimist kui ühte võimalikku kaitsemeedet mitmeti arutatud.[167]

Ka mujal maailmas on püütud andmete lokaliseerimist sätestada siseriiklikes õigusaktides ning mõned riigid nõuavad isikuandmete lokaliseerimist kaitse-eesmärgil. Näiteks Venemaal kehtestatud föderaalseaduse kohaselt tuleb Venemaal kogutud isikuandmed säilitada Venemaal

[164] Rutherford, M. The CLOUD Act: Creating Executive Branch Monopoly Over Cross-Border Data Access. – Berkeley Technology Law Journal, 2019, 34(4), lk 1177-1204.
[165] Carlson, M. Behind the Curve: Schrems II and the Need for Increased US Data Protections in a Global Economy. J. Corp. L.,2021/47, lk 210.
[166] Chander, A., lk 782.
[167] Vt nt Hill, J.; Chander, A.

asuvates serverites. Nimelt võeti Venemaal vastu nn isikuandmete seadus[168], milles §18 lõikes 5 nõutakse, et Venemaal asuvad isikuandmete koopiad tuleb kõigil Venemaa territooriumil tegutsevatel isikuandmete töötlejatel säilitada Venemaal. See puudutab ka välismaiste ettevõtete esindusi, kes töötlevad Venemaal asuvate Venemaa kodanike isikuandmeid. Samuti on Hiinas vastu võetud küberjulgeoleku seadus, mille artiklis 37 nõutakse, et kriitilisi infosüsteeme kasutavate ettevõtete andmed ja andmete töötlemise seadmed peavad olema Hiina territooriumil.[169] Samuti on välismaiste ettevõtete puhul nõutud koostöö Hiina valitsusega seoses andmete kättesaadavuse ja turvalisusega, mis nõuab, et "kriitilised infovõrgud" peavad olema lokaliseeritud Hiinas. Ka Brasiilia on kaalunud isikuandmete lokaliseerimise nõude kehtestamist, kuigi konkreetsed õigusaktid võivad varieeruda.[170]

EL-il on strateegia edendada pilveteenuseid, et saada andmetest majanduslikku väärtust ning pilveteenuseid peetakse EL-i laiema digitaalse ümberkujundamise keskseks komponendiks. 2020. aasta detsembris algatas ENISA avaliku arutelu pilveteenuste uue küberturvalisuse sertifitseerimisskeemi (EUCS) kandidaadi üle. Andmeed on EL-i majanduskasvu põhiprioriteet ja aastatel 2018–2025 peaks andmemajanduse väärtus Euroopas peaaegu kolmekordistuma. Euroopa Komisjoni kavatsus on rahastada üle-euroopaliste ühiste koostalitlusvõimeliste andmeruumide loomist strateegilistes sektorites, mis hakkavad toimima pilveteenustel. Andmemajanduse kasvu edendamiseks Euroopas kavatseb EL luua EU Cloud Federationi, mis sisaldab eneseregulatsiooni norme ja standardeid seoses turvalisuse, energiatõhususe, andmekaitse, koostalitlusvõime ja õiglase konkurentsiga. Lisaks on ELi eesmärk luua Euroopa avatud teaduspilv, et majutada ja töödelda uurimisandmeid. EL läheneb pilveteenustele terviklikult, et tagada kõrged standardid andmekaitses ja küberturvalisuse.[171]

On leitud, et andmete lokaliseerimine ei lahenda välisseire probleemi ega paranda isikuprivaatsust, kuid õõnestab teisi Euroopa Liidu väärtusi.[172] Lokaliseerimisnõuetel võib olla mõju hoopiski

[168] Venemaa Föderaalseadus “Isikuandmete kohta”. – N 152-F3.
[169] Stanford Cyber Policy Center. Translation: Cybersecurity Law of the People’s Republic of China (Effective June 1, 2017). (29.06.2018). – https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/ (10.04.2023).
[170] 2018. aastal võttis Brasiilia vastu seaduse "Lei Geral de Proteção de Dados" (LGPD), mille artikkel 33 sisaldab sätteid isikuandmete lokaliseerimise kohta. Vt: General Personal Data Protection Act – https://lgpd-brazil.info/, (10.04.2023).
[171] Cooper, D. jt. Covington & Burling LLP. EU Cloud Initiatives in 2021 and 2022. (26.02.2021). – https://www.globalpolicywatch.com/2021/02/eu-cloud-initiatives-in-2021-and-2022/ (10.04.2023).
[172] Chander, A., lk 771.

andmete turvalisuse vähenemisele. Ettevõtete sund hoida kohalikke andmekeskusi võib põhjustada minimaalsete ressurssidega rajatiste loomist, mis lubavad tõenäolisemalt võrku sissetungi ja andmetega seotud kompromisse. Lõpuks kanduvad vastavuskulud üle tarbijatele, kui kaupade ja teenuste hindu tõstetakse kohalike teenuste rahastamiseks, selle asemel et kasutada tsentraliseeritud teeninduskeskusi, mis võivad hoopiski suurendavad tõhusust ja kaitset.[173] Piiriüleste andmevoogude piirangud pärsivad niigi kaubandust: digitaalset ja mittedigitaalset, toodete ja teenustega kauplemist. Teiseks õõnestab andmete lokaliseerimine eesmärki suurendada kaubandust, mis oli aga üks üldmääruse laiem eesmärk – nii selle V peatükk kui ka mitmed teised sätted (nt üldmääruse põhjenduspunkt 101) väljendavad soovi kaitsta andmeid nende edastamisel, mitte edastamise keelamist ega liikumise piiramist kui eesmärki. Siiski tähistab üldmääruse sõnastuses andmete „vaba liikumine“ läbivalt ainult tähendust liidusiseses mõttes, kuna EL-ist väljapoole liikuvate isikuandmetega kaasnevad alati piirangud.

Kokkuvõtvalt on pärast Privacy Shieldi kaitsemehhanismi kehtetuks tunnistamist *Schrems II* otsusega välja pakutud andmete lokaliseerimise lahendust kolmandate riikide andmetöötlejatele, kes soovivad andmeid EL-i ja USA vahel edastada. *Schrems II* otsus ajendas andmete lokaliseerimise nõudeid pidama vahendiks, mis kaitseb isikuandmeid välismaiste luureagentuuride kätte sattumise eest. Euroopa ettevõtetele on pakutud lahendusi andmete salvestamiseks EL-is. Kuigi ettevõtjate jaoks oleks andmete lokaliseerimise juures positiivseks küljeks ressursside kokkuhoid, ei tagaks andmeserverite loomine asukohapõhiselt ilmselt odavamat teenust. Probleemiks sellisel lähenemisel on ka tõdemus, et USA Cloud Act võimaldab USA ametiasutustel juurdepääsu Euroopa isikuandmetele, mis on salvestatud väljaspool USA-d, sh Euroopas. Cloud Actil on seega oluline mõju isikuandmete kaitsele ja rahvusvahelisele õigusele ning andmete lokaliseerimine EL-is ei tagaks seega sobivat eesmärki.

[173] U.S. Chamber of commerce. Business Without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity. – Hunton & Williams. https://www.huntonak.com/images/content/3/0/v3/3086/Business-without-Borders.pdf, lk 2 (10.04.2023)

3.4. Võimalikud lahendused isikuandmete turvalise edastamise võimalusteks tulevikus EL-i ja USA vahel

Schrems I kohtuasjas 2015. aastal EL-USA vahelise Safe Harbor lepingu ning *Schrems II* kohtuasjas 2020. aastal EL-USA vahelise Privacy Shield rahvusvahelise lepingu kui üldmääruse V peatüki kaitsemeetme tühistamine Euroopa Kohtu poolt tõi kaasa olulised muutused EL-USA andmekaitse valdkonnas ning tõstis esile vajaduse tagada leida uus ja tõhusam andmekaitsestandardi rahvusvahelises andmeedastuses. Hinnanguliselt kasutas Atlandi-ülesel andmevahetusel Privacy Shield lepingut enam kui 5000 USA ettevõtet, kusjuures EL-i ja USA vahelise kaubanduse ja investeeringute väärtuseks on hinnatud umbes 7,1 triljonit dollarit.[174] Seega tekitas Privacy Shield otsuse tühistamine paljudes ettevõtjates ebakindluse seoses tulevase EL-i ja USA andmeedastusega. Pärast *Schrems II* otsust ja sellega tühistatud Privacy Shield lepingut koostasid nii EL-i kui ka USA ametivõimud koostöös riiklike ametiasutustega täiustatud uue lepingu, mille eesmärk on kaitsta isikuandmeid ja tagada piiriülene andmevoog, mis hõlmab ka isikuandmete vahetamise ärilisi aspekte Atlandi-ülesel andmeedastusel. [175] Milliseid võimalusi ja probleemkohti võib ette näha veel jõustumata EL-USA uue andmekaitseraamistikuga seoses, vaatleme alljärgnevalt.

Atlandi-üleste andmevoogude osatähtsust arvestades allkirjastas USA president Joe Biden 2022. aasta oktoobris uue andmekaitsealase lepingu nimega EU-US Data Privacy Framework (DPF) jaoks täidesaatva korralduse (Executive Order). 13. detsembril 2022 teatas Euroopa Komisjon, et on käivitanud selle põhjal DPF piisavuse otsuse kinnitamiseks ning avaldas EL-USA andmekaitseraamistiku piisavuse otsuse eelnõu.[176]

Korraduse eesmärk on kehtestada õiguslikult siduvad kaitsemeetmed, mis aitavad lahendada Euroopa Liidu Kohtu poolt *Schrems II* kohtuasjas tuvastatud probleeme, et kaitsta üksikisikute

[174] Tiffith, L. IAB Applauds President Biden's Executive Order Addressing Transatlantic Data Flows. (07.10.2022). – https://www.iab.com/news/iab-applauds-president-bidens-executive-order-addressing-transatlantic-data-flows/ (29.03.2023).

[175] Commission implementing decision (draft) pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework. 2022. – https://commission.europa.eu/document/e5a39b3c-6e7c-4c89-9dc7-016d719e3d12_en (29.03.2023).

[176] The White House. Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities. (07.10.2022). – https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/ (29.03.2023).

õigusi kahju hüvitamisele ning võimaldada EL-i andmesubjektidel esitada kaebus kodanikuvabaduste kaitse ametnikule, kes jälgib, et USA luureagentuurid järgiksid eraelu puutumatust ja põhiõigusi. Kui andmekaitseraamistik heaks kiidetakse, on EL-i organisatsioonidel võimalik isikuandmeid vabalt edastada USA organisatsioonidele, kes on raamistiku kohaselt sertifitseeritud.[177] Sertifikaadi saab omandada, kui organisatsioon võtab endale kohustuse järgida uusi privaatsuspõhimõtteid – EL-USA andmekaitseraamistiku põhimõtteid. Asjaomased organisatsioonid peavad teatud ajavahemike tagant kinnitama, et nad järgivad privaatsuspõhimõtteid. EL-i andmesubjektid saavad oma õigusi teostada, esitades kaebuse otse USA ise-sertifitseeritud organisatsioonile, sõltumatule vaidluste lahendamise organile USA-s või EL-is tasuta, vahekohtule või oma riigi andmekaitseasutusele.[178] Ettevõtete jaoks vähendaks andmeedastusleping kaitsemehhanismina töömahukaid juriidilisi läbirääkimisi, mis on vajalikud Atlandi-ülese andmeedastuse läbiviimiseks viisil, mis vastab EL-i andmekaitse standarditele. Andmekaitsealase lepingu, nagu oli seda Privacy Shield, puudumisel, kasutavad ettevõtted sageli standardseid andmekaitseklausleid kinnitamaks, et andmeedastus toimub üldmääruse kohaselt. Nende probleem on, nagu töös varasemalt mainitud, et nende rakendamine koos mõjuhinnangu läbiviimisega kolmanda riigi õiguskorra suhtes on väga töömahukas protsess, eeldades enne nende rakendamist läbirääkimisi ja analüüsi.

DPF-iga soovitakse kehtestada mitmetasandiline hüvitamismehhanism, millel on sõltumatu menetlus. Esimesel tasandil saavad EL-i üksikisikud esitada kaebusi USA kodanikuvabaduse kaitse ametnikule, kes asub riikliku luure direktori büroos. Seejärel saavad nad otsused edasi kaevata täitevvõimu uuele andmekaitsekohtule. Kohus valib igaks juhtumiks eriadvokaadi, kes kaitseb kaebuse esitaja huve kohtuasjas.[179] DPF jõustumine on võimalik pärast Euroopa Andmekaitsenõukogu arvamust, konsulteerimist asjaomaste sidusrühmadega ja heakskiitu komitee esindajatest koosnevalt EL-i liikmesriikide esindajatelt.[180]

---

[177] European Commission. Questions & Answers: EU-U.S. Data Privacy Framework, draft adequacy decision. (13.12.2022). - https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_7632 (29.03.2023).

[178] The White House. Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities. (07.10.2022). – https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/ (29.03.2023).

[179] Commission implementing decision (draft) pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework. 2022. – https://commission.europa.eu/document/e5a39b3c-6e7c-4c89-9dc7-016d719e3d12_en (29.03.2023).

[180] European Commission. Questions & Answers: EU-U.S. Data Privacy Framework, draft adequacy decision. (13.12.2022). – https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_7632 (29.03.2023).

Uue andmekaitseraamistiku osas on üles näidatud ka muret selle kaitse piisavuse osas, skeptilisust lisab enne seda kehtinud Privacy Shieldi suhteliselt lühike eluiga ning uue raamistiku sarnasus sellele. Maximillian Schrems leiab, et uue andmekaitseraamistiku kehtivuse õiguslik vaidlustamine oleks edukas, pidades seda ajakohastatud Privacy Shield andmeedastuse raamistikuks[181] ning on avaldanud arvamust, et ta võib selle tehingu vaidlustada.[182] "USA jälitusrežiimi probleeme ei saa ravida ainult täidesaatva korraldusega," ütles USA kodanikuvabaduste liidu ja riikliku julgeoleku projekti vanemadvokaat Ashley Gorski oma avalduses ning leidis, et vajalik oleks välja töötada ja ellu viia sisukas järelevalvereform. Kriitikat on jaganud ka Ühendkuningriigis asuv globaalsete vastavusküsimuste konsultant Tash Whitaker, leides, et leping tõenäoliselt ei täida kaitse piisavuse nõudeid ning massijälgimine jätkub samal viisil, sõltumata täitevkorralduse sõnastuse muudatustest, kuna puudub andmesubjektide õiguskaitse USA siseriikliku õiguse raames.[183]

Veebruaris 2023 avaldas Euroopa Parlamendi kodanikuvabaduste, justiits- ja siseasjade komisjon EL-USA andmekaitseraamistiku arvamuse eelnõu, milles soovitati mitte võtta vastu otsust USA kohta piisavuse kohta, tuginedes kavandatud EL-USA andmete privaatsuse raamistikule, öeldes, et DPF ei taga EL-i kodanikele EL-iga samaväärset andmekaitse taset. Komitee kutsus komisjoni üles uuesti läbirääkimisi pidama, kuid tema arvamus ei ole komisjonile siduv, kuna tema osa vastuvõtmise protsessis piirdub kontrolliõigusega. [184]

Euroopa Parlamendi komisjon võttis vastu sarnase kriitika, juhtides tähelepanu järgmisele:

- lihtsalt termini "proportsionaalsus" kasutamine on ebapiisav, kui USA õigusaktide definitsioonid ja tõenäoline tõlgendus on erinevad;
- Executive Orderi kohaldamisel puudub kindlus ja ettenähtavus, kuna USA president võib seda igal ajal muuta;

[181] Lama, A., Auty, C. M. Is Privacy Shield 2.0 on the horizon? (11.10.2022). – Bryan Cave Leighton Paisner. https://www.bclplaw.com/en-US/events-insights-news/is-privacy-shield-20-on-the-horizon.html (10.04.2023).

[182] New US Executive Order unlikely to satisfy EU law. (07.10.2022). NOYB – European Center for Digital Rights. – https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law (10.04.2022); Statement by TACD on the announcement of a New EU-U.S. Personal Data Transfers Framework. (07.10.2022). – Trans Atlantic Consumer Dialogue. https://tacd.org/statement-by-tacd-on-the-announcement-of-a-new-eu-u-s-personal-data-transfers-framework/ (10.04.2022).

[183] Trueman, C. EU-US data sharing agreement: Is it a done deal? (12.10.2022). – https://www.computerworld.com/article/3676284/eu-us-data-sharing-agreement-is-it-a-done-deal.html (29.03.2023).

[184] European Parliament. Draft Motion for a resolution to wind up the debate on the statement by the Commission pursuant to Rule 132(2) of the Rules of Procedure on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP)). (14.02.2023). – https://www.europarl.europa.eu/doceo/document/LIBE-RD-740749_EN.pdf (10.04.2023).

- massiandmete kogumine signaalluure abil ei ole keelatud ning riigi julgeolekueesmärkide loetelu saab president täiendada ilma avaliku suhtluseta;
- USA-l ei ole erinevalt teistest piisavuse otsusega riikidest föderaalset andmekaitseseadust;
- andmekaitse läbivaatamiskohtu DPF-i hüvitamismehhanism ei vasta EL-i põhiõiguste hartas sätestatud erapooletuse või sõltumatuse standarditele ning andmesubjektide jaoks puudub föderaalne edasikaebamise viis.[185]

2023. aasta märtsis arutasid parlamendiliikmed resolutsiooni ettepaneku eelnõu komisjoni piisavuse järelduse eelnõu kohta, mis hõlmab ELi ja USA andmekaitseraamistikku, ning EDPB asjakohast arvamust.[186]

EDPB esitas oma arvamuse DPF-i kohta, mis võeti vastu 28. veebruaril[187], tuues esile olulisi parandusi, kuid väljendades ka muret. EDPB ei andnud selgesõnalist soovitust selle kohta, kas komisjon peaks vastu võtma piisavuse otsuse, vaid tõi välja ülejäänud mureküsimused, sealhulgas andmesubjektide õigused, edasiandmine, erandite ulatus, andmete hulgikogumine ja hüvitamismehhanism. Lisaks on EDPB seisukoht, et DPF-i piisavuse otsuse vastuvõtmine peaks sõltuma ajakohastatud põhimõtete ja protseduuride vastuvõtmisest täitevmääruse rakendamiseks kõigis USA luureagentuurides. Seega, kuigi EDPB arvamus näib lõppkokkuvõttes positiivsem kui Euroopa Parlamendi komisjoni karm järeldus, tõstab see siiski esile mitmeid probleeme. Kuigi Euroopa Parlamendi komisjoni arvamus ei ole siduv, vaatab Euroopa Komisjon läbi Euroopa Parlamendi ja EDPB arvamused piisavuse otsuse vastuvõtmisel. Isegi kui Euroopa Komisjon teeb DPF-i kohta otsuse, tundub peaaegu vältimatu, et M. Schrems või teised aktivistid esitavad sellele juriidilise vaidlustuse. Kokkuvõttes tervitab EDPB täiustusi võrreldes andmekaitseraamistikuga Privacy Shield, eelkõige vajalikkuse ja proportsionaalsuse põhimõtete tunnustamist ning tõhustatud järelevalve- ja hüvitamiskorda, kuid leiab, et üldmääruse piisavuse viite põhjal peaksid kolmanda riigi õigusraamistikus sisalduma andmekaitse põhikontseptsioonid ja põhimõtted, olles kooskõlas Euroopa andmekaitseõiguses sätestatud mõistetega. Siiski rõhutab EDPB, et raamistiku tõhusus sõltub sellest, mil määral seda praktikas järgitakse.[188]

[185] *Ibidem*.
[186] *Ibidem*.
[187] European Data Protection Board. Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework. (28.02.2023). – https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf (10.04.2023)
[188] *Ibidem*.

Eelneva põhjal saab öelda, et EL-USA DPF on vastuoluline teema juba enne selle kehtima hakkamist. Varasem Privacy Shield otsus tühistati kohtulikus vaidluses ja uus raamistik sarnaneb sellele, mis tekitab muret selle piisava kaitse taseme suhtes. USA jälitusrežiimi küsimused nõuavad ulatuslikku järelevalvereformi ning USA seaduste ja nende tõlgenduse erinevus võib tekitada probleeme proportsionaalsusega. Samuti on mure massijälgimise pärast ja selle puudumise tõttu, et andmesubjektidele ei anta föderaalseid õiguskaitsevahendeid USA-s.

Töö autori hinnangul on tõsine märk, et Euroopa Parlamendi kodanikuvabaduste, justiits- ja siseasjade komisjon on soovitanud mitte võtta vastu otsust USA kohta piisavuse kohta, tuginedes kavandatud EL-USA andmete privaatsuse raamistikule. Samuti ei ole EDPB andnud selget heakskiitu DPF-ile, väljendades muret seoses andmesubjektide õiguste, edasiandmise, erandite ulatuse ja andmete hulgikogumisega.

Üks peamisi muresid autori arvates ongi uue raamistiku sisuline sarnasus eelnevalt kehtinud Privacy Shieldi andmeedastuse raamistikuga, mis tunnistati kehtetuks Euroopa Kohus 2020. aasta otsusega. Seetõttu on arusaadavad Euroopa institutsioonide kahtlused ja teatav murekoht uue raamistiku piisavuse osas. Kui raamistik jõustub ja võib juba ette näha, et lühikese aja jooksul kaotab oma kehtivuse, võib see jätta ettevõtetele ebakindla õigusliku seisundi – andmetöötlejad peavad järgima andmekaitsestandardeid, mis nõuab neilt investeeringuid andmetöötluse süsteemidesse ja protsessidesse. Kui DPF jõustub ja kaob kiiresti, võib see tuua ettevõtetele kaasa kulutusi, mis ei too aga kaasa õiguskindlust. Lisaks võib DPF kaasa tuua õiguslikke probleeme, kui andmetöötlejad ja järelevalveasutused ei suuda vastavalt tegutseda. See omakorda võib põhjustada trahve või kohtuvaidlusi, mis võivad olla kulukad ja kahjustada ettevõtte mainet. Seetõttu on oluline tagada, et raamistik, mida plaanitakse peale *Schrems I* ja *Schrems II* kohtuasjades peetud vaidlusi jõustada, oleks välja töötatud jätkusuutlikult.

Kriitikud on väljendanud muret ka USA jälitusrežiimi probleemide pärast ning leidnud, et seda ei saa lahendada ainult täidesaatva korraldusega. Samuti on probleemiks andmekaitse piisav tase, sest USA-l ei ole ühtset föderaalseadust, mis tagaks piisava kaitse Euroopa kodanike andmetele ja massijälgimine jätkub samal viisil, sõltumata täitevkorralduse sõnastuse muudatustest. Töö autor nõustub, et seni, kuni eri õiguskordade vahel valitsevad põhimõttelised erisused, ei saa neid lahendada kokkulepetega, mille suhtes jäävad ülimuslikuks siseriiklikud õigusaktid.

Kokkuvõtvalt võib öelda, et jõustumata EL-USA DPF-i peamiseks probleemiks on selle madal piisavuse ja usaldusväärsuse hinnang ning töö autor näeb probleemkohana Euroopa Parlamendi ja

EDPB antud madalat hinnangut, viitega sellele, et raamistikus tuleks teha muudatusi. DPF lühiajaline kestvus põhjustaks ebakindlust ja probleeme nii andmetöötlejatele kui ka järelevalveasutustele. Eelkõige on probleem selles, et kui DPF raamistik ei taga piisavat sisulist kaitset isikuandmete töötlemise eest, võib see eelkõige põhjustada kahju andmesubjektidele, mis võib kokkuvõttes kaasa tuua andmesubjektide põhiõiguste rikkumisi.

KOKKUVÕTE

Käesoleva töö eesmärk oli uurida, kuidas Euroopa Parlamendi ja nõukogu määruses 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (üldmääruses) sätestatud isikuandmete edastamise piirangud kaitsevad isikuandmeid nende edastamisel kolmandate riikide andmetöötlejatele. Üldmääruses sätestatud asjakohaste kaitsemeetmete uurimise eesmärgiks oli tuvastada nende piirangute peamised õiguslikud probleemid ning teha ettepanekuid isikuandmete kaitse tõhustamiseks nende edastamisel kolmandate riikide andmetöötlejatele.

EL-is on isikuandmete kaitse põhiõigus ning seda kaitseb Euroopa õigusraamistik üldmääruse, ELTL-i ja Euroopa Liidu põhiõiguste harta. Andmekaitseõigus keskendub inimeste privaatsuse ja eraelu puutumatuse kaitsmisele ning selle taustaks on õigus privaatsusele ja eraelu kaitsele, mis on tunnustatud peaaegu igas maailma riigis. Euroopas on andmekaitse põhiõigus eraelu puutumatuse element, mida ei mõisteta põhiõigusena kõikides riikides.

Kui isikuandmeid edastatakse väljaspool EL-i asuvatele andmetöötlejatele, ei pruugi kohalduda enam EL-is sätestatud kõikehõlmav õigusraamistik, vaid kehtib ennekõike üldmäärus. Kui kolmanda riigi andmetöötleja töötleb EL-i andmesubjektide isikuandmeid, kohalduvad talle üldmääruse sätted vastavalt üldmääruse artiklile 3, ent andmetöötleja kolmandas riigis peab arvestama ka oma siseriiklikku õiguskorda. Kui kolmas riik ei ole saanud Euroopa Komisjonilt üldmääruse V peatüki artiklis 45 nimetatud kaitse piisavuse otsust, tuleb andmeedastajal selle riigi andmetöötlejale isikuandmete saatmiseks või kättesaadavaks tegemiseks rakendada üldmääruse V peatüki artiklis 46 nimetatud kaitsemeetmeid ning vaid äärmuslikel juhtudel võib rakendada artiklis 49 ette nähtud erandeid.

Üldmääruse üks eesmärke isikuandmete edastamisel kolmandate riikide andmetöötlejatele on tagada andmete kaitse samaväärselt EL-is ette nähtud tasemele ning vältida olukorda, kus andmetöötlejal tekib huvi viia andmed liidust välja, et neid seal vabalt töödelda. Lisaks on oluline kaitsta isikuandmeid välisriikide ametiasutuste ebaproportsionaalse sekkumise eest, mille problemaatika on muutunud väga aktuaalseks pärast Edward Snowdeni paljastusi USA luure massiliste isikuandmete kogumise kohta, ning *Schrems I* ja *Schrems II* kohtuotsuseid.

Töö analüüsi käigus selgus, et üldmääruse kaitsemeetmete rakendamise eesmärk, tagada isikuandmete kaitse kõikjal, kus neid töödeldakse, on õiguslikult täidetud. See tuleneb nii üldmääruse artiklis 3 sätestatud territoriaalsest kohaldamisalast kui ka V peatükis loetletud tingimustest andmeedastusel kolmandate riikide andmetöötlejatele. Samuti on õiguslike kaitsemeetmete kohaldamisega täidetud eesmärk andmeahelas osalevatele andmetöötlejatele kohalduvate piirangute läbi välistada, et andmetöötlejal ei tekiks huvi viia andmed liidust välja eesmärgiga neid seal vabalt töödelda.

Töös on leitud, et üldmääruse artikkel 3 ja V peatüki regulatsioon isikuandmete edastamisel on oma eesmärgilt mõneti kattuvad, ent need pole teineteisega vastuolus. Üldmääruse artikkel 3 lõige 2 laiendab üldmääruse mõjuala üle maailma, sõltumata sellest, millise riigi andmetöötlejale isikuandmed edastatakse. Üldmääruse V peatüki nõuded täpsustavad meetmeid ja nõudeid andmeedastusel kolmandate riikide andmetöötlejatele.

Üldmääruse V peatüki artiklis 46 kirjeldatud kaitsemeetmed seavad andmeedastusele kolmandatesse riikidesse ranged nõuded, kehtestades eesmärgi, et isikuandmete edastamisel liiguks kaitse andmetega kõikjale kaasa. Kui isikuandmete edastamine toimub riikidesse väljaspool EL-i, tuleb kindlaks teha, millisele andmekaitsetasemele riik vastab. Kui selline piisavuse otsus, nagu on kirjeldatud üldmääruse artiklis 45, puudub, võib üldmääruse artikli 46 alusel vastutav töötleja või volitatud töötleja edastada isikuandmeid kolmanda riigi andmetöötlejale asjakohaste kaitsemeetmete rakendamisel.

Andmete edastajatele koormavaks peetud artikli 46 asjakohaste kaitsemeetmete tõlgendamine, rakendamine ja kolmanda riigi õiguskorra analüüs võivad osutuda väga ressursimahukaks. Selliste meetmete rangus ja põhjalikkus on tekitanud küsimuse, kas kõrge kaitsestandard tegelikult lisab praktikas piisavalt õiguskindlust ja turvalisust.

Nimelt peavad andmetöötlejad üldmääruse artikli 46 alusel toimuva andmeedastuse korral rakendama sättes toodud kaitsemeetmeid ning kaitse taseme piisavuse hindamiseks kolmandas riigis läbi viima andmeedastuse mõjuhinnangu, millega tagada vastavalt üldmääruse artikli 46 lõikele 1, et andmesubjektide kohtulikult kaitstavad õigused ja tõhusad õiguskaitsevahendid on kättesaadavad. Üldmääruse sõnastus ei anna mõjuhinnangu osas täpseid juhiseid, selle läbiviimise kohustus tuleneb kohtupraktikast ning Euroopa Andmekaitsenõukogu (EDPB) antud juhistest. Selline mõjuhinnang peab hõlmama suures osas samade tingimuste arvestamist nagu on sätestatud

üldmääruse artikli 45 lõikes 2. Selles on kirjeldatud asjaolud, mida Euroopa Komisjon peab võtma arvesse kaitse piisavuse otsuse tegemiseks.

Andmetöötlejale kolmandas riigis kehtivad asukohariigi siseriiklikud õigusaktid ning need ei pruugi need olla vastavuses Euroopa õigusega. Vastuolu siseriikliku õiguse ja üldmääruse normide rakendamisel võib muutuda üldmäärusega kohustuseks pandud piirangute ja kohustuste järgimise võimatuks ning vähendada üldmääruse artiklis 46 toodud kaitsemeetmete rakendamisel nende tõhusust. Üldmääruse V peatüki üks eesmärke on aga kaitsta isikuandmeid volitamata juurdepääsu eest. Seda eesmärki on rõhutanud ka Euroopa Kohtu praktika kahe lepingulise kaitsemeetme, EL-i ja USA vahel sõlmitud Safe Harbori ja Privacy Shield´i, kehtetuks tunnistamise otsuses. Kui kolmanda riigi siseriiklik õiguskord on vastuolus üldmääruse põhimõtetega, ei ole Euroopa andmesubjektide isikuandmed kolmandas riigis kaitstud samaväärselt üldmääruses ette nähtud kaitsestandardiga.

Vähendamaks riske, mis kaasnevad probleemidega EL-i ja kolmandate riikide õiguskordade erinevuses, on töös analüüsitud, millised õiguslikud lahendused võiksid tõhustada isikuandmete samaväärse kaitse taseme saavutamist ja andmekaitseõiguse kui põhiõiguse mõistmist sarnaselt EL-i standardile kogu maailmas. Kuigi isikuandmete töötlemist Euroopa-siseselt on välja pakutud kui kaitsemeedet, ei näe töö autor selles sobivat võimalust. Andmete lokaliseerimise põhimõte halvaks paljude riikide vahelist ettevõtlust ja majanduskoostööd ning ei oleks kooskõlas ka üldmääruse ideega reguleerida andmevahetust ja andmete liikumisega seotud koostööd riikide vahel.

Kaaluda võiks hõlbustavate meetmete pakkumist Euroopa andmeedastajatele, mis aitaksid hinnata kolmandate riikide õiguskorda ja andmekaitsemeetmeid. Sellised abivahendid võiksid olla osaliselt automatiseeritud ja nende kasutamine võimaldaks tõsta töö efektiivsust ning vähendada võimalikku inimlikku viga. Samuti, kui mõne riigi õiguskord on selline, mis välistab võimaluse EL andmekaitsepõhimõtteid järgida, võiks selline teave olla andmeedastajale avalikult usaldusväärsest allikast kättesaadav, et vältida kahju tekkimist isikuandmete edastamisega riiki, millel on madalam andmekaitsestandard. Arvestades, et käesoleval ajal kasutavad ka väikeettevõtjad hulgaliselt koostööpartnereid kolmandates riikides, on teadlikkuse üldine tõstmine väga vajalik.

Andmekaitsealaste standardite õiguslik ühtlustamine on üks võimalus, mida on välja pakutud ka õiguskirjanduses. See protsess võib olla keeruline, kuid pikemas perspektiivis võimaldab see mõista andmekaitsealaseid eesmärke ja piiranguid ühtlaselt, ilma et kolmandate riikide õigusakte

tuleks ühtlustada üldmäärusega. Andmekaitsealaste õigusaktide ja standardite ühtlustamiseks on vaja põhimõttelist käsitlust ning rahvusvahelist koostööd ja dialoogi erinevate riikide ja rahvusvaheliste organisatsioonide vahel andmekaitsealaste eesmärkide ja piirangute osas, mis võimaldaks säilitada riikide eripärad, kuid rakendada neid ühtsetel alustel.

Võimalike lahendustena seoses EL-USA andmevahetusega, kelle vahel on kehtinud rahvusvahelised andmekaitselepingud ja mille kehtetuks tunnistamine on mõjutanud märkimisväärselt kogu üldmääruse V peatüki kaitsemeetmete rakendamise ja tõlgendamise küsimusi, on töös põgusalt vaadeldud andmekaitseraamistiku DPF arengut. Uue EL-USA DPF peamiseks probleemiks on selle madal hinnang Euroopa Parlamendi ja EDPB poolt piisavuse ja usaldusväärsuse osas, mistõttu nõuaks see täiendavat arutelu ja paranduste tegemist enne selle rakendamist. DPF raamistiku lühiajaline kestvus põhjustaks ebakindlust ja probleeme nii andmetöötlejatele kui ka järelevalveasutustele ning kui raamistik ei taga piisavat sisulist kaitset isikuandmete töötlemise eest, võib see eelkõige põhjustada ka lühiajalisel kehtivusel kasu asemel kahju.

Käesolev magistritöö aitab paremini mõista kaitsemeetmete kohaldamise põhimõtteid seoses isikuandmete edastamisega kolmandate riikide andmetöötlejatele ning selgitab EL-i andmeedastusreegleid, mis on sageli raskesti tõlgendatavad. Töö aitab selgitada ka erinevate juhiste ja kohtupraktika sisu, mis on seotud kaitsemeetmete rakendamisega. Samuti aitab käesolev töö mõista Euroopa Kohtu kohtupraktika mõju üldmääruse V peatüki sätete kohaldamisele, kuna see on oluliselt muutnud andmete edastamise ja kaitse põhimõtteid kolmandate riikide andmetöötlejatele. Töö annab ülevaate Schrems kohtuotsuste praktilistest tagajärgedest andmeedastuse temaatikas ning nende mõjust isikuandmete kaitsele nii EL-is kui ka väljaspool seda.

LEGAL PROBLEMS OF IMPLEMENTING APPROPRIATE SAFEGUARDS IN TRANSFERRING PERSONAL DATA TO RECIPIENTS IN THIRD COUNTRIES

Summary

The globalization has created a lot of cross-border data exchange, companies have been transforming their business processes over the last decade, managing their operations where it is most profitable for them. The power of data creates new and modern business models. Therefore, it is very important to ensure an effective safeguards both in the European Union (EU) and outside it, in order to value the value and follow the principles in the processing of personal data.

The purpose of the data protection legislation is to ensure that the protection of the data of natural persons located in the EU moves with the data everywhere. Data protection is not only a right in the EU, but also a fundamental right protected by the Treaties of the European Union and the Charter of Fundamental Rights. At the heart of this is people's right to privacy.

In the EU, data protection is regulated by Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons in the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, which entered into force on May 25, 2018 and is applicable in all EU member states (GDPR). The GDPR regulates the collection and processing of personal data in all EU member states and imposes a number of data protection obligations on data controllers and data processors. The GDPR meets the needs of today's digital world and is considered to be the shaper of European data protection law, which is established for the protection of fundamental rights, and it is the primary legal act that regulates data protection and also in the sense of fundamental law in the EU.

In the EU, data protection is a fundamental right and is protected by the Treaties of the European Union and the Charter of Fundamental Rights. Data protection law focuses on the protection of individual´s privacy which is based on the right to privacy and protection of privacy, as it is recognized in almost every country in the world. In Europe, the fundamental right to data protection is an element of privacy, which is not understood as a fundamental right in all countries.

If personal data is transferred to data processors located outside the EU, the comprehensive legal framework set out in the EU no longer applies. The GDPR applies to such data transmission on the basis of Article 3, taking into account the safeguards specified in Chapter V of the GDPR. If the third country does not have a primary safeguards, the adequacy decision of protection of the European Commission, the appropriate safeguards specified in Article 46 of the GDPR must be applied, and only in extreme cases, derogations based on Article 49 GDPR.

The purpose of the GDPR for such data transfer restrictions is to ensure a level of protection of personal data regardless of where the data is transferred. The GDPR transfer mechanisms are also intended to exclude a situation where a data processor would be interested in taking data out of the EU with the aim of freely processing it there. In addition, there is the need to protect personal data from disproportionate interference by foreign authorities, the problem of which was clearly evident in the *Schrems I*, also in the light of the revelations made by Edward Snowden concerning the activities of the United States intelligence services, and *Schrems II* judgments.

To the extent that the data transfer outside of the EU to a data processor in third countries entails additional risks in connection with different legal systems and applicable law in order to be in line with the provisions of the GDPR, the problem of this thesis is that the level of personal data protection of data subjects located in the EU according to the GDPR may not be outside the EU equivalent to that guaranteed in the Union. In addition, in the absence of the adequacy decision of protection referred to in Article 45 of the GDPR, the implementation of the safeguards specified in Article 46 of the GDPR is a complex and time-consuming process, the description of the safeguards in Chapter V of the GDPR is complex, which does not ensure legal clarity, requiring field-based knowledge of the implementation of these requirements in legislation, guidelines and case law for the implementation of the safeguards.

The purpose of the master's thesis is to find out whether and how the conditions for the transfer of personal data to data processors in third countries in Article 46 of the GDPR protect personal data, what are the main legal issues of these restrictions and whether and how it is possible to improve protection when transferring personal data to data processors in third countries.

The master's thesis seeks answers to the following questions:

1) What is the legislative background and concept of personal data protection in the European Union, taking into account, among other things, the extraterritorial scope and purposes of the GDPR?

2) What is the level of protection of Chapter V of the GDPR for the transfer of personal data to third countries, and do the appropriate safeguards provided for in Article 46 of the GDPR, using the example of standard contractual clauses, ensure the level of personal data protection provided for in the GDPR and compliance with the purposes of the GDPR?

3) What legal measures could ensure an equivalent level of protection of personal data when transferred to data processors in third countries?

A combination of historical, qualitative and comparative research methods is used to achieve the goal of the master's thesis. In terms of normative sources, attention is primarily paid to the provisions of the GDPR and Directive 95/46/EC, and to some extent also to EU legislation related to the right to data protection in the EU legal space. The GDPR and the Directive 95/46/EC, in terms of the subject of this thesis, have been most influenced by the decisions of the European Court of Justice *Schrems I* and *Schrems II*, in which the provisions are additionally examined. It should be noted that both judgments have had an impact on Directive 95/46/EC. However, several principles of case law and Directive 95/46/EC have been transferred to the GDPR and remained valid, and this is also reflected in the EDPB guidelines cited in the paper.

Several non-normative sources have also been used in the thesis, including comments on the GDPR, articles in legal publications and other scientific publications, positions, announcements of EU institutions, public statements of persons working in the field of data protection, working documents, press releases and policy announcements. The instructions of the European Commission, the European Data Protection Supervisor and, in particular, EDPB play an important role in the interpretation of the provisions of the GDPR. The analysis of the material obtained in the course of such data collection and processing, including the opinions of legal scholars studying the topic, contribute to the achievement of the thesis´ purpose, both in highlighting the wording and purpose of legislation, as well as in the analysis of implementation and issues.

During the analysis of the thesis, it became clear that the purpose of the GDPR to ensure the protection of personal data wherever it is used or processed is theoretically fulfilled. This results both from the territorial scope of application set out in Article 3 of the GDPR and from the

safeguards contained in Chapter V, which aim to ensure the protection of data when they are transferred to third countries. In addition, this legal approach also protects against data being taken out of the EU to be processed more freely in unrestricted jurisdictions.

The substantive problem in the protection of personal data manifests itself in a situation related to the second data transfer purpose of the GDPR. Namely, if the recipient of data in a third country that does not have an adequacy decision of protection is subject to the domestic legislation of the host country, which may not be in accordance with European law, it may make it impossible to comply with the restrictions and obligations imposed by the GDPR and reduce their effectiveness when implementing the protection mechanisms listed in Article 46 of the GDPR. For example, the conclusion of a contract with standard data protection clauses between two companies, a data transmitter located in the EU and a data receiver located in a third country, may not provide sufficient legal protection against the work of third country intelligence agencies. However, one of the purposes of Chapter V of the GDPR is to protect personal data from unauthorized access. This goal has also been emphasized by the practice of the European Court of Justice in the legal process of annulment of two contractual safeguards, Safe Harbor and Privacy Shield concluded between the EU and the USA. If the domestic legal order of the third country is in conflict with the principles of the GDPR, the personal data of European data subjects in the third country is not protected at a sufficient level in the sense of the protection standard provided for in the GDPR.

In order to reduce the risks associated with problems in the difference between the legal systems of the EU and third countries, the work has analyzed which measures could bring closer to an equivalent level of protection of personal data and the understanding of the right to data protection as a fundamental right similar to the EU standard. Although the storage of data in Europe has been proposed as an idea to maintain the level of data protection, the author of the paper does not see it as a suitable option. The principle of data localization would harm business and economic cooperation between many countries, and would also not be consistent with the idea of the GDPR to regulate data exchange and cooperation related to data movement between countries.

Certainly, one could consider offering facilitating measures to European data experts that would help evaluate the legal order and data safeguards of third countries. Such tools could be partially automated, and their use would allow to increase work efficiency and reduce possible human error. Also, if the legal system of some countries is such that excludes the possibility of data protection principles, such information could be publicly available to the data transferor from a reliable source

to avoid harm by transferring personal data to jurisdictions with low protection. Considering that nowadays small businesses also use a large number of cooperation partners in third countries, general awareness raising is very necessary.

Harmonization of data protection standards is one option that has also been proposed in the legal literature. This process can be complex, but in the long run it allows for a consistent understanding of data protection objectives and limitations without having to harmonize all national laws with a GDPR. Harmonization of data protection laws and standards requires a principled approach and cooperation and dialogue between different countries and international organizations regarding data protection goals and restrictions, which would allow preserving the specificities of countries, but applying them on a uniform basis.

The development of the data protection framework DPF has been briefly examined with possible solutions in connection with the EU-US data exchange, between which international data protection agreements have been in force and whose invalidation has significantly affected the implementation and interpretation of the safeguards of Chapter V of the GDPR. The main problem with the new EU-US data protection framework is its low assessment of adequacy and reliability by European institutions, which points to doubts about its validity and requires further discussion and improvements before its implementation. The short-term duration of the DPF framework would cause uncertainty and problems for both data processors and supervisory authorities, and if the framework does not ensure sufficient substantive protection against the processing of personal data, it may cause harm instead of benefit, especially during the short-term validity.

This master's thesis could help to better understand the principles of applying data protection mechanisms in connection with the transfer of personal data to third countries and clarify the complex EU data transfer rules, which are often difficult to interpret. The work could also explain the various guidelines and case law related to data protection mechanisms, which would help to better understand their implementation. Also, this work could make a valuable contribution in relation to the impact of the *Schrems I* and *Schrems II* judgments, which have significantly changed the principles of data transfer to third countries and cancelled the protection mechanisms that were in force on the basis of the GDPR. The work could provide an overview of the practical consequences of the Schrems judgments in the topic of data transfer and their impact on the protection of personal data both in the EU and outside it.

In connection with the problem of applying the data safeguards discussed in the paper, the harmonization of legislation in third countries could be considered in order to apply the principles of personal data protection in a uniform manner. Harmonization of legal acts may also include, for example, the specification of restrictions on the transfer of personal data or the creation of new data protection mechanisms that would ensure adequate protection of personal data. It can also mean developing guidelines, especially when new technologies are rapidly developing that require new regulations. Such guidelines would help companies dealing with personal data protection to understand and implement data protection mechanisms when transferring personal data to third countries, and they could be helpful to companies that process personal data and need to transfer it to third countries.

KASUTATUD KIRJANDUS

1) Aaronson, S. A. Data is different, and that's why the world needs a new approach to governing cross-border data flows. - Digital Policy, Regulation and Governance, 03/2019.
2) Aguilar, J. F. L. on behalf of the Committee on Civil Liberties, Justice and Home Affairs. Draft motion for a resolution to wind up the debate on the statement by the Commission pursuant to Rule 132(2) of the Rules of Procedure on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP)). (14.2.2023). – https://www.europarl.europa.eu/doceo/document/LIBE-RD-740749_EN.pdf, (27.02.2023).
3) Andmekaitse inspektisoon. Andmete edastamine välisriiki. (21.06.2021) – https://www.aki.ee/et/teenused-poordumisvormid/andmete-edastamine-valisriiki (30.03.2023).
4) Article 29 Data Protection Working Party Press release. The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data (02.12.2009). – https://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2009/pr_01_12_09_en.pdf (06.03.2023).
5) Article 29 Data Protection Working Party. Working Party on Police and Justice. The Future of Privacy - Joint Contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. (01.12.2009). – https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf (27.03.2023).
6) Bu-Pasha, S. Cross-border issues under EU data protection law with regards to personal data protection. Information & Communications Technology Law, 2017, 26(3).
7) Burri, M. Data flows and global trade law. Big data and global trade law. Cambridge University Press, 2020.
8) Carlson, M. Behind the Curve: *Schrems II* and the Need for Increased US Data Protections in a Global Economy. The Journal of Corporation Law, 2021/47.
9) Chander, A. Is Data Localization a Solution for *Schrems II*? – Journal of International Economic Law, 23(3), 2020.
10) Christakis, T. „Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 1). News and comments on EU law. (13.11.2020). –

European Law Blog. https://europeanlawblog.eu/2020/11/13/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-1/ (13.02.2023).

11) Cloud Act. Frequently Asked Questions. – US Departement of Justice. https://www.justice.gov/criminal-oia/page/file/1153466/download (20.04.2023).
12) Commission of the European Communities. First report on the implementation of the Data Protection Directive (95/46/EC). – COM(2003) 265 final, 15.05.2003.
13) Commission implementing decision (draft) pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework. 2022. – https://commission.europa.eu/document/e5a39b3c-6e7c-4c89-9dc7-016d719e3d12_en (29.03.2023).
14) Cooper, D., Vos, S., Szewczyk, B., Oberschelp de Meneses, A. Covington & Burling LLP. EU Cloud Initiatives in 2021 and 2022. (26.02.2021). - https://www.globalpolicywatch.com/2021/02/eu-cloud-initiatives-in-2021-and-2022/, (10.04.2023).
15) Council of Europe. Parties to Convention 108. - https://www.coe.int/en/web/data-protection/national-information (27.03.2023).
16) Daigle, B. and Khan, M. The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities. – Journal of International Commerce and Economics, 06/2020.
17) Data protection: European Commission launches the process towards adoption of the adequacy decision for the Republic of Korea. 16.06.2021. – European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964 (11.04.2023).
18) Determann, L. Adequacy of data protection in the USA: myths and facts. - International Data Privacy Law, 22.09.2016, 6 (3).
19) Dhont, J. X. Schrems II. The EU adequacy regime in existential crisis? – Maastricht journal of European and comparative law, 26(5).
20) Docksey, C. Four fundamental rights: finding the balance. – International Data Privacy Law, 2016/6(3).
21) Euroopa Andmekaitsenõukogu. Suunised 1/2019 määruse (EL) 2016/679 kohaste toimimisjuhendite ja järelevalvet teostavate asutuste kohta versioon 2.0. (04.06.2019). -

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_et.pdf (10.04.2023).

22) Euroopa andmekaitseõiguse käsiraamat. – Euroopa Liidu Põhiõiguste Amet ja Euroopa Nõukogu. Luxembourg: Euroopa Liidu Väljaannete Talitus, 2020.
23) Euroopa Komisjon. Andmekaitse EL-is. – https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_et (21.11.2022).
24) Euroopa Komisjoni teatis Euroopa Parlamendile ja Nõukogule. Isikuandmete vahetamine ja kaitsmine globaliseerunud maailmas. – 2017 COM/2017/07 final, 10.01.2017.
25) Euroopa Komisjoni raport. 15.05.2003. First report on the implementation of the Data Protection Directive (95/46/EC). – https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52003DC0265&from=EN (07.02.2023).
26) Euroopa Liidu Kohus. Pressiteade nr 91/20, Luxembourg, 16.07.2020. Kohtuotsus (kohtuasi C-311/18) Data Protection Commissioner vs. Maximillian Schrems ja Facebook Ireland. Euroopa Kohus tunnistab kehtetuks otsuse 2016/1250 isikuandmete kaitse piisavuse kohta ELi-USA andmekaitseraamistikus Privacy Shield.
27) Euroopa Parlament. USA Riikliku Julgeolekuagentuuri järelevalveprogramm, ELi liikmesriikide jälgimisasutused ning mõju ELi kodanike põhiõigustele. P7 TA(2014)0230 9.11.2017. – ELT C 378/104.
28) European Commission. Adequacy decisions. How the EU determines if a non-EU country has an adequate level of data protection. - https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (21.03.2023).
29) European Commission. Data protection in the EU. – https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en (21.11.2022).
30) European Commission. European Commission adopts new tools for safe exchanges of personal data. (04.06.2021). – https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847 (10.04.2023).
31) European Commission. International data flows: Commission launches the adoption of its adequacy decision on Japan. (05.09.2018). – https://ec.europa.eu/commission/presscorner/detail/en/IP_18_5433 (27.09.2019).
32) European Commission. Questions & Answers: EU-U.S. Data Privacy Framework, draft adequacy decision. 13.12.2022. - https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_7632 (29.03.2023).

33) European Data Protection Board. Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679. (25.05.2018). – https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en (10.04.2023).
34) European Data Protection Board. EDPB adopts final version of Recommendations on supplementary measures, letter to EU Institutions on the privacy and data protection aspects of a possible digital euro and designates three EDPB Members to the ETIAS Fundamental Rights Guidance Board. (21.06.2021). – https://edpb.europa.eu/news/news/2021/edpb-adopts-final-version-recommendations-supplementary-measures-letter-eu_en (10.04.2023).
35) European Data Protection Board. Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR. (14.02.2023). – https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_en (11.03.2023).
36) European Data Protection Board. Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), 12.11.2019. - https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf (10.04.2023).
37) European Data Protection Board. Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework. (28.02.2023). - https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf (10.04.2023).
38) European Data Protection Board. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Version 2.0, (18.06.2021). – https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf (10.04.2023).
39) European Data Protection Board. Recommendations 02/2020 on the European Essential Guarantees for surveillance measures. (10.11.2020). – edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf (europa.eu) (10.04.2023).

40) European Data Protection Board. Statement 02/2022 on personal data transfers to the Russian Federation. (12.07.2022). – https://edpb.europa.eu/system/files/2022-07/edpb_statement_20220712_transferstorussia_en.pdf (10.04.2023).
41) European Data Protection Supervisor. Data Protection. - https://edps.europa.eu/data-protection/data-protection_en (25.11.2022).
42) European Data Protection Supervisor. Data Protection. – https://edps.europa.eu/data-protection/data-protection_en#Cross_border (26.02.2023).
43) European Data Protection Supervisor. Privacy – a fundamental right. – https://edps.europa.eu/data-protection/data-protection_en#Cross_border (26.02.2023).
44) European Parliament. Understanding EU data protection policy. – https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/698898/EPRS_BRI(2022)698898_EN.pdf (10.04.2023).
45) Evans, M., White, L., Daddar, S., Kessler, D, Ross, S. L., Ritzer, C. Schrems II landmark ruling: A detailed analysis. 07/2020. – Norton Rose Fulbright. https://www.nortonrosefulbright.com/en-jp/knowledge/publications/ad5f304c/schrems-ii-landmark-ruling-a-detailed-analysis (10.04.2023).
46) Goddard, M. The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. International Journal of Market Research, 2017, 59(6), pp.704-705.
47) Gulczyńska, Z. A certain standard of protection for international transfers of personal data under the GDPR. - International Data Privacy Law, 11(4), 11/2021.
48) Hamilton, D. S., Quinlan, J. P. Annual Survey of jobs, trade and investment between the United States and Europe 2020. – The Transatlantic Economy.
49) Hill, J. The growth of data localization post-Snowden: Analysis and recommendations for U.S. policymakers and business leaders. In The Hague Institute for Global Justice, Conference on the Future of Cyber Governance. 05/2014.
50) Houser, K.A., Voss, W.G. Personal data and the GDPR: providing a competitive advantage for US companies. – American Business Law Journal, 19.06.2020.
51) International Association of Privacy Professionals and Ernst & Young, Annual Privacy Governance Report 2019. – https://iapp.org/resources/article/iapp-ey-annual-governance-report-2019/ (12.12.2022).
52) Karistusseadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seadus (Euroopa Liidu õigusest tulenevad rahatrahvid) 94 SE, 22.02.2023. – Riigikogu.

https://www.riigikogu.ee/tegevus/eelnoud/eelnou/1bfa1944-2de6-449d-a788-887bc84cfd0f/Karistusseadustiku%20muutmise%20ja%20sellega%20seonduvalt%20teiste%20seaduste%20muutmise%20seadus%20(Euroopa%20Liidu%20%C3%B5igusest%20tulenevad%20rahatrahvid) (20.04.2023).

53) Kuner, C, Bygrave, L.A., Docksey, C., Drechsler, L., Tosoni, L. The EU General Data Protection Regulation: A Commentary/Update of Selected Articles. – Update of Selected Articles, 04.05.2021.

54) Kuner, C. Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law. – International Data Privacy Law, 5/2015.

55) Kuner, C. Reality and illusion in EU data transfer regulation post Schrems. - German Law Journal, 2017, 18(4).

56) Kuner, C. The Schrems II judgment of the Court of Justice and the future of data transfer regulation. European Law Blog. – European Law blog, (17), 17.07.2020.

57) Lama, A., Auty, C. M. Is Privacy Shield 2.0 on the horizon? (11.10.2022). – Bryan Cave Leighton Paisner. https://www.bclplaw.com/en-US/events-insights-news/is-privacy-shield-20-on-the-horizon.html (10.04.2023).

58) Lenaerts, K, Gutiérrez-Fons, J.A. To say what the law of the EU is: methods of interpretation and the European Court of Justice. Academy of European Law. Distinguished Lectures of the Academy. 2013/9.

59) Lõhmus, U. Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne 2012. – https://pohiseadus.ee/sisu/3497/paragrahv_26 (27.02.2023).

60) Lynskey, O. The foundations of EU data protection law. – Oxford University Press, 2015.

61) New US Executive Order unlikely to satisfy EU law. (07.10.2022). NOYB – European Center for Digital Rights. – https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law (10.04.2022).

62) OECD. Report on the cross-border enforcement of Privacy Laws. – The Organisation for Economic Co-operation and Development, 10/2006.

63) OneTrust DataGuidance. US Privacy Laws. Comply with US Privacy Laws. - https://www.dataguidance.com/comparisons/usa-privacy-laws (10.04.2023).

64) Parkins, D. The world's most valuable resource is no longer oil, but data. (06.05.2017). – The Economist. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (26.02.2023).

65) Perlroth, N., Tsang, A., Satariano, A. Marriott hacking exposes data of up to 500 million guests. 11/2018. – The New York Times. https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html (10.04.2023).
66) Peukert, C., Bechtold, S., Batikas, M., Kretschmer, T. Regulatory spillovers and data governance: Evidence from the GDPR. – Marketing Science, 41(4), 2022.
67) Pringle, R. „Data is the new oil“: Your personal information is now the world’s most valuable commodity. (25.08.2017). – CBC News. https://www.cbc.ca/news/science/data-is-the-new-oil-1.4259677 (26.02.2023).
68) Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (11.07.2013). – https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 (25.11.2022).
69) Rosentau, M. The General Data Protection Regulation and its Violation of EU Treaties. Juridica International, 27/2018.
70) Rutherford, M. The CLOUD Act: Creating Executive Branch Monopoly Over Cross-Border Data Access. – Berkeley Technology Law Journal, 2019, 34(4).
71) Rydning, J., Reinsel, D., Gantz, J. The digitization of the world from edge to core. – Framingham: International Data Corporation. 11/2018.
72) Sanchez-Rola, I., Dell'Amico, M., Kotzias, P., Balzarotti, D., Bilge, L., Vervier, P.A. and Santos, I. Can i opt out yet? GDPR and the Global Illusion of Cookie Control. – In Proceedings of the 2019 ACM Asia conference on computer and communications security. 07/2019.
73) Schwartz, P.M., Peifer, K.N. Transatlantic data privacy law. – Georgetown Law Journal, 106, 2017.
74) Solove, D.J. Understanding privacy. – Harvard University Press, 05/2008.
75) Stanford Cyber Policy Center. Translation: Cybersecurity Law of the People’s Republic of China (Effective June 1, 2017). (29.06.2018). – https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/ (10.04.2023).
76) Statement by TACD on the announcement of a New EU-U.S. Personal Data Transfers Framework. (07.10.2022). – Trans Atlantic Consumer Dialogue. https://tacd.org/statement-by-tacd-on-the-announcement-of-a-new-eu-u-s-personal-data-transfers-framework/ (10.04.2022).
77) Svantesson, D.J.B. The extraterritoriality of EU data privacy law – its theoretical justification and its practical effect on US businesses. – Stanford Journal of International Law, Nr 1 (2014).

78) The Schrems II Decision: The Day After. International Association of Privacy Professionals IAPP. – LinkedIn. https://www.linkedin.com/posts/iapp---international-association-of-privacy-professionals_the-schrems-ii-decision-the-day-after-activity-6689891497254420480-wy00 (10.04.2023).
79) The White House. Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities. (07.10.2022). – https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/ (29.03.2023).
80) Tiffith, L. IAB Applauds President Biden's Executive Order Addressing Transatlantic Data Flows. (07.10.2022). – https://www.iab.com/news/iab-applauds-president-bidens-executive-order-addressing-transatlantic-data-flows/ (29.03.2023).
81) Tovino, S.A. The HIPAA privacy rule and the EU GDPR: illustrative comparisons. – Seton Hall Law Review. UNLV Williams S. Boyd School of Law, 2017/47.
82) Trueman, C. EU-US data sharing agreement: Is it a done deal? (12.10.2022). – https://www.computerworld.com/article/3676284/eu-us-data-sharing-agreement-is-it-a-done-deal.html (29.03.2023).
83) U.S. Chamber of commerce. Business Without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity. – Hunton & Williams. https://www.huntonak.com/images/content/3/0/v3/3086/Business-without-Borders.pdf (10.04.2023).
84) Voss, W.G. Transatlantic Data Transfer Compliance. 2022. – Boston University Journal of Science & Technology Law, 2022/28.
85) Weiss, M. A., Archick, K. U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield. – Congressional Research Service. 19.05.2016.

KASUTATUD ÕIGUSAKTID

86) 4. juuni 2021. aasta Euroopa Komisjoni rakendusotsus 2021/914 kolmandatesse riikidesse isikuandmete edastamise lepingu tüüptingimuste kohta vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) 2016/679. – ELT L 199/31, lk 31-61.

87) 12. juuli 2016. aasta Euroopa Komisjoni rakendusotsus (EL) 2016/1250 isikuandmete kaitse piisavuse kohta ELi-USA andmekaitseraamistikus Privacy Shield vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ 1. lisa (Privacy Shield otsus). – ELT L 207/1 (2016/4176).
88) 23. jaanuari 2019. aasta Euroopa Komisjoni rakendusotsus (EL) 2019/419, isikuteabe kaitse seaduse raames Jaapani pakutava isikuandmete kaitse piisavuse kohta vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) 2016/679 (teatavaks tehtud numbri K(2019) 304 all) (EMPs kohaldatav tekst). – ELT L 76/1, lk 1-58.
89) 23. oktoobri 2018. aasta Euroopa Parlamendi ja Nõukogu määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ. – ELT L 295/39, lk 39-98.
90) 24. oktoobri 1995. aasta Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. – ELT L 281, 23.11.1995, lk 31-50.
91) 27. aprilli 2016. aasta Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK. – ELT L 119/89, 4.5.2016, lk 89-131.
92) 27. aprilli 2016. aasta Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). – ELT L 119, 4.5.2016, lk 1-88.
93) Council of Europe. Convention 108+: Convention for the Protection of Individuals with Regard to the Processing of Personal Data. 2018. – https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (24.03.2023).
94) Eesti Vabariigi põhiseadus. – RT I, 15.05.2015, 2.
95) Euroopa Komisjoni 26.07.2000 otsus nr 2000/520/EÜ vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ piisava kaitse kohta, mis on ette nähtud programmi Safe Harbor põhimõtetega ja sellega seotud korduma kippuvate küsimustega, mille on välja andnud Ameerika Ühendriikide kaubandusministeerium. – ELT L 215, 25.08.2000, lk 7-47.

96) Euroopa Liidu põhiõiguste harta. – ELT L 2012/C 326/02, lk 391–407.
97) Euroopa Liidu toimimise lepingu konsolideeritud versioon. – ELT C 326, lk 1-390.
98) Inimõiguste ja põhivabaduste kaitse konventsioon. – RT II 2010, 14, 5.
99) Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon. Vastu võetud 28.01.1981. – RT II 2001, 1, 3.
100) Isikuandmete kaitse seadus. – RT I, 04.01.2019, 11.
101) Lissaboni leping. – ELT 2007/C 306/1.
102) ÜRO inimõiguste ülddeklaratsioon (Peaassamblee resolutsioon 217A). – A/RES/217.
103) Montreux Declaration. The protection of personal data and privacy in a globalized world: a universal right respecting diversities. - https://edps.europa.eu/sites/edp/files/publication/05-09-16_montreux_declaration_en.pdf (27.03.2023).

Välisriikide õigusaktid:

104) Lei Geral de Proteção de Dados (LGPD). https://lgpd-brazil.info/ (10.04.2023).
105) Venemaa Föderaalseadus “Isikuandmete kohta”. – N 152-F3.
106) Clarifying Lawful Overseas Use of Data Act, H.R.1625 (Cloud Act). - 115th Congress. https://www.congress.gov/bill/115th-congress/house-bill/1625/text.

KASUTATUD KOHTUPRAKTIKA

Euroopa Inimõiguste Kohtu praktika:

107) ECHR 37138/14, *Szabó and Vissy v Hungary*, 12.01.2016.
108) ECHR nos 58170/13 jt, *Big Brother Watch and Others v. the United Kingdom*. 13.09.2018.

Euroopa Kohtu praktika:

109) EKo C-191/15, *Verein für Konsumenteninformation versus Amazon EU Sàrl*. ECLI:EU:C:2016:612.
110) EKo C-230/14, *Weltimmo s.r.o. versus Nemzeti Adatvédelmi és Információszabadság Hatóság*. ECLI:EU:C:2015:639.
111) EKo C-311/18, *Data Protection Commissioner versus Facebook Ireland Limited, Maximillian Schrems*, ECLI:EU:C:2020:559.

112) EKo C-362/14, *Maximillian Schrems versus Data Protection Commissioner*, ECLI:EU:C:2015:650.
113) EKo C-511/18, *La Quadrature du Net and Others v Premier ministre and Others*, ECLI:EU:C:2020:791.
114) EKo C–623/17, *Privacy International versus Secretary of State for Foreign and Commonwealth Affairs and others,* ECLI:EU:C:2020:790.

Euroopa Kohtu kohtujuristi ettepanekud:

115) EK C-311/18, *Data Protection Commissioner versus Facebook Ireland Limited, Maximillian Schrems*, kohtujurist Saugmandsgaard Øe, H. ettepanek, punktid 124-126.
116) EK C-362/14, *Maximillian Schrems versus Data Protection Commissioner*, kohtujurist Y. Bot´i ettepanek.

MUUD KASUTATUD ALLIKAD

117) Advocate general of the CJEU, (07.07.2020). Eurofound. – https://www.eurofound.europa.eu/observatories/eurwork/industrial-relations-dictionary/advocate-general-of-the-cjeu (05.02.2023).
118) Amazon Web Service. Privacy Notice. (10.01.2023). – https://aws.amazon.com/privacy/, (03.04.2023).
119) Antonova, J. Euroopa andmekaitsereformist läbi keeleprisma. – Õiguskeel 1/2015.
120) Chai, W. Google Analytics. Tech Target, Business Analytics. (04/2021). – https://www.techtarget.com/searchbusinessanalytics/definition/Google-Analytics, (10.04.2023).
121) Dropbox Help centre. Where is my data stored? - https://help.dropbox.com/security/physical-location-data-storage, (07.02.2023).
122) Open AI Privacy Policy. 23.01.2023. – https://openai.com/policies/privacy-policy. (04.04.2023).