TARTU ÜLIKOOL
SOTSIAALTEADUSTE VALDKOND
ÕIGUSTEADUSKOND
Üldosakond
IT-õiguse programm

Carel Kivimaa

EUROOPA KOMISJONI RAKENDUSOTSUSE (EL) 2016/1250 KEHTIVUST MÕJUTAVAD OLULISED ARENGUD USA JA EUROOPA LIIDU ÕIGUSES

Magistritöö

Juhendajad

LL.M Mati Kaalep

J.S.D Helen Eenmaa-Dimitrieva

Tartu

2017

SISUKORD

SISSEJUHATUS....4

1. Atlandiülene isikuandmete edastamine....11

1.1. Isikuandmete kolmandatesse riikidesse edastamise õiguslik alus....12

1.1.1. Artikkel 26(1) erandid....14

1.1.2. Piisavad tagatised....15

1.1.3. Adekvaatsusotsus....16

1.2. USA kui ebapiisava andmekaitse tasemega riik....18

1.2.1. Andmekaitse ja privaatsusõiguse vahekorrast....18

1.2.2. Andmete privaatsusõigus USA õiguskorras ja selle pakutav isikuandmete kaitse tase EL-i andmekaitse seisukohast....24

1.2.2.1. Andmete privaatsusõigus föderaalsel tasandil....24

1.2.2.2. Andmete privaatsusõigus osariikide tasandil....29

1.2.2.3. Järeldus USA andmekaitse taseme kohta....30

1.3. Atlandiüleses andmevahetuse õiguslik raamistik....32

1.3.1. Safe Harbor ja kohtuasi C-362/14 Schrems v. Data Protection Commissioner....33

1.3.2. Safe Harbor'i lõpp ja Privacy Shield'i algus....40

1.3.2.1. Privacy Shield õigusraamistik....42

2. Komisjoni rakendusotsuse 2016/1250 alusel toimuva isikuandmete edastamise järjepidevust ohustavad tegurid....44

2.1. USA uus administratsioon, kui pärast otsuse 2016/1250 vastuvõtmist esinenud USA-st tulenev oluline asjaolu Privacy Shield programmi jätkuva piisava kaitse taseme tagamise positsioonilt....46

2.1.1. Avalike organite kinnitused Privacy Shield programmi käsitleva adekvaatsusotsuse eeldustena....46

2.1.1.1. PPD-28 roll Privacy Shield programmis....49

2.1.1.2. Presidentaalsed seadusandlikud aktid USA õiguses....50

2.1.1.3. PPD-28 õiguslik tähendus tänases USA-s....51

2.1.1.4. Eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon (PCLOB) ja Privacy Shield ombudsman 53
2.1.2. President Trumpi 25. jaanuari täidesaatev korraldus ja selle mõju Privacy Shield'ile 55
2.1.3. Vahekokkuvõte 57
2.2. Privacy Shield programmi põhimõtete vastavus GDPR-ile 58
2.2.1. Töötlemise põhimõtted 60
2.2.1.1. Töötlemise seaduslikkus, õiglus ja läbipaistvus 62
2.2.1.2. Eesmärgipärane töötlemine ja eesmärk kui töötlemist piirav element 67
2.2.1.3. Säilitamise piiramise põhimõte 70
2.2.1.4. Turvalisuse põhimõte 71
2.2.1.5. Andmesubjekti kontroll oma andmete üle 72
2.2.2. Vahekokkuvõte 73
KOKKUVÕTE 75
Summary 82
Lühendid 89
Kasutatud kirjandus 91
Kasutatud õigusaktid 93
Kasutatud kohtupraktika 95
Muud kasutatud materjalid 96

SISSEJUHATUS

Andmed, eriti isikuandmed, on kahekümne esimese sajandi nafta! Sellist kujundit kasutavad informatsioonitehnoloogia -ning majandusasjatundjad isikuandmete majanduslikule väärtusele viidates juba aastaid.[1] Andmed käesoleval sajandil on nagu nafta 18. sajandil: tohutu kasutamata väärtusallikas, mis selle potentsiaali äratundjale ja rakendajale suurt tulu võib tuua.[2]

Isikuandmete väärtus on niivõrd kõrgele tõusnud tänu infotehnoloogia kiirele arengule ja laialdasele levikule. Kõrgtehnoloogilised nutiseadmed on odavamad kui kunagi varem ning see on avanud *online*-maailma tohutule hulgale inimestele, kelle arv kasvas eelmise aasta lõpuks 3, 4 miljardini.[3] See loob interneti sisuloojatele massiivse kliendibaasi, kes iga uue kasutajakonto, guugeldamise ning isegi hiireklõpsuga endast järjest rohkem informatsiooni maha jätavad.

Elektroonilised andmed, mis isikutest serveritesse ning andmebaasidesse talletatakse ning mida erinevatest eesmärkidest lähtudes andmetöötlejad andmesubjektidele teenuste pakkumiseks ja profileerimiseks töötlevad, võimaldavad nende kohta teha järjest täpsemaid ning üksikasjalikumaid järeldusi. Selline praktika aga vähendab tahes-tahtmata isikute kontrolli enda andmete üle ehk väheneb andmesubjektide võimalus iseennast teistele kättesaadava informatsiooni kaudu määratleda. Isiku õigust end informatsiooniliselt määratleda kaitseb Euroopa Inimõiguste Konventsiooni artikkel 8.[4]

Problemaatilisust isikute kohta käivate andmete töötlemise ning isiku, kui õiguste ja vabaduste subjekti vahelises seoses on nähtud juba ammu enne internetiajastut. Näiteks, Saksamaa Föderaalne Konstitutsioonikohus (*Bundesverfassungsgericht*) ütles juba 1983. aastal kuulsas rahvaloenduse otsuses (*Volkszählungsurteil*), et andmete automaatseks kogumiseks ja

---

[1] M. Palmer; *Data is the new oil*; ANA Marketing Maestros blog 03.11.2006; kättesaadav: http://ana.blogs.com/maestros/2006/11/data_is_the_new.html (01.05.2017); P. Rotella; *Is data the new oil?*; Forbes 02.04.2012; kättesaadav: http://www.forbes.com/sites/perryrotella/2012/04/02/is-data-the-new-oil/#2caf418677a9 (01.05.2017); C. Jablonski; *Data is the oil of 21st century: Gartnersupply chain exe* ; Trade Shift blog 15.05.2015; kättesaadav: http://blog.tradeshift.com/data-oil-21st-century-gartner-supply-chain-exec/ (01.05.2017); C. Liem, G. Petropoulos; *The economic value of personal data for online platforms, firms and consumers*; Bruegel blog 14.01.2016; kättesaadav: http://bruegel.org/2016/01/the-economic-value-of-personal-data-for-online-platforms-firms-and-consumers/ (01.05.2017)

[2] J. Toonders; *Data is the new oil of digitaal economy*; Wired; kättesaadav: http://www.wired.com/insights/2014/07/data-new-oil-digital-economy/ (01.05.2017)

[3] Live Internet Stats; *Internet Users*; kättesaadav: http://www.internetlivestats.com/internet-users/ (01.05.2017)

[4] A. Nõmper, E. Tikk; *Informatsioon ja õigus*; Juura: Tallinn 2007; lk 38-39; M. Männiko; *Õigus privaatsusele ja Andmekaitsele*; Juura: Tallinn 2011; lk 18-19

töötlemiseks tuleb luua selged põhimõtted ning reeglid, mis tagaksid, et nende andmetega seotud isikud ei muutuks vaid pelgaks andmete objektiks.[5]

Esimesed seadused, mida võiks pidada andmekaitsealasteks, pärinevad juba 1970ndatest aastatest. Küllaltki varsti pärast seda hakati rakendama ka rahvusvahelisi andmekaitse ning andmete edastamist käsitlevaid regulatsioone. Nende eesmärgiks oli tagada ühtlane andmekaitse tase erinevates riikides ja lähtuvalt andmete majanduslikust kasulikkusest, ka andmete edastamise piirangute vältimine riikide vahel.

Kuigi andmete, eriti isikuandmete, kaitse vajalikkuses on riigid enam-vähem üksmeelel[6], ei läheneta sellele sugugi sarnaselt. Erinev lähenemine isikuandmete kaitsele Ameerika Ühendriikides ning Euroopa Liidus (edaspidi „EL“) ongi käesoleva töö põhiline lähtekoht.

Euroopa andmekaitseõigus põhineb Euroopa Parlamendi ja nõukogu direktiivil 95/46/EÜ (edaspidi „direktiiv“ ja „direktiiv 95/46“)[7], mida peetakse kõige suuremat mõju avaldanud andmekaitse instrumendiks.[8] Reguleerides põhjalikult isikuandmete töötlemist[9], kusjuures terminid „isikuandmed“[10] ja „töötlemine“[11] on defineeritud väga laialt, ning piirates isikuandmete edastamist riikidesse ja piirkondadesse, mis direktiiviga pakutavale andmekaitsetasemele ei vasta, on EL näiteks kõrgetasemelise andmekaitse rakendamisest. Andmekaitse ning laiemalt privaatsuse olulisus eurooplastele nähtub ka sellest, et EL-i aluslepingute kohaselt on isiku õigus andmekaitsele kuulutatud iseseisvaks põhiõiguseks.[12]

Ameerika Ühendriikides ei käsitleta andmekaitset üldisest privaatsusõigusest eraldi ja see, mida EL-is nimetatakse andmekaitseks, omab teisel pool Atlandit pigem andmete või informatsiooni privaatsuse nime.[13] Informatsiooni privaatsust reguleerivad seadused lähenevad isikuandmetele

---

[5] Saksa Konstitutsioonikohtu 15.12.1983 otsus Volkszählungsurteil; openJur 2012; punkt 185; kättesaadav: http://openjur.de/u/268440.html (01.05.2017)

[6] J. Clark, K. Lucente;; *Data Protection Laws of the World – Full Handbook*; DLA Piper, 2017, lk 4

[7] Euroopa Parlamendi ja nõukogu 24.10.1995. a direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta; ELT L 281, 23.11.1995, lk 31-50.

[8] C. Kuner; *Transborder Data Flow Regulation and Data Privacy Law*; Oxford University Press; Oxford, 2013; lk 40

[9] Direktiiv 95/46 artikkel 3(1)

[10] Direktiiv 95/46 artikkel 2(a) kohaselt on isikuandmed igasugune teave tuvastatud või tuvastatava isiku (andmesubjekti) kohta. Tuvastatav isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige isikukoodi põhjal või ühe või mitmele tema füüsilisele, füsioloogilisele, vaimsele, majanduslikule, kultuurilisele või sotsiaalsele identsusele omase joone põhjal.

[11] Direktiivi 95/46 artikkel 2(b) kohaselt on isikuandmete töötlemine iga isikuandmetega tehtav toiming või toimingute kogum, olenemata sellest, kas see on automatiseeritud või mitte, näiteks kogumine, salvestamine, korrastamine, säilitamine, kohandamine või muutmine, väljavõtete tegemine, päringu teostamine, kasutamine, üleandmine, levitamine või muul moel avaldamine, ühitamine või ühendamine, sulgemine, kustutamine või hävitamine

[12] Euroopa Liidu Põhiõiguste Harta (edaspidi ELPH) artikkel 8(1) sätestab: „Igaühel on õigus oma isikuandmete kaitsele“

[13] R. Ku, R. Shih; *Data Privacy as a Civil Right: The EU Gets it?*; Kentucky Law Journal, Vol 103 nr 3; 2014/2015; lk 396

õigusliku kaitse andmisel EL-ist erinevalt. USA õiguses puuduvad sellised üldised määratlused nagu „isikuandmed“ või „töötlemine“. USA vastav regulatsioon on EL-i poolt vaadatuna lünklik, sest õiguslikku kaitset pakutakse vaid sellist tüüpi isikuandmetele, mille piiranguteta töötlemine ja kogumine võib kaasa tuua suuremat kahju – näiteks finantsandmed ja meditsiiniandmed. Selline fragmentaarne lähenemine isikuandmete kaitsele ei vasta EL-i standarditele ning seega, vastavalt kehtivale EL-i õigusele, ei tohiks EL-ist isikuandmete ilma piiranguteta edastamist USA-sse toimuda.

Samas on tänapäeval ülimalt oluline võimaldada EL-i ja USA vahel võimalikult piirangute vähest Atlandiülest andmete, sealhulgas isikuandmete, vahetamist.[14] Nimelt moodustab Ameerika Ühendriikide ning EL-i vaheline kaubandus maailma SKT-st üle 50 protsendi[15] ning digitaalmajanduse osakaal võtab aasta-aastalt sellest üha suurema osa.[16] Selle tugeva majandussideme püsimise eelduseks on modernse vabakaubanduse kontekstis ka võimalikult vaba Atlandiülene isikuandmete edastamine.[17]

Võimalikult vaba isikuandmete EL-ist USA-sse edastamise eesmärki silmas pidades on pooled tänaseks suutnud sõlmida juba teise õigusraamistiku, millega liitunud ning milles sätestatud isikuandmete töötlemise reegleid rakendavad USA ettevõtted võivad EL-ist edastatavaid isikuandmeid ilma täiendavaid tagatisi andmata töödelda. Praegu kasutatav raamistik kannab nime *Privacy Shield* ning Euroopa Komisjoni (edaspidi „Komisjon“) rakendusotsuse (EL) 2016/1250[18] (edaspidi „rakendusotsus 2016/1250“) kohaselt on andmesubjektide, kelle isikuandmeid *Privacy Shield* programmi alusel USA-sse edastatakse, andmekaitseõigused tagatud samaväärselt EL-i õigusega.[19]

Privacy Shield ning rakendusotsus 2016/1250 on varasema analoogse õigusraamistiku *Safe Harbor* ja rakendusotsuse 2000/520/EÜ[20] (edaspidi „rakendusotsus 2000/520“) täiendatud ning

---

[14] B. M. Marcinkowski; *Privacy Paradox(es): In Search of a Transatlantic Data Protection Standard*; Ohio State Law Journal, Vol 74 nr 6, lk 1170

[15] Euroopa Liidu delegatsioon USA-s; *EU-US facts & figures*; kättesaadav: http://www.euintheus.org/what-we-do/eu-us-facts-figures/ (01.05.2017); Business Coalition for Transatlantic Trade; *Economic Benefits of a Transatlantic Trade and Investment Partnership*; kättesaadav: http://www.transatlantictrade.org/faqs/economic-benefits-of-a-transatlantic-trade-and-investment-partnership/ (01.05.2017)

[16] J. Meltzer; *The importance of the internetand transatlantic dataflows for U.S. and EU trade and investment*; Global Economy & Development working paper 79, oktoober 2014; lk 5; kättesaadav: http://www.brookings.edu/~/media/research/files/papers/2014/10/internet-transatlantic-data-flows-meltzer/internet-transatlantic-data-flows-version-2.pdf (01.05.2017)

[17] *Ibid*, lk 8

[18] Euroopa Komisjoni rakendusotsus (EL) 2016/1250, 12. juuli 2016, isikuandmete kaitse piisavuse kohta ELi-USA andmekaitseraamistikus Privacy Shield vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ, ELT L 207, 01.08.2016, lk 1-112

[19] Rakendusotsus 2016/1250 artikkel 1

[20] Euroopa Komisjoni otsus, 26. juuli 2000, 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

põhjalikum versioon. Euroopa Kohus (edaspidi „EK“) leidis oktoobris 2015 otsuses C-362/14, *Schrems v Data Protection Commissioner,* et *Safe Harbor* raamistik siiski ei taga isikuandmete kaitset nõutud tasemel ning tunnistas seega ka rakendusotsuse 2000/520 kehtetuks.[21]

Ilma *Safe Harbor*'i põhimõtteid sisuliselt hindamata, leidis EK, et *Safe Harbor* ei kaitse isikuandmeid USA valitsuse salajaste luureprogrammide eest.[22] Tähelepanu pälvinud luureprogrammid pärinesid rakendusotsuse 2000/520 tegemise järgsest ajast ning see oli ilmselt ka EK ajendiks otsuses C-362/14 *Schrems* rõhutada, et kolmandate riikide õiguskorda või rahvusvahelisi kohustusi andmekaitse taseme poolest piisavaks hindavaid rakendusotsuseid (edaspidi „adekvaatsusotsused“) on vaja regulaarselt kontrollida.[23] Sellega nõustus EK kohtujuristi Yves Bot arvamusega, kes juhtis tähelepanu asjaolule, et kolmandate riikide andmekaitse taseme kohta tehtud Komisjoni otsused on teistest Komisjoni otsustest oluliselt erinevad, sest nende hilisem kehtetus ei pruugi tuleneda Komisjoni eksimusest otsuse vastuvõtmise ajal, vaid adekvaatsusotsuse tühisuse võib põhjustada ka muutused hinnatava kolmanda riigi õiguslikus ja faktilises olukorrast või muud hilisemad faktilised muutused ja asjaolud.[24]

Rakendusotsuses 2016/1250 on selle seisukohaga juba arvestatud ning sätestatud reegel, mille kohaselt korraldab Komisjon kord aastas kontrolle ning hindab *Privacy Shield* raamistiku poolt pakutava isikuandmete kaitse taseme jätkuvat piisavust.[25] Lisaks on rakendusotsuses, artiklitest 4(2) ja 4(3) tulenevalt, ka liikmesriikidel kohustus teavitada Komisjoni, kui selguvad asjaolud, mis viitavad *Privacy Shield* programmi ebapiisavale andmekaitse tasemele.

Kuna adekvaatsusotsuse alusel isikuandmete järjepidev edastamine EL-ist USA-sse on mõlemale poolele selle tohutu majandusliku tähenduse tõttu oluline, on oluline ka võimalikult varakult tuvastada kehtivas Atlandiülest isikuandmete edastamist võimaldavas õigusraamistikus probleemid, mille adresseerimata jätmine tähendaks vastava rakendusotsuse tühisust ning adekvaatsusotsuse alusel toimuva isikuandmete edastamise lakkamist.

Käesoleva töö eesmärk ongi tuvastada ning juhtida tähelepanu pärast rakendusotsuse 2016/1250 jõustumist aset leidnud ning aset leidvatele olulistele muutustele USA ja EL-i õiguskorras, mille adresseerimata jätmine ning mille suhtes ennetava tegevuse teostamata

küsimustega, mille on välja andnud Ameerika Ühendriikide kaubandusministeerium; 2000/520/EÜ. – ELT L 215/7, 25.08.2000, lk 119-138

[21] EK 6.10.2015 otsus asjas C-362/14 *Schrems v Data Protection Commssioner*

[22] *Ibid* p 90-95

[23] EK C-362/14 *Schrems*, punktid

[24] EK C-362/14, *Schrems*, kohtujuristi Yves Bot ettepanek, punktid 131-137

[25] Rakendusotsus 2016/1250 artikkel 4(4)

jätmine võib taaskord kulmineeruda Atlandiülese isikuandmete edastamise õigusraamistiku blokeerimisega EK poolt selle andmekaitse taseme ebapiisavuse tõttu.

Arvestades pärast rakendusotsuse 2016/1250 vastuvõtmist toimunud ning peagi toimuvaid asjaolusid, millel võib olla oluline mõju rakendusotsuse kehtivusele, on autori arvates tähelepanuväärseid sündmusi kaks: USA uus administratsioon president Donald Trumpi juhtimisel ning direktiivi 95/46 asendamine andmekaitse üldmäärusega[26] (edaspidi „GDPR“) mais 2018.

Jälgides *Privacy Shield* õigusraamistiku struktuuri, avaldavad nimetatud muutused mõju õigusraamistiku erinevatel tasanditel – esiteks, USA uus administratsioon juhib kogu valitsussektorit lähtuvalt oma poliitikast ja maailmavaatest ning sellega võivad kaasneda ebakindlused eelmise administratsiooni poolt *Privacy Shield* programmi dokumentides antud kinnituste ning lubaduste osas ja teiseks, GDPR-iga muutub adekvaatsusotsuste andmise õiguslik alus, aga ka EL-i andmekaitse tase, millele vastavust edaspidi adekvaatsusotsuste andmisel hindama hakatakse.

Sellest lähtudes on käesoleva töö uurimusküsimuseks: kas *Privacy Shield* programm käesoleval kujul tagab EL-i andmekaitseõigusega sisuliselt samaväärse isikuandmete kaitse taseme USA uue administratsiooni kontekstis ning pärast GDPR-i kohaldamist mais 2018. Lähtudes uurimusküsimusest, püstitab autor hüpoteesina positsiooni, et *Privacy Shield* programmi poolt tagatav isikuandmete kaitse tase ei vasta käesoleval hetkel USA-st tulenevate muutuste tõttu EL-i andmekaitse tasemele ja PS põhimõtted ei vasta GDPR-i poolt pakutavale isikuandmete kaitse tasemele. Arvestades, et GDPR-iga kaasneva EL-i andmekaitsetaseme tõusu osas valitseb kirjandusest ning ekspertide hulgas konsensus, on siinesitatud uurimusküsimuse teise osa puhul autori eesmärgiks tuvastada konkreetsed puudujäägid *Privacy Shield* põhimõtetes võrreldes GDPR-is sätestatud andmetöötlus põhimõtetega.

Esitatud küsimusele vastamiseks analüüsib autor esiteks USA administratsiooni vahetusest tulenevaid elemente, millel võib olla mõju rakendusotsuse 2016/1250 järjepidevusele ja teiseks, *Privacy Shield* programmis sätestatud isikuandmete töötlemise põhimõtteid GDPR-is sätestatud isikuandmete töötlemise põhimõtetele.

Sarnasel teemal uurimustöid ei ole autorile teadaolevalt varem tehtud, seda peamiselt seetõttu, et *Privacy Shield* õigusraamistik ja rakendusotsus 2016/1250 on käesoleva töö koostamise aja

[26] Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiiv 95/46/EÜ kehtetuks tunnistamise kohta; Euroopa Liidu Teataja, 04.05.2016, L119/1

seisuga olnud töös kõigest kaheksa kuud.[27] Arvestades *Privacy Shield* õigusraamistiku värskust, kogu EL-i andmekaitseõiguses esinevaid arenguid ning muutusi käesoleva töö kirjutamise ajal ja isikuandmete piiriülese piiranguteta liikumise olulisust digitaalmajanduses, on käesoleva töö teema väga aktuaalne. Seda nii *Privacy Shield* programmi jätkuva piisava andmekaitse taseme tagamise üle järelevalvet teostavatele EL-i liikmesriikide ja EL-i enda organitele, andmesubjektidele aga ka isikuandmeid üle Atlandi edastatavatele ja vastuvõtvatele ettevõtetele, kellele stabiilne õiguskeskkond on väga oluline ning keda käesoleva töö tulemused võivad mõjutada Atlandiülese isikuandmete edastamise teostamiseks rakendama *Privacy Shield* õigusraamistikule alternatiivseid võimalusi.

Töö on jagatud kaheks osaks: sissejuhatav 1. peatükk, milles autor annab ülevaate EL-i isikuandmete kolmandatesse riikidesse edastamise regulatsioonist, tutvustab Atlandiülese isikuandmete edastamise, kui andmekaitseõiguse alavaldkonna õiguslikku raamistikku, selle ajalugu ning nimetatud alavaldkonna tekkimise eeldust ehk USA andmekaitseõiguse ebapiisavat isikuandmete kaitse taset EL-i poolt vaadatuna. Selles alapeatükis soovib autor valgust heita põhjustele, miks USA õigussüsteemi suhtes ei ole võimalik välja anda adekvaatsusotsust, vaid adekvaatsusotsuse andmine on võimalik vaid *Privacy Shield* või *Safe Harbor* tüüpi õigusraamistike suhtes. 2. peatükis pöördub autor esitatud uurimusküsimusele vastamise juurde.

Arvestades püsitatud uurimusküsimuse kaheastmelisust, on autor jaganud ka uurimusküsimusele vastust otsiva 2. peatüki kaheks. Esimeses osas analüüsib autor USA-st tulenevaid *Privacy Shield* programmi piisava andmekaitse taseme jätkuvust mõjutavaid asjaolusid ning tähelepanu all on USA presidendi Donald Trumpi ja tema uue administratsiooni tegevus alates jaanuarist 2017 kuni käesoleva töö koostamiseni. Kuna *Privacy Shield* programmis on USA valitsuse poolsetel kinnitustel eriti oluline osa luureastuste poolt teostatava isikuandmete töötlemise piiramisel, lasub ka analüüsi raskuskese neil kinnitustel. Teises alapeatükis analüüsib autor GDPR-is sätestatud isikuandmete töötlemise põhimõtete pakutava andmekaitse taseme vastavaust *Privacy Shield* põhimõtetele.

Käesoleva töö põhianalüüsi koostamisel on autor lähtunud eeldusest, et rakendusotsus 2016/1250 oli selle tegemise ajal, 12. juulil 2016, õiguspärane ning kehtiv ehk *Privacy Shield* õigusraamistik tagas selle alusel USA andmetöötlejatele edastatud isikuandmete kaitse taseme,

[27] Komisjon rakendusotsus 2016/1250 anti välja 12.07.2016, kuid USA andmetöötlejad saavad *Privacy Shield* programmiga liituda ning selle alusel isikuandmeid EL-ist vastu võtta alates kuupäevast 01.08.2016 – Euroopa Komisjon; *EU-U.S. Privacy Shield fully operational from today;* pressiteade 01.08.2016; kättesaadav: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=33704 (30.04.2017)

mis sisuliselt oli samaväärne EL-i andmekaitse tasemega. Kuigi käesoleva töö koostamise seisuga on EK-sse esitatud hagi rakendusotsuse 2016/1250 tühiseks tunnistamiseks, üritab autor vältida hinnangu andmist rakendusotsuse 2016/1250 kehtivusele või tühisusele, kuid vajadusel on valmis selles osas olulistele nüanssidele tähelepanu pöörama. Käesoleva töö eesmärgiks on tuvastada *Privacy Shield* programmi probleemsed kohad, et oleks võimalik rakendada vajalikke meetmeid nende kõrvaldamiseks ning tagada rakendusotsuse 2016/1250 järjepidevus.

Töö esimeses osas kasutab autor peamiselt dogmaatilist meetodit, et teha kindlaks eeldused programmide *Privacy Shield* ja *Safe Harbor* kehtestamiseks ning analüüsib sellest eesmärgist lähtudes USA õiguskorda ja EL-i õigusest tulenevaid eeldusi kolmandatesse riikidesse isikuandmete edastamise kohta. Teises peatükis kasutab autor võrdlev- analüütilist meetodit kõrvutades peatükis 2.1. USA õiguses esinenud arenguid ja nende mõju *Privacy Shield* programmis antud kinnitustele ja kehtivat EL-i andmekaitse taset. Peatükis 2.2. analüüsib autor *Privacy Shield* programmiga sätestatud kohustuslike andmekaitse põhimõtete poolt pakutavat andmekaitse taset GDPR-ist lähtudes.

Lisaks asjakohastele EL-i ja USA õigusaktidele kasutab autor töös erinevaid EL-i institutsioonide poolt väljaantud juhendava ja selgitava iseloomuga dokumente ja EK otsuseid.

Töö kokkuvõttes esitab autor vastused töös püstitatud küsimustele ning võtab kokku töös tehtud järeldused.

1. Atlandiülene isikuandmete edastamine

Terminiga „Atlandiülene“ viidatakse tavaliselt millelegi Euroopa ja Põhja-Ameerika vahelisele. Veelgi sagedamini kasutatakse seda sõna Euroopa Liidu ja Ameerika Ühendriikide suhtele osutamisel. Näiteks on Atlandiülene Majandusnõukogu ning Atlandiülene kaubandus- ja investeerimispartnerluse leping konkreetselt EL-i ja USA vahelise suhte elemendid.[28] Nii puudutab ka Atlandiülene isikuandme edastamine kui kitsam alavaldkond EL-i andmekaitseõiguses konkreetselt neid kahte piirkonda.

Eraldi alavaldkonnana saab Atlandiülesest andmevahetusest rääkida alates Euroopa Komisjoni 26. juuli 2000. a. otsusest 2000/520/EÜ, millega Euroopa Komisjon tunnistas *Safe Harbor* õigusraamistikuga kooskõlas USA äriühingutele edastatavad isikuandmed kaitstuks.

Safe Harbor õigusraamistiku vajalikkuse tingis aga Euroopa Parlamendi ja Nõukogu direktiivi 95/46/EÜ jõustumine.[29] Kuna 1995. aasta direktiiv tagas Euroopa Liidus, võrreldes muu maailmaga tänu oma ulatuslikule kohaldusalale[30], küllaltki kõrge andmekaitse taseme[31], oli tarvis kindlustada, et kaitse, mis direktiiviga isikute andmetele anti, ei kannataks andmete edastamisel riikidesse, kus puudub direktiiviga 95/46 võrdväärne isikuandmete kaitse tase. Vastupidine oleks tinginud olukorra, kus andmete töötlemiseks saadetakse need lihtsalt direktiivi mõjupiirkonnast välja. Andmete turvalisuse tagamiseks väljaspool direktiivi geograafilist mõjuala ehk kolmandates riikides, piirati direktiiviga 95/46 andmete edastamist sellistesse riikidesse ning piirkondadesse, kuhu edastades isikuandmete turvalisus ning isikute kontroll oma andmete üle langeks.[32] Seda reguleerib direktiivi 95/46 artikkel 25(1), mille kohaselt võib isikuandmete edastamine kolmandatesse riikidesse toimuda ainult juhul, kui see

---

[28] USA Riigi departemang; *About Transatlantic Economic Council*; kättesaadav: https://www.state.gov/p/eur/rt/eu/tec/c33255.htm (01.05.2017); Euroopa Komisjon; *What is TTIP about?*; kättesaadav: http://ec.europa.eu/trade/policy/in-focus/ttip/about-ttip/ (20.04.2017)

[29] W. Gregory Voss; *The Future of Transatlantic Data Flows: Privacy Shield or Bust*; Journal of Internet Law; vol 19 nr 11; Mai 2016; lk 9

[30] Direktiivi 95/46 artikli 3(1) kohaselt kohaldatakse direktiivi isikuandmete täielikult või osaliselt automatiseeritud töötlemise suhtes ja isikuandmete automatiseerimata töötlemise suhtes, kui kõnealused isikuandmed kuuluvad kataloogi või kui nad kavatsetakse hiljem sellesse kanda. Arvestades, et terminid „töötlemine“ ja „isikuandmed“ omavad samuti direktiivi kohaselt laia ulatust, kohaldub, direktiiv põhimõtteliselt kõikide toimingute suhtes, mida tuvastatud või tuvastatava füüsilise isiku kohta käiva teabega tehakse;

[31] Euroopa Liidu Põhiõiguste Amet ja Euroopa Nõukogu Euroopa Inimõiguste kohus. *Euroopa andmekaitse käsiraamat*; Luxembourg: Euroopa Liidu Väljaannete Talitus 2015; lk 3 (edaspidi viidatud kui „Euroopa andmekaitse käsiraamat“)

[32] W. Gregory Voss; lk 9

riik tagab andmekaitse piisava taseme. USA andmekaitse tase üksinda, ilma *Safe Harbor* või *Privacy Shield* raamistike poolt pakutavate täiendusteta, on seega EL-i poolt vaadatuna ebapiisav, vastasel juhul ei oleks olnud põhjust isikuandmete Atlandiüleseks edastamiseks eraldi õigusraamistikus kokku leppida.[33]

Käesoleva peatüki eesmärk ongi anda ülevaade Atlandiülesest isikuandmete edastamisest, selle vajalikkusest ning ajaloost. Selleks käsitleb järgnev alapeatükk EL-i regulatsiooni isikuandmete kolmandatesse riikidesse edastamise kohta – millised võimalused eksisteerivad isikuandmete õiguspäraseks edastamiseks väljapoole direktiivi 95/46 mõjuala. Nagu allpool näha, selgub nimetatud alapeatükist, et kolmandatesse riikidesse isikuandmete piiranguteta ja vaikimisi edastamine on võimalik, kui edastamise sihtriik tagab isikuandmete „piisava kaitsetaseme".

Nagu juba tõdetud, ei ole USA andmekaitse tase piisav. Selleks, et mõista, milles USA andmekaitse taseme ebapiisavus seisneb ning mis on põhjustanud Atlandiüleste isikuandmete edastamist võimaldavate õigusraamistike sätestamise vastaval kujul, leiab peatükis 1.2. käsitlust esiteks, privaatsusõiguse ning andmekaitseõiguse kujunemislugu Euroopas ja USA-s ning teiseks, USA õiguskorra andmekaitset käsitlev osa.

Peatükis 1.3. vaatleb autor Atlandiülese isikuandmete edastamise õiguslikku olukorda õigusraamistike *Safe Harbor* ja *Privacy Shield* näitel ning nimetatud õigusvaldkonna tähtsaimat Euroopa Kohtu otsust asjas C-362/14 *Schrems.*

1.1. Isikuandmete kolmandatesse riikidesse edastamise õiguslik alus

Peamine instrument Euroopa Liidus isikuandmete kaitse reguleerimisel on kuni 25. maini 2018 direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. Tegemist on mahukaima ekstraterritoriaalse andmekaitse reeglistikuga ja sellisena ka isikuandmete kaitse õiguse arengu seisukohalt olulisim.[34] Direktiivi kohaldamisalasse ei kuulu isikuandmete töötlemine, mis jääb väljapoole ühenduse õigust ja mis on seotud avaliku korra, riigikaitse, riigi julgeoleku ja riigi toimingutega kriminaalõiguse valdkonnas, samuti kui füüsiline isik töötleb andmeid isiklikel või kodustel eesmärkidel.[35]

[33] USA õiguskorra on hinnanud ebapiisavaks Artikkel 29 Töörühm enne *Safe Harbor* raamistikus kokku leppimist töödokumendis nr 15: *Arvamus 1/99 Andmekaitse tasemest Ameerika Ühendriikides ja käimasolevast arutelust Euroopa Komisjoni ja Ameerika Ühendriikide vahel*; 26.01.1999; lisaks on ebapiisavust deklareerinud Euroopa Komisjon rakendusotsustes 2000/520/EÜ punktides 4 ja 10 ning tunnistanud rakendusotsuse 2016/1250 artiklis 1. USA Kaubandusministeerium on samuti ebapiisavaust tõdenud rakendusotsuse 2016/1250 lisa 2 II lisa punkt 1
[34], A. Nõmper, E. Tikk; lk 67
[35] Direktiiv 95/46 artikkel 3(2)

Sellegipoolest on direktiiviga reguleeritavate isikute ning tegevuste ring väga lai tulenevalt direktiivi järgsest definitsioonist terminitele „isikuandmed“ ning „töötlemine“.

Käesoleva töö seisukohast väärib suurimat tähelepanu direktiivi IV peatükk, mis sätestab reeglid isikuandmete kolmandatesse riikidesse edastamise kohta. Kuna direktiivi 95/46 tagab kõigis liikmesriikides vähemalt direktiivis sätestatud ulatuses andmekaitse miinimum taseme, ei ole põhjust andmesubjekti isikuõiguste kaitse tagamise eesmärgil liikmesriikide vahelist andmevahetust piirata. Riikide suhtes, kus direktiiv ei kohaldu, tuleb aga olla tähelepanelikum. Isikuandmete edastamine riikidesse, kus puudub Euroopa Liiduga võrdväärne isikuandmete kaitse tase on keelatud.[36] Ilma sellise keeluta kaotaks EL-i andmekaitse regulatsioon mõtte, sest piiranguteta töötlemiseks edastataks isikuandmed lihtsalt riiki, kus töötlemisele reegleid kehtestatud ei ole. Kuna andmekaitse on ELPH artiklis 8 sätestatud põhiõigus, tähendaks kolmandatesse riikidesse andmete piiranguteta edastamise lubatavus andmesubjektide põhiõiguse riivet.

Artiklis 25 sisalduva põhireegli kohaselt võib isikuandmeid edastada vaid sellistesse riikidesse, kus on tagatud andmekaitse piisav tase. Taseme piisavuse üle otsustab Komisjon.[37] Kui sellist otsust kolmanda riigi suhtes ei ole, peavad liikmesriigid artikkel 25(4) kohaselt võtma kasutusele vajalikke meetmeid, et isikuandmeid sinna ilma täiendava kaitseta ei edastataks. See tähendab, et liikmesriigi pädev asutus peaks iga konkreetse isikuandmete edastamise toimingu puhul olema veendunud, et ka sihtkohas oleks nende kaitse tagatud. Selline kolmanda isiku pidev sekkumine andmevoogudesse mõistagi mõjub piiravalt andmetöötlejate tegevusele ning arvestades isikuandmete majanduslikku tähtsust, ka modernsele vabakaubandusele.

Samas on direktiivi preambuli mitmes punktis rõhutatud piiriülese andmevahetuse olulisust nii liikmesriikide vahel kui ka rahvusvahelisel tasandil.[38] Andmevoogude piiramine liikmesriikide ning kolmandate riikide vahel ei ole direktiivi eesmärgiks, pigem vastupidi, kuid oluline on leida lahendus, mis võimaldaks eurooplaste isikuandmete piisava kaitse ka väljaspool EL-i õiguse kohaldumisala

Selleks pakub direktiivi artikkel 26(1) üldreeglist erandid, mille esinemisel võib andmeid edastada ka sellisesse riiki, mille andmekaitsereeglid ei taga piisavat kaitset direktiivi tähenduses. Lisaks lubab artikkel 26(2) isikuandmeid edastada, kui vastutav töötleja ise rakendab „piisavaid tagatisi“ tagades nii isikuandmete kaitse sihtriigis. Kui eelnevatele lisada

[36] Direktiiv 95/46 artikkel 25(1) ning põhjendus nr 57
[37] Direktiiv 95/46 artikkel 25(6)
[38] Direktiiv 95/46 põhjenduse punktid 6, 7, 56

artiklis 25(6) nimetatud alus, on direktiivi kohaselt kolm võimalikku olukorda, mis lubavad isikuandmeid edastada ka riikidesse, mis ei ole direktiiviga kohustatud riikideks:

1. esineb mõni artikkel 26(1) nimetatud eranditest;
2. artikkel 26(2) kohaselt on vastutav töötleja andnud piisavaid tagatisi andmekaitse reeglite järgimise kohta;
3. sihtriigi andmekaitse taseme kohta on Komisjon teinud artikkel 25(6) alusel adekvaatsusotsuse.

1.1.1. Artikkel 26(1) erandid

Direktiivi 95/46 artikkel 26(1) kohaselt on isikuandmete edastamine või edastamise kogum kolmandasse riiki, mis ei taga andmekaitse piisavat taset lubatud teatud asjaolude esinemisel. Nimetatud on andmesubjekti ühemõttelist nõusolekut edastamiseks, andmesubjektiga sõlmitud lepingu täitmist, kui edastamise eeldust, edastamise vajalikkust andmesubjekti eluliste huvide kaitseks ja üldistest huvidest tulenevat vajadust isikuandmete edastamiseks.

Artikkel 26(1) erandite puhul on tegemist kindlate, piiratud arvuga juhtumitega, mille eesmärgiks võiks direktiivi 95/46 põhjenduse punkt 56 valguses olla rahvusvahelistes kaubandussuhetes vajaliku paindlikkuse tagamine, aga ka tasakaalu tagamine erinevate huvide vahel. Neid erandeid põhireeglist tuleb tingimata tõlgendada kitsendatult.[39]

Direktiiv 95/46 artikkel 29 alusel loodud töörühm (edaspidi „WP29“) on seoses artikkel 26(1) tõlgendamisega rõhutanud, et nimetatud erandite rakendamine peaks olema võimalik vaid erandlikel juhtudel. Neid peaks olema võimalik kasutada isikuandmete edastamisel kolmandatesse riikidesse viimases järjekorras – kui tegemist on riigiga, mille suhtes puudub adekvaatsusotsus ning piisavate tagatiste andmine ei ole mõistlik ega otstarbekas. Vältida tuleb olukordi, kus andmetöötlejad kasutavad neid läbivalt, jättes tähelepanuta võimaluse tagada andmesubjekti õiguste kaitse lepinguliste tüüptingimustega või kontserni-siseste eeskirjadega.[40]

[39] Artikkel 29 Töörühm töödokument WP 114, 25. november 2005, lk 7
[40] *Ibid* lk 9

1.1.2. Piisavad tagatised

„Piisavad tagatised“ artikkel 26(2) kohaselt võivad tuleneda näiteks andmete edastaja ning andmete vastuvõtja vahel sõlmitud lepingust, mis kohustab pooli andmete töötlemisel järgima kindlaid reegleid. Neid reegleid on kaht tüüpi: Euroopa Komisjoni poolt koostatud lepingulised tüüptingimused isikuandmete kaitse tagamise kohta, mida pooled peaksid andmevoogude takistamise vältimiseks kasutama originaalkujul ja *ad hoc* lepingulised klauslid, milles pooled lepivad ise kokku, kuid mis peavad saama kinnitatud kohaliku andmekaitse institutsiooni (nt Andmekaitse Inspektsiooni) poolt.[41]

Lepingulisi tüüptingimusi on kahte tüüpi: lepingulised tingimused, mida peaksid rakendama isikuandmete edastamisele vastutavad töötlejad (andmete edastamine direktiivi artikkel 2d mõttes vastutavalt töötlejalt vastutavale töötlejale)[42] ning tingimused, mis rakenduvad isikuandmete edastamisele vastutavalt töötlejalt volitatud töötlejale.[43] Kui andmeid edastav vastutav töötleja ja kolmandas riigis asuv vastuvõtja (nii vastutav kui volitatud) reguleerivad oma suhet eelnimetatud lepinguliste tüüptingimustega, on see järelevalveasutusele küllaldane tõend selle kohta, et andmekaitse tagamiseks rakendatakse piisavaid meetmeid.[44]

Kuigi direktiivi artiklis 26(2) seda *expressis verbis* väljendatud ei ole, tunnustavad kohalikud andmekaitse institutsioonid ka kontserni sise-eeskirjade alusel kolmandatesse riikidesse isikuandmete edastamist.[45] Kontserni sise-eeskirjad (*Binding Corporate Rules*) on õiguslikult siduvad andmetöötlusreeglid, mis tagavad äriühingu või äriühingu grupi (kontserni) sees piisava andmekaitse taseme. Need reeglid kehtestab kontsern ise oma andmetöötlusprotsessidele ja nende reeglite kaudu on kaitstud kogu andmevahetus kontserni sees, olenemata millises konkreetses riigis parasjagu kontserni andmetöötleja viibib ning kas selle riigi andmekaitse tase on Komisjoni poolt tunnustatud adekvaatseks või mitte.[46]

Tähelepanuväärne artikkel 26(2) puhul on asjaolu, et isikuandmete edastamise riiki, mis ei taga kaitse piisavat taset, muutub lubatavaks kõigest vastutava töötleja poolt piisavate tagatiste esitamisega. Lepinguga on küll võimalik sihtkoha riigi töötlejat panna edastatud isikuandmete

[41] C. Kuner; lk 43
[42] Komisjoni otsus, 15. juuni 2001, kolmandatesse riikidesse isikuandmete edastamise lepingu tüüptingimuste kohta direktiivi 95/46/EÜ alusel (2001/497/EÜ) ja Komisjoni otsus, 27. detsember 2004, millega muudetakse otsust 2001/497/EÜ kolmandatesse riikidesse isikuandmete edastamise lepingu alternatiivsete tüüptingimuste kogumi kasutuselevõtu kohta (2004/915/EÜ)
[43] Komisjoni otsus, 5. veebruar 2010, kolmandatesse riikidesse asuvatele volitatud töötajatele isikuandmete edastamise lepingu tüüptingimuste kohta nõukogu ja Euroopa Parlamendi direktiivi 95/46/EÜ alusel (2010/87/EL)
[44] Euroopa andmekaitse käsiraamat; lk 136
[45] Euroopa Komisjon *Binding Corporate rules*; 02.08.2016; kättesaadav: http://ec.europa.eu/justice/data-protection/article-29/bcr/index_en.htm (28.02.2017)
[46] C. Kuner; lk 43-44

töötlemisel järgima kindlaid reegleid, kuid vastutaval töötlejal puudub igasugunegi võimalus mõjutada, millist töötlemist sihtkoha riigi ametiasutused edastatavatele isikuandmetele rakendada võivad või millised seadusliku kohustused lasuvad sihtkoha riigi töötlejal oma ametiasutuste ees isikuandmete töötlemisel.

1.1.3. Adekvaatsusotsus

Artikkel 25(6) annab Euroopa Komisjonile võimaluse otsustada, et kolmas riik tagab kaitse piisava taseme artikkel 25(2) tähenduses siseriikliku õigusega või endale võetud rahvusvaheliste kohustustega. Artikkel 25(2) kohaselt pöörab Komisjon kolmanda riigi andmekaitse taset hinnates tähelepanu andmete laadile, kavandatud töötlemistoimingute eesmärgile ja kestusele, päritoluriigile ja sihtriigile, kolmanda riigi kehtivatele üldistele kui ka konkreetse sektori õigusnormidele ja riigis järgitavatele ametieeskirjadele ja turvameetmetele. Üldistatult tähendab see kolmandas riigis isikuandmete töötlemisele rakenduvate reeglite ning põhimõtete sisu ja nende efektiivse rakendamise tagamise hindamist. Hinnatava riigi õiguskorda või rahvusvahelisi kohustusi tuleks kõrvutada direktiivist tulenevate printsiipide ning protseduuri ja täideviimise reeglitega, mille tuumik annabki ette miinimumreeglid või miinimumtaseme, millele hinnatav õiguskord vastama peaks.[47] Kolmanda riigi suhtes tehtud adekvaatsusotsus võimaldab sinna piiranguteta isikuandmete edastamist ning sel puhul kaob ka vajadus artikkel 26(1) erandite kasutamisele või piisavate tagatiste rakendamisele. [48]

Euroopa Komisjon on tänase seisuga langetanud 12 sellist adekvaatsusotsust erinevate riikide ja piirkondade kohta, kuhu kuuluvad näiteks Kanada, Andorra, Argentiina, Guersney.[49] Adekvaatsusotsuse alusel isikuandmete edastamine ei erine isikuandmete edastamisest liikmesriikide vahel. Seega lihtsustab see tunduvalt kogu EL-i piiridest välja ulatuva isikuandmete vahetuse protsessi. Seetõttu on neile, kolmandate riikide andmetöötlejatele, kes soovivad eurooplaste isikuandmetele ligipääsu kindlasti oluline, et selline otsus tema asukohariigi kohta eksisteeriks.[50]

[47] Artikkel 29 Töörühm; *Working Document Transfers of personal data to third countries: Applying artickles 25 and 26 of the EU data protection directive*; 24.07.1998; lk 5; kättesaadav: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf (01.02.2017)
[48] Euroopa andmekaitse käsiraamat; lk 132
[49] Vt Euroopa Komisjoni koduleheküg vastuvõetud adekvaatsusotsuste kohta, kättesaadav: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (01.02.2017)
[50] Euroopa andmekaitse käsiraamat; lk 132

Adekvaatsusotsuse tegemine on üpris kompleksne protsess, millele tavaliselt kulub mitu aastat.[51] See protsess algab tavaliselt Komisjoni ettepanekuga, millele järgneb direktiivi 95/46 artikkel 29 alusel loodud liikmesriikide andmekaitseasutuste juhtidest koosneva töögrupi (edaspidi „WP29“) arvamus hinnatava riigi andmekaitse taseme kohta ning artikkel 31 alusel loodud töörühma arvamus. Järgneb Komisjoni liikmete adekvaatsusotsus. Kogu perioodi vältel on Euroopa Parlamendil ja nõukogul õigus Komisjoni tähelepanu pöörata erinevatele otsuse aspektidele, nõuda otsuse ülevaatamist, parandamist või otsuse tegemisest hoidumist.[52]

Praktikas võib kolmandal riigil ka poliitilistest kaalutlustest lähtuvalt tekkida probleeme kõikide adekvaatsusotsuse protsessis osalevate asutuste ja liikmesriikide heakskiidu saamisel. Näiteks, 2010. aastal venitas Iirimaa valitsus Iisraelile adekvaatsusotsuse andmist, sest iirlased süüdistasid Iisraeli valitsust Iiri passide võltsimise skandaalis. Ka Austraaliale adekvaatsusotsuse andmise viivitamine tõstis poliitilisi pingeid Austraalia ja EL-i vahel 2000. aastal.[53]

Artikkel 25(6) kohaselt võivad kolmanda riigi võetud rahvusvahelised kohustused samuti tagada andmekaitse piisava taseme selles riigis, hoolimata riigi siseriikliku korra ebapiisavusest.

Asjaolu, et USA andmekaitse taset ei saa EL-i poolt vaadatuna pidada piisavaks, leiab põhjalikumat käsitlust allpool. Nagu autor seal selgitab, tuleneb USA andmekaitse taseme ebapiisavus pigem USA-s kandvast liberaalmajanduslikust põhimõttest, mis välistab EL-i tüüpi andmekaitseregulatsiooni rakendamise erasektori vastutavatele töötlejatele ja seega on USA osas adekvaatsusotsuse tegemine võimalik vaid juhul, kui USA võtab omale rahvusvahelised kohustused, mille alusel isikuandmete edastamine sinna oleks lubatud. Praegu kehtivat kohustuste paketti nimetatakse *Privacy Shield*'iks. Tegemist on Atlandiüleses andmevahetuse teise peatükiga varasema *Safe Harbor*'i järel. Neist õigusraamistikest tuleb lähemalt juttu peatükis 1.3.

[51] C. Kuner; lk 65
[52] Euroopa Komisjon, *Commission decisionons on the adequacy of the protection of personal data in third countries*, kättesaadava: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (01.03.2017)
[53] C. Kuner, lk 66

1.2. USA kui ebapiisava andmekaitse tasemega riik

Käesolevas alapeatükis on tähelepanu all USA õiguskord, täpsemalt selles sisalduv reeglistik, mida Euroopa Liidu poolt vaadatuna nimetaksime andmekaitseks. „Andmekaitse“ on pigem Euroopakeskne termin, millega tähistatakse privaatsusõigusega paralleelset õigusvaldkonda ning mis on EL-is tagatud põhiõigusena. USA-s peetakse „andmekaitse“ ekvivalendiks „andmete privaatsust“ (*data privacy*), mis on seal üldise privaatsusõiguse lahutamatu komponent.[54]

„Ebapiisav andmekaitse tase“ on võrdlusel põhinev määratlus. See määratlus lähtub võrreldava õiguskorra andmekaitset käsitleva õigusnormistiku kõrvutamisest võrdleva ehk siinkohal EL-i andmekaitseõigusega ja selle poolt andmesubjektile pakutava kaitsetasemega. Kuna USA ja EL-i õiguskordade lähtekoht isikuandmete kaitsmisel on juba kontseptuaalselt erinev – Euroopas andmekaitse, kui eraldiseisev põhiõiguslik tagatis ning USA-s privaatsusõigus, kui üldine üksikisiku loomulik õigus eraldatusele – alustab autor USA õiguskorra pakutava isikuandmete kaitse taseme käsitlemist ajaloolisest-teoreetilisest andmekaitseõiguse ja privaatsusõiguse vahekorra selgitamisest. See käsitlus on vajalik ka selleks, et mõista, isikuandmete Atlandiülest edastamist võimaldavate õigusraamistike vajalikkust.

Pärast andmekaitse ja privaatsusõiguse vahekorra selgitamist, liigub autor edasi USA õiguskorras sisalduvate isikuandmete töötlemist reguleerivate õigusaktide juurde ja püüab alapeatükis 1.2.2. välja tuua USA andmekaitse taseme ebapiisavuse tunnused.

1.2.1. Andmekaitse ja privaatsusõiguse vahekorrast

Euroopas on isikuandmete kaitseõigus ning privaatsusõigus eristatavad ning teatud määral on neid võimalik ka teineteisest sõltumatult käsitleda. Nii ajalooliselt kui ka intuitiivselt eelneb privaatsusõigus andmekaitseõigusele. Intuitiivselt selles mõttes, et privaatsus, ka selle sõna kõige igapäevasemas tähenduses, mahutab enda alla palju enamat, kui teatud laadi andmete kaitset soovimatute andmelekete vastu. Näiteks kuulub privaatsuse sfääri ka privaatne kirjavahetus ja kodune elu, rääkimata muust, mida peame privaatsusõigusega hõlmatuks.

[54] S. Cobb; *Data Privacy and data protection: US law and legislation white paper*, 26.042016, lk 1; kättesaadav: https://www.welivesecurity.com/2016/04/26/data-privacy-data-protection-us-law-legislation-white-paper/ (01.05.2017)

Ajalooliselt on privaatsusõigus varasem, sest selle sündi on õiguskirjanduses[55] tavaliselt seotud USA õigusteadlastega Samuel Warren ning Louis Brandeis ja nende poolt 1890. aastal avaldatud artikliga „The Right to Privacy".[56] Pisut rohkem kui kümme aastat pärast artikli ilmumist hakkasid Ameerika kohtud ning seadusandja arutlema privaatsuse ja eraelu puutumatuse kui tunnustatud õiguse olemasolu võimalikkusest. Esmalt arutati seda 1902. aastal, kui New York'i osariigi apellatsiooni kohus lükkas asjas *Roberson v. Rochester Folding Box Co.* tagasi Warren'i ja Brandeis'i artiklis toodud selgitused privaatsuse ja eraelupuutumatuse õiguslikult tunnustatud kaitse vajadusest ning otsustas, et privaatsus ei ole õiguslikult kaitstud hüve.[57] Seda otsust saatis vali avalik hukkamõist, mis viis New York'i seadusandja vastu võtma määruse, mille kohaselt isiku nime või kujutise kasutamine reklaamides, ilma isiku nõusolekuta, muutus väärteoks ning kahju hüvitamise aluseks. Aastal 1905 langetas Georgia osariigi kohus asjas *Pavesich v. New England Life Insurance Co.* otsuse, millega tunnustati esmakordselt isiku õigust privaatsusele ning hageja kasuks mõisteti välja ka kahjuhüvitis.[58]

Nagu iga seadusega tunnustatud õigushüve, on ka privaatsust väärtustatud juba ammu ennem seadussätteid ning kodifikatsioone. Privaatsuse seadusliku kaitsmise kontseptsiooni alussuhteks on indiviidi ning teda ümbritseva sotsiaalse ühiskonna vahekord. Idee avalikust sfäärist ning privaatsest sfäärist, kuhu avalikkusel asja ei ole, eeldab kindlat ühiskonnakorraldust. Olemuselt on tegu vastandusega, mis on võimalik vaid ühiskonnas, kus võimustruktuurid tunnustavad oma võimu ulatuse piiratust, seega ei saa privaatsusõiguseset rääkida absolutistlikes ühiskonnakorraldustes.[59]

Selles mõttes on loogiline, et esmalt hakati tunnustama üksikisiku õigust privaatsusele või eraelu puutumatusele suhtes isik – valitseja/riik. Näiteks üks esimesi olulisemaid garantiisid isiku eraelu puutumatuse kohta riigivõimu omavoli eest sätestati 1791. aastal USA-s, kui Ameerika Ühendriikide konstitutsioonile lisati Õiguste Deklaratsioon (*Bill of Rights*), milles sisalduv neljas täiendus (*fourth amendment*) sätestab isikute õiguse olla kaitstud iseenda ja oma

[55] W. Prosser; *Privacy* - R. Wacks; *Privacy. Volume II, Privacy and the Law*; Dartmouth Publishing Company Limited; 1993; lk 47-49; J. Thomson; *The Right to Privacy*; - R. Wacks; *Privacy Volume I, The Concept of Privacy;* Dartmouth Publishing Company Limited; 1993, lk 3-5; D. Solove, P. Schwartz; *Information Privacy Law*; Wolters Kluwer Law & Business; New York, 2011, lk 10-11

[56] L. Brandeis, S. Warren; *The Right to Privacy* – R. Wacks; *Privacy. Volume II, Privacy and the Law*; Dartmouth Publishing Company Limited; 1993; lk 3-30

[57] D. Solove, P. Schwartz, lk 25-26

[58] W. Prosser; *Privacy* - R. Wacks; lk 48-49; D. Solove, P. Schwartz, lk 26

[59] R. Wacks; *Privacy Volume I, The Concept of Privacy;* Dartmouth Publishing Company Limited; 1993, lk *xi*

kodu alusetute läbiotsimiste ning dokumentide ja vara konfiskeerimise eest, vastavaks aluseks saab olla vaid kohtulik luba.[60]

Isiku eraelu puutumatust ning privaatsust teiste isikute sekkumise eest hakati tõsisemalt kaitsma palju hiljem. Siin ilmnebki ülal mainitud Warren'i ja Brandeis' artikli olulisus. Autorite eesmärgiks oli leida isiku eraelu kaitsele õiguslik alus, mis töötaks ka teiste eraõiguslike isikute sekkumise vastu. Nad tõid välja, et idee isiku vara ning füüsilise puutumatuse kaitsest on niisama vana kui tavaõiguslik õigustraditsioon ise, kuid traditsiooniline tõlgendus sellisest kaitsest, kui pelgalt materiaalsete väärtuste tunnustamisest on poliitiliste, sotsiaalsete ning majanduslike muutuste kontekstis jäänud liialt kitsaks.[61] Muutused, mida autorid silmas pidasid olid peamiselt seotud kaasaskantavate kaamerate ning niinimetatud kollase ajakirjanduse tekke ja levikuga.[62]

Eastman Kodak Company tõi 1884. aastal turule odavad ning kaasaskantavad fotokaamerad, mis võimaldasid kõigil jäädvustada kõiki ja kõike. Varem oli fotograafia olnud vaid professionaalide pärusmaa.[63] Warren'it ning Brandeis'i pani muretsema sellise tehnoloogia kasutuselevõtt tolleaegse meedia poolt, mida autorid nimetasid ilmseid kõlbelisi ning omandi piire süstemaatiliselt üle astuvaks seltskonnaks, tänu kellele „… ei kuulu kuulujutud enam laiskadele ja kõlvatutele, vaid on muutunud kaubandusartikliks, mida tööstuslikult ning jultunult edendatakse".[64]

Autorid leidsid, et tavaõiguslikust õigustraditsioonist on tuletatav kaitse ka sellistele tunnetuslikele väärtustele nagu privaatsus või eraelu puutumatus. Nad täheldasid, et varasemad tõlgendused näiteks õigusest elule või vabadusele olid kitsad, tähendades vastavalt isiku õigust kaitsele vägivalla eest ning õigust pääseda otseste vabadust piiravate vahendite eest. Filosoofilise ning teadusliku teadmise suurenedes ja selle tulemusel ühiskonna teadlikkuse laienemisega ning sellega kaasnevate sotsiaalsete muutuste tõttu tunnustatakse nüüd õigust elule laiemalt, pigem kui õigust elu nautimisele ning vabaduse all mõeldakse tervet klastrit erinevaid põhiõiguslikke vabadusi (sõnavabadus, liikumisvabadus, südametunnistusvabadus, usuvabadus jne). Sellest nähtub, et tsivilisatsiooni arenedes on kasvanud vajadus järjest enam kaitsta immateriaalset osa igapäeva elust. Samamoodi tingisid Warren'i ja Brandeis'i kaasaegsed tehnoloogilised ning sotsiaalsed muudatused isiku eraelu ja privaatsuse õigusliku

[60] The White House, *The Constitution*, kättesaadav: https://www.whitehouse.gov/1600/constitution (15.03.2017); Bill of Rights Institute *Bill of Rights of the United States of America (1791)* kättesaadav: https://www.billofrightsinstitute.org/founding-documents/bill-of-rights/ (15.03.2017)
[61] L. Brandeis, S. Warren; *The Right to Privacy* – R. Wacks, lk 3
[62] D. Solove; *Understanding Privacy*; Harvard University press; Cambridge, MA, 2009, lk 15-16
[63] *Ibid*
[64] L. Brandeis, S. Warren; *The Right to Privacy* – R. Wacks, lk 4

kaitse tunnustamise vajaduse: „… pressi pealetükkivus ning avalik kuulujuttude levitamine on muutnud privaatsuse ja üksinduse indiviididele vajalikumaks ja olulisemaks, sest selle rikkumine võib isikule kaasa tuua valu ja stressi, mis on palju tõsisem kui mõni kehavigastus“.[65]

Warren ja Brandeis'i kohaselt peitub privaatsuse alusprintsiip isiku puutumatuses ja seda kõige isiklikumas mõttes ehk meelerahus, mida pakub teadmine, et tal on igasugust sekkumist oma sisesfääri võimalik vältida. Autorid leidsin, et ameerikalik tavaõigus tagab igale isikule õiguse otsustada millises ulatuses tema mõtted, emotsioonid ja arvamused võiksid saada avalikkusele teatavaks. Selle õiguse ehk privaatsuse nimetasid nad õiguseks saada rahule jäetud, mis on kõige üldisem õigus isiku puutumatuse juures – isiku õigus oma isiklikkusele.[66]

See oli üks esimesi definitsioone, mida kirjanduses privaatsusele anti – õigus saada rahule jäetud.[67] Hiljem on seda ka defineeritud, kui õigust otsustada, kui palju isiku mõtete ja tunnete, privaatsete tegevuste ja suhete kohta avalikkus teab; kui õigust varjata informatsiooni teiste eest; kui erinevaid intiimsuse vorme jne.[68] Kõiki neid definitsioone on kritiseeritud kui liiga laia või liiga kitsast.[69] Ühisosa neis definitsioonides on see, et isiku sisesfäärile pakutakse kaitset välise sekkumise eest, problemaatilisem on välja selgitada, kuhu täpsemalt peaks tõmbama piiri selle sisemise ning avalikkusele kättesaadava vahele.

Andmekaitseõiguse alguseks peetakse 1970ndaid aastaid, mil Euroopas hakati seoses andmete automatiseeritud töötlemisega tähelepanu pöörama erinevate andmevaldkondade, kui võimalikku majanduslikku väärtust omavatele informatsioonisfääridele, mille tulemusel hakkasid seadusandjad kehtestama mitmeid andmekaitseseaduseid üle Euroopa. Neist esimeseks oli 1970. aastal Saksamaal, Hesseni liidumaal kehtestatud andmekaitse regulatsioon.[70] Ka USA esimene andmete privaatsust käsitlev seadus on aastast 1970 kui võeti vastu *Fair Credit Reporting Act* (FCRA), millega seati piiranguid krediidiasutuste käsutuses olevate tarbijate andmete töötlemisele ning nähti ette andmesubjektidele teatavad õigused oma krediidiasutuse valduses olevatele andmetele.[71]

Andmete kaitsmisest hakati samuti rääkima tehnoloogia ja sellest tulenevalt sotsiaalsete muutuste kontekstis. Eelmise sajandi 70nendatel arenes arvutitehnoloogia jõudsasti ning järjest suurenev isikuandmete töötlemine ja mahukate andmepankade loomine tekitas paljudes

[65] *Ibid* lk 4-6
[66] *Ibid* lk 8, 11-13; D. Solove, lk 16
[67] M. Tzanou; *Is Data Protection the Same as Privacy? An Analysis of Telecommunications' Metadata Retention Measures*; Journal of Internet Law, Vol 17, nr 3; September 2013; lk 23
[68] *Ibid*
[69] *Ibid*, lk 24
[70] C. Kuner; lk 26;
[71] S. Cobb, lk 2

murelikkust.[72] Selle murelikkuse põhjused olid aga pigem majanduslikud, kui põhiõigustest lähtuvad, nagu varem privaatsusõiguse puhul oli olnud. Eelnevat illustreerib hästi fakt, et esimene rahvusvaheline initsiatiiv andmekaitse regulatsiooni suunas tuli Majanduskoostöö ja Arengu Organisatsiooni poolt (edaspidi OECD) 1980. aastal, kui koostati juhend eraelu ja piiriülesest isikuandmete kaitsest.

OECD on nimelt majandus- ja sotsiaalpoliitikaga tegelev organisatsioon, mille ülesandeks on edendada poliitikaid, mis parandaksid majanduslikku ja sotsiaalset heaolu. OECD mõõdab produktiivsust ning rahvusvahelise kaubanduse ja investeeringute voolu, ning ei tegele inimõigustega. OECD 1977. aastal piiriülese andmevoogude alasel sümpoosionil märgiti andmekaitse majanduslikku ning poliitilist olulisust tuues välja, et informatsioonil on majanduslik jõud ning väärtus ja võimekus teatud laadi andmeid töödelda ning talletada võib anda riigile nii poliitilised kui ka tehnoloogilised eelised teiste riikide ees. Sümpoosioni tulemusel hakatigi koostama OECD 1980. aasta juhendit. Juhendi koostamisel peeti küll silmas järjest suurenevat isikuandmete automatiseeritud töötlemise praktikat, kuid selle kaugem eesmärk oli siiski takistada informatsiooni vaba liikumise piiranguid, mis oleks majanduslikku ja tehnoloogia arengut pärssinud. Seega oli OECD-le oluline, et meetmed, mida isikuandmete kaitse lipu all välja tuuakse, ei takistaks piireüleseid andmevooge.[73]

Selline majanduslik dimensioon ei puudunud ka EL-i 1995. aasta direktiivil 95/46. Direktiivi preambuli mitmes punktis on selgitatud andmekaitse reeglite ning liikmesriikide vahel vabade andmevoogude tagamise olulisust siseturule ning majandusele.[74] Samal ajal tunnustati ka andmekaitse olulisust isikuõiguste seisukohast, pidades seda privaatsuse ja eraelu kaitse üheks dimensiooniks.[75] Hoolimata selle algsest majanduslikust tähendusest, on praeguseks andmekaitse tunnustatud EL-is kui põhiõigus.

Andmekaitse defineerimisega aga ei ole selliseid filosoofilisi probleeme nagu privaatsusõiguse puhul. Peamine andmekaitse tuumik peitub normides, mis reguleerivad isikute kohta käivate andmete kogumist, talletamist, teisaldamist ja nende seotud muud tegevust ehk töötlemist. Euroopa Liidu andmekaitse direktiivi kohaselt on andmekaitse eesmärgiks isikuandmete töötlemisel füüsiliste isikute põhiõiguste ja –vabaduste kaitse, eelkõige lähtudes isiku õigusest

[72] C. Kuner, lk 24
[73] *Ibid*; lk 24-25
[74] Direktiiv 95/46 põhjenduse punktid 3, 5, 7, 8
[75] *Ibid*; põhjenduse punkt 10

eraelu puutumatusele.[76] Seega on mõisted „töötlemine“ ning „isikuandmed“ andmekaitseõiguses kesksel kohal.

Lõplikuks andmekaitse eesmärgiks võiks pidada õiglase andmete töötlemise ning sellise töötlemise tulemuste tagamist. Töötlemise õiglus on tagatud andmekaitse printsiipide rakendamisega.[77] Eesti kehtivas isikuandmete kaitse seaduses[78] (edaspidi IKS) on neid põhimõtteid sätestatud seitse: seaduslikkuse, eesmärgikohasuse, minimaalsuse, kasutuse piiramise, andmete kvaliteedi, turvalisuse ja individuaalse osaluse põhimõte.[79]

Siiski ei peitu andmekaitse sisu vaid informatsiooni privaatsuse kindlustamises, pigem on tegemist informatsiooni autonoomiat tagava õigusvaldkonnaga. Õigusliku autonoomia kontseptsioon on kõige täpsemalt kirjeldatav läbi informatsioonilise enesemääratluse.[80] Informatsiooniline enesemääratlus on osa isiku enesemääratlusõigusest, mille alla kuuluvad veel mitmed komponendid nagu näiteks seksuaalne enesemääratlus, kehaline enesemääratlus, rahvuslik enesemääratlus jne. Need komponendid on muuhulgas kaitstavad privaatsusõigusega.[81]

Printsiibis garanteerib informatsiooniline enesemääratlusõigus indiviidi õigust ise kindlaks määrata, millist tema kohta käivat informatsiooni, millises ulatuses ja kellele võib avaldada.[82]

Eriala kirjanduses on palju käsitletud privaatsusõiguse ning andmekaitseõiguse vahekorda just Euroopas, kus andmekaitseõigus on tõusnud põhiõiguseks privaatsusõiguse kõrval. Teoreetiliselt võib olla vaieldav, kas andmekaitsele eraldiseisva ja autonoomse tähenduse andmine on õigustatud. Näiteks on Gloria Gonzalez Fuster oma monograafias *The Emergence of Personal Data Protection as a Fundamental Right* täheldanud, et andmekaitse sai põhiõigusliku tähenduse alles ELPH artikliga 8 ning sellises tähenduses ei leia seda ühestki ELPH preambulis nimetatud allikast.[83] EL-i andmekaitse peamise dokumendi, direktiiv 95/46 preambulis on selgitatud, et andmekaitse reeglite eesmärk on tagada Euroopa Inimõiguste Konventsiooni artiklis 8 ja ühenduse põhimõtetes tunnustatud põhivabaduste ja –õiguste, eelkõige eraelu puutumatuse kaitse.[84] Fusteri sõnul tulenes selline transformatsioon peamiselt

[76] Direktiiv 95/46 artikkel 1(1)
[77] M. Tzanou; September 2013, lk 26
[78] Isikuandmete kaitse seadus, RT I, 1996, 48, 944.
[79] Isikuandmete kaitse seadus, § 6, RT I, 06.01.2016, 10.
[80] M. Tzanou; *Data Protection as a fundamentaal right next to privacy? Reconstructing a not so new right*; International Data Privacy Law, Vol. 3, No. 2; 2013; lk 89
[81] M. Männiko; lk 41
[82] M. Tzanou; *Data Protection as…;* 2013, lk 89
[83] G. Fuster; *The Emergence of Personal Data Protection as a Fundamental Right of the EU*; Springler; Cham, 2014, lk 2
[84] Direktiiv 95/46 põhjenduse punkt 10

keeleteoreetilistest, mitte õiguslikest asjaoludest. Nimelt, on põhjus selles, et „andmekaitse“, kui termini tähendus on aja jooksul läbi erinevate reeglistike aga ka tänu mitme-keelelisele Euroopa kogukonnale, kus erinevates keeltes on see termin omandanud pisut erinevaid varjundeid, muutunud. Viimati lisas „andmekaitsele“ uue tähenduskihi direktiiv 95/46, kus seda kasutati siseturu kontekstis. See omaette tähendusega õiguslik objekt oli selle sajandi alguseks piisavalt kaugenenud privaatsus- ja eraelu puutumatuse õiguse kontseptsioonist, et leidis tunnustust eraldiseisva õigusvaldkonnana.[85] Reaalsus on siiski see, et Euroopas on andmekaitse põhiõigusena kaitstud ja tänaseks ka laialdaselt sellisena tunnustatud kõigi EL-i institutsioonide poolt. Siiski on privaatsusõiguse ning andmekaitseõiguse vanem-lapse laadsed sidemed ilmsed, samuti nagu fakt, et esimene on palju laiem valdkond, kui teine.

Võrdluseks on Ameerika Ühendriikide õiguskorras need kaks palju lähemalt seotud ning nagu allpoolsest käsitlusest nähtub, ei ole tihti võimalik neid eristadagi.

1.2.2. Andmete privaatsusõigus USA õiguskorras ja selle pakutav isikuandmete kaitse tase EL-i andmekaitse seisukohast

1.2.2.1. Andmete privaatsusõigus föderaalsel tasandil

Ühendriikide privaatsusõigus moodustab ebaühtlase ning killustunud süsteemi föderaalsetest ning osariikide seadustest. Näiteks on reguleeritud privaatse informatsiooni kasutamine valdkondades, nagu patsientide registrid, mootorsõidukite registrid, õpilaste andmed, ka näiteks videolaenutusandmed jne., kuid puuduvad printsiibid ning regulatsioon, mis pakuks kaitset isikuandmetele tervikuna.[86] USA-s on umbes kakskümmend erinevat riiklikku privaatsuse ja andmete turvalisust käsitlevat seadust ning sadu taolisi seadusi osariikide tasandil, näiteks California osariigis reguleerib privaatsust ning andmete kaitset kakskümmend viis erinevat seadust.[87]

[85] G. Fuster; lk 59-61, 71, 104, 253-254
[86] S. Diorio; *Data Protection Laws: Quilts versus Blankets*; Syracuse Journal of International Law and Commerce; Vol 42, Nr 2; 2015; lk 491
[87] J. Clark, K. Lucente; lk 491

USA-s kui tavaõiguslikus õigussüsteemis on lisaks seadusetele isikuandmete kaitse taseme kujundamisel osa ka kohtute loodud pretsedentidel, mis *common law* riikides võrreldes kontinentaalse õigussüsteemi riikidega omavad üldises õigusloomes väga olulist rolli.[88]

Lisaks on USA andmete privaatsuse õiguses kasutusel mitmed juhendid, mis on väljatöötatud erinevate valitsusasutuste ning tööstusharugruppide poolt eesmärgiga edendada ning propageerida isikuandmete kaitset erasektoris. Need juhendid ei oma seaduslikku jõudu ja on osa ise-reguleerimisraamistikest, mida käsitletakse „parima praktikana". Kuigi nende juhendite rakendamine ning järgimine ei ole ettevõtetele, kes isikuandmeid töötlevad, kohustuslikud, peavad need, kes siiski otsustavad neid oma äritegevuses rakendada, omaksvõetud reegleid järgima. USA Föderaalne Kaubanduse Komisjon (edaspidi FTC – *Federal Trade Commission*) on järelevalveasutus, mis kontrollib, et ettevõtted omale võetud andmekaitse alastest kohustustest kinni peaksid. Selleks on FTC-l õigus rakendada meetmeid andmete töötlejate vastu, kes kasutusse võetud andmekaitse- ning privaatsuspoliisidest kinni ei pea.[89]

Selline isereguleerimise põhimõte on USA-s läbiv. See põhineb liberaal-majanduslikul printsiibil, mille kohaselt parim majanduslik korraldus on vaba riiklikest piirangutest, sest loomulik konkurents, mis vabal turul valitseb, seab ise paika normid ja reeglid, mida ettevõtjad turul eksisteerimiseks järgima peavad.[90] Kui kanname selle põhimõtte üle andmete töötlemisega tegelevale majandussektorile, siis loogika peitub selles, et ettevõtjad, kes pakuvad kaupu või teenuseid, millega kaasneb isikuandmete töötlemine hakkavad ise, lähtudes turu vajadustest, enda poolsele andmete töötlemisele seadma piiranguid. Erinevate privaatsus- ning andmekaitsepoliiside rakendamisega võidetakse tarbijate usaldus ning need, kes vastavaid reegleid oma majandustegevuses ei rakenda, jäävad turul alla, sest tarbijad ei usalda neid ettevõtjaid oma andmeid töötlema.

Samal ajal põhinevad Ühendriikide privaatsusseadused peamiselt poliitilisel vabadusel ning isiku kodu puutumatusel valitsuse sekkumise eest. Võrdluseks nähakse Euroopas andmekaitse eesmärgina ka isiku sotsiaalse väärikuse tagamist teiste ühiskonna liikmete ees. USA-s pannakse sellele vähem rõhku, näiteks ei muretseta kuigi palju meedia poolse võimaliku privaatsuse rikkumise pärast, peamine tähelepanu on suunatud privaatautonoomia säilitamisele isiku kodus ning kodu puutumatusele nii, nagu see on sätestatud USA konstitutsiooni neljandas

[88] J. Burke; *Kohtuniku roll Ameerika õigussüsteemis*; Juridica, 1993, nr 3, lk 59 (lk 59-60); R. Narits; *Õiguse Entsüklopeedia*; Juura; Tallinn, 2007, lk 58-59

[89] I. Jolly; *Data protection in United States: Overview*; kättesaadav: http://uk.practicallaw.com/6-502-0467?q=*&qp=&qo=&qe= (13.03.2017)

[90] Encyclopedia.com; *Economic liberalism*; kättesaadav: http://www.encyclopedia.com/topic/liberalism.aspx (13.03.2017)

paranduses.[91] See läheb aga tihti vastuolu sõnavabaduse ning teiste isikute muude põhiõigustega. Sageli näeb Ameerika õigus prioriteeti sõnavabadusel isiku privaatsusõiguse ees. Heaks näiteks siinkohal on politseiarhiivi fotod, mida uurimisasutus teeb süüteo kahtlusalustest (*mug shot*). Ühendriikides on politseiarhiivi fotod avalik informatsioon, mida avalikustatakse erinevatel interneti lehtedel eesmärgiga avalikult häbistada isikuid, kes on kahtlusalustena kinnipeetud. Seejuures ei oma tähendust, kas süüdistatav talle etteheidetavas teos ka tegelikult süüdi on või mitte. Kontrastina on Ühendkuningriikide kõrgeim kohus leidnud, et politseiarhiivi fotod kahtlusalustest, kelle süü ei leia tõendamist, tuleb hävitada, sest nende säilitamine tähendaks isikute inimõiguste rikkumist.[92]

Seda, et ameeriklaste mured andmete kaitsel on peamiselt suunatud valitsuse sekkumise vastu, illustreerib 1974. aasta Privaatsusseadus (*The Privacy Act of 1974*). Tegemist on ulatusliku isikuandmete alase regulatsiooniga, mille eesmärgiks on pakkuda kaitset isikute kohta käivatele andmetele, mis on erinevatesse andmekogudesse ning registritesse talletatuna föderaalsete institutsioonide käsutuses. See seadus võeti vastu 1974. aastal, pidades silmas tehnoloogia ning eriti arvutite arenguga kaasnenud automatiseeritud isikuandmete töötlemise laia levikut valitsuse poolt.[93]

Privacy Act sätestab reeglid, kuidas ning milliseid isikuandmeid võib valitsus koguda, säilitada, kasutada ning hävitada. USA Privaatsusseaduse tähenduses on kohustatud isikuteks ainult föderaalsed organid, kelle hulka kuuluvad täidesaatva võimu, sõjaväe, avalik-õiguslike juriidiliste isikute ning muude iseseisvate föderaalsete asutuste organid. Privaatsusseadus garanteerib ameerika kodanikele ning õiguslikul alusel USA territooriumil resideeruvatele isikutele kolm peamist õigust. Esiteks, õigus saada informatsiooni andmete kohta, mida asutus tema kohta andmebaasidesse kogunud on, kui ei esine ühtegi seaduses toodud erandit. Teiseks, õigustatud isik võib nõuda andmete parandamist föderaalorgani andmebaasides, mis ei ole õiged, ajakohased, relevantsed või täielikud ning kolmandaks on õigustatud isikul õigus saada

[91] USA Konstitutsioon neljas parandus sätestab: „Keelatud on rikkuda inimeste õigust olla kaitstud iseenda ja oma kodu põhjendamatu läbiotsimise ning dokumentide ja vara alusetu konfiskeerimise eest. Vastav määrus väljastatakse ainult usutava põhjenduse korral, mille kohta antakse vanne või pühalik kinnitus ja milles on kirjeldatud esmajoones läbiotsitavat kohta, vahistatavat isikut või konfiskeeritavat eset.“ Cornell'i Ülikooli õigusinstituut; *U.S. Constitution: Fourth Amendment;* Kättesaadav: https://www.law.cornell.edu/constitution/fourth_amendment (21.04.2017)

[92] S. Diorio; 2015; lk 499

[93] *The Privacy Act of 1974*; kättesaadav: https://www.law.cornell.edu/uscode/text/5/552a (24.04.2017)

kaitset õigustamatute privaatsusriivete eest, mis tulenevad isikuandmete kogumisest, kasutamisest, avaldamisest ning säilitamisest.[94]

Asjaolu, et *Privacy Act*'is sisalduvad õigused on kasutatavad ainult USA kodanike ning USA-s viibivate isikute poolt pälvis suurt tähelepanu pärast Edward Snowden'i paljastusi USA luureasutuste luureprogrammide kohta ning päädis USA kongressi poolt seaduse *Judicial Redress Act* (edaspidi „JRA") vastuvõtmisega.[95] JRA[96] on lühike, kõigest kahest paragrahvist koosnev, seadus, mis sätestab, et määratud riikide kodanikele võimaldatakse hoolimata *Privacy Act*'is sisalduvast piirangust, siiski õigus kohaldada *Privacy Act*'ist tulenevaid õigusi. Määratud riigid nimetab USA peaprokurör mitmete USA juhtivate ametnike nõusolekul, kui riik vastab JRA-s nimetatud eeldustele.[97] EL tervikuna kuulub määratud riikide hulka.[98]

Föderaalsel tasandil on veel olulisemateks andmekaitse alasteks seadusteks Terviskindlustuse teisaldatavuse ning vastutuse seadus (*Health Insurance portability and Accountability Act*) ehk HIPAA, mille teine peatükk sätestab riiklikud standardid isikute raviandmete ja muude isiklike terviseandmete töötlemisele. Põhireegli kohaselt tuleb tervise ja ravialaste andmete töötlejatel rakendada andmeprivaatsuse tagamiseks sobilikke meetmeid, lisaks seab HIPAA piiranguid ning tingimusi, isiku nõusolekuta selliste andmete avaldamise ning kasutamise kohta. Lisaks annab seadus patsientidele kontrolli oma tervisealase informatsiooni üle, lubades patsientidel nõuda andmekoguja käest koopiat oma terviseandmetest ning ka vigaste andmete parandamist.[99]

Järgmine kirjanduses esile tõstetud föderaalne andmekaitsealane seadus on laste internetiprivaatsuse kaitsmise seadus (*Children's Online Privacy Protection Act*) ehk COPPA. COPPA eesmärgiks on anda lapsevanematele õigus otsustada, milliseid nende laste andmeid kaubandustegevusega ning andmetöötlemisega tegelevad ettevõtted võivad töödelda. Lapsed selle seaduse tähenduses on nooremad kui 13-aastased. Kohustatud isikuteks on interneti lehekülgede omanikud, kelle teenused on suunatud alla 13-aastastele lastele või kes teavad, et nende teenuseid kasutavad alla 13-aastased. Kohustatud isikud peavad seaduse kohaselt saama

---

[94] USA Justiitsministeerium; *Overview of the The privacy Act of 1974*, kättesaadav: https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition (15.03.2017)
[95] K. McGinnis; *President Obama Signs New Privacy Law – Judicial Redress Act*; 04.03.2016, JDSupra; kättesaadav: http://www.jdsupra.com/legalnews/president-obama-signs-new-privacy-law-59057/ (24.04.2017)
[96] USA Kongress; *H.R. 1428 – Judicial Redress Act of 2015*, kättesaadav: https://www.congress.gov/bill/114th-congress/house-bill/1428/text (09.04.2017)
[97] JDR artikkel 2(b)
[98] Euroopa Komisjoni pressiteade; *Questions and Anwser on the EU-U.S. Data Protection „Umbrella Agreement"*; 01.12.2016 Brüssel; kättesaadav: http://europa.eu/rapid/press-release_MEMO-16-4183_en.htm (24.04.2017)
[99] USA Tervishoiu ja Teenindusministeerium; *The HIPAA Privacy Rule*; kättesaadav; http://www.hhs.gov/hipaa/for-professionals/privacy/ (15.03.2017)

lapse andmete töötlemiseks lapsevanemalt loa, teavitama lapsevanemat tema lapse kohta kogutud andmetest, austama vanema soove tema lapse kohta kogutud andmete käigust ning tagama mõistlikud andmete turvalisust tagavad protseduuri reeglid.[100]

USA-l puudub üks kindel ja ametlik riiklik andmekaitseorgan, mis tegeleks kõigi andmekaitsealaste seaduste rakendamise ning nende alusel järelevalve korraldamisega. Siiski on neil olemas FTC, mis omab jurisdiktsiooni kaubandusettevõtete tegevuse üle ja selle kaudu omab ka õigust rakendada föderaalset järelevalvet privaatsuse ning eriti interneti privaatsuse valdkonnas.[101] FTC loodi USA Kongressi poolt 1914. aastal eesmärgiga takistada ebaõiglast konkurentsi kommertssektoris. Kuigi korruptsiooni ning ausa konkurentsi tagamise valdkondades on FTC-l laiad volitused, on nende tegevus õiglase informatsiooni töötlemise ja andmete privaatsuse tagamisel siiski piiratud. FTC ei saa ettevõtetele peale panna kohustusi rakendada ausa informatsiooni töötlemise printsiipe või poliise oma veebilehtedel ning internetialasele tegevusele.[102] Erandiks sellest on ettevõtjad, kes töötlevad laste andmeid, sest neile on kohustuslik föderaalses COPPA-s toodud reeglite järgimine, nimelt kuulub FTC ülesannete hulka ka COPPA rakendamine. Ülesannete täitmisel piirduvad FTC volitused ettekirjutuste tegemiste ning trahvide määramise õigusega neile ettevõtetele, kes rikuvad mõnda nende tegevusele rakenduva föderaalse seaduse sätteid või neile, kes on lubanud oma tegevuses mingeid kindlaid andmetöötluse või privaatsuse reegleid järgida, kuid on nende reeglite vastu eksinud. Enamikel ettevõtetel ei lasu aga mingisugust kohustust neid reegleid oma tegevusele rakendada.[103]

Üks kuulsamaid menetlusi, kus FTC rakendas talle kuuluvaid volitusi, toimus 2010. aastal, kui FTC tuvastas olulisi privaatsusreeglite rikkumisi sotsiaalvõrgustiku Twitter tegevuses. FTC tuvastas, et Twitter ei rakendanud piisavaid ja mõistlikke andmete turvalisuse tagamise abinõusid, kuigi oli omale sellise kohustuse privaatsuspoliisiga võtnud. Twitteri süsteemist avastati turvaaugud, mis põhjustasid mitmete Twitteri kasutajate privaatsete andmete lekke ning võimaldasid häkkeritele ligipääsu privaatsetele kontodele.[104] Leke oli veel sellevõrra tähelepanuväärsem, et üheks turvaaugu ohvriks oli tollane presidendikandidaat Barack Obama, kelle kontol postitati kütuse loterii reklaami. FTC menetluse tulemusena kohustus Twitter

[100] Föderaalne Kaubanduse Komisjon; *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for You Business*; kättesaadav: https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance (15.03.2017)
[101] *Ibid*
[102] S. Diorio; 2015; lk 494
[103] *Ibid*
[104] United States of America Federal Trade Commission complaint in the matters of Twitter Inc. Docket NO. C-4316; lk 3-4, kättesaadav: https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twittercmpt.pdf (15.03.2017)

tugevdama oma turvameetmeid ning lubas sõltumatul kolmandal osapoolel testida ning hinnata Twitteri privaatsusmeetmeid.[105]

1.2.2.2. Andmete privaatsusõigus osariikide tasandil

Kohalikul tasandil on mitmed osariigid võtnud vastu konstitutsioonilisi sätteid privaatsusõiguse tagamiseks, siiski ei keskendu need kuigivõrd palju informatsiooni privaatsuse ehk andmekaitse tagamisele. Eriti osariikide tasandil on Ühendriikides peamisteks õiguse kujundajateks kohtud ning seega ei olegi ehk kõige olulisem sätestada eraldi andmekaitsealaseid seadusi, vaid oodata, et kohtud hakkaksid privaatsusõiguse rikkumisena nägema ka isikuandmete valdkonna rikkumisi. Selleni näib aga olevat veel pikk tee, sest ka privaatsusõiguslikes vaidlustes tunnustatakse tavaliselt vaid kõige tõsisemaid ründeid privaatsushuvide vastu ja seda nii osariigi- kui föderaaltasandil. Andmekaitsealaseid riived kuuluksid Ameerika tavaõiguse kohaselt käsitlemisele privaatsushagide kontekstis. [106]

Tavaõiguse doktriini kohaselt esineb neli õiguslikku alust privaatsushagi esitamiseks: 1) hagejat on esitatud vales valguses (valeinformatsiooni levitamine hageja kohta); 2) hageja privaatset informatsiooni on õigusvastasel avalikustatud; 3) hageja privaatsusesse on sekkutud; 4) hageja nime või temaga sarnasust on pahausklikult ära kasutatud. Siiani on USA kohtud pigem eitanud, et andmekaitsealased isikute õiguste rikkumised on privaatsusõiguslike sätete poolt kaitstud.[107]

Kõigil USA 50 osariigil on oma seadused, mis reguleerivad privaatsust ning mõnel juhul ka andmekaitset.[108] Üks kirjanduses esile tõstetumaid osariike andmekaitse regulatsiooni poolest on California. Tegemist on osariigiga, kus rakendatakse kõige mahukamat privaatsusregulatsiooni terves föderatsioonis. Mitmed neist kohalikest seadustest omavad ka osariigi piiridest kaugemale ulatuvat mõju, sest sätestavad andmekaitse või privaatsusreeglid, mida California kodanike andmeid töötlevad isikud järgima peavad.[109]

California osariigi privaatsusseadused sarnanevad Euroopa omadele. Näiteks sära valguses seaduse (*The Shine the Light Law*) järgi peavad ettevõtted, kes jagavad andmesubjekti andmeid kolmandate isikutega, sellest andmesubjekti teatama ning andmesubjekti soovil sellisest jagamisest hoiduma. Lisaks peavad ettevõtted andmete turvalisuse seaduse kohaselt (*the data*

[105] S. Diorio; 2015; lk 495
[106] *Ibid;* lk 496
[107] *Ibid*
[108] EPIC; *Privacy Laws by State*; kättesaadav: https://www.epic.org/privacy/consumer/states.html (24.04.2017)
[109] I. Jolly; 2014/2015*; State privacy laws*;

security law) tagama mõistlikud turvameetmed, et isikuandmed oleksid lubamatute lekete eest kaitstud. California on ka üks vähestest osariikidest, kus on kohalik andmekaitse amet (*Office of Privacy Protection*).[110]

2015. aasta mai seisuga on neljakümne seitsmes osariigis rakendatud seaduseid, mis kohustavad ettevõtjaid andmesubjekte teatama nende isikuandmete lekkimisest ning vähemalt kahekümne üheksa osariigi seaduste kohaselt peavad andmetöötlejad teatud olukordades hävitama isiku nõudel tema kohta käivaid andmeid.[111]

1.2.2.3. Järeldus USA andmekaitse taseme kohta

Seega nähtub USA isikuandmete kaitse puudulikus peamiselt selle valdkonna fragmentlikkusest: paljud andmesubjektiga seotud andmed, mis EL-is on isikuandmetena kaitstud, ei ole seda USA-s. USA õiguskord ei paku kaitset igasugusele teabele tuvastatud või tuvastatava andmesubjekti kohta, vaid sektoripõhiselt ja detsentraliseeritult pannes rõhu pigem turu enda võimele seada piiranguid, kui riigi sekkumisele.[112]

On üldiselt mõistev, et isikuandmete sektoripõhine kaitsmine ei taga sama tulemust, mis EL-i stiilis üldine regulatsioon, mis kohaldub isikuandmete töötlemisele, kusjuures mõlemad terminid on definitsioonilt väga laiad. Kuid lisaks ei leia USA õiguskorras tunnustust mitmed olulised põhimõtted, mis EL andmekaitse seisukohast on olulised ning mida tuleb rakendada iga töötlemise puhul.[113] Näiteks ei kohaldu enamikele USA andmetöötlejatele eesmärgipärasuse põhimõte ja kasutuse piiramise põhimõte või minimaalsuse põhimõte, sest tihti võivad andmetöötlejad kogutud isikuandmeid töödelda ilma andmesubjekti nõusolekuta ka eesmärkidel ning mahus, millest andmesubjekt ei ole teadlik.[114] Lisaks ei ole täielikult või vähemalt EL-i standarditele vastavas ulatuses tagatud andmete kvaliteedi põhimõte.[115]

Üheks oluliseks tunnuseks euroopaliku andmekaitse juures on kindalasti veel asjaolu, et piiratud on isikuandmete edastamist riikidesse, kus andmekaitse tase on isikuandmeid edastavast riigist madalam. Näiteks Ameerika Ühendriikide seadusandluses piirangut andmete

---

[110] *Ibid*
[111] *Ibid*
[112] G. Shaffer; *Globalization and social protection: the impact of EU and International rules in the ratcheting up of U.S. data privacy standards*; Talv 2000; vol 25, Yale Journal of International law, lk 27
[113] Direktiiv 95/46 põhjenduse punkt 12
[114] C. Hoofnagle; *Comparative study on diferent approaches to new privacy challanges in particular in the light of technological developments – country studies- United States of America*; Mai 2010, Euroopa Komisjoni uurimus, lk 23-24 ja 29, kättesaadav: http://ec.europa.eu/justice/data-protection/document/studies/index_en.htm (01.05.2017)
[115] *Ibid*, lk 25

edastamisele kolmandatesse riikidesse ei leia, kui mainimata jätta mõnd tüüpi valitsuse informatsiooni edastamise piirangud.[116]

Osariikide tasandil võivad selliste piirangute rakendamised olla USA konstitutsiooni kohaselt ka keelatud.[117] Nimelt on USA konstitutsiooni artikkel 1 lõige 8 kolmanda lause kohaselt vaid Kongressil õigus „… reguleerida kaubandust osariikide, võõrriikide ning indiaanihõimudega.“[118] Seda nn kaubandusklauslit on üheltpoolt käsitletud kui Kongressi pädevust määrava ning teiselt poolt osariikide suveräänsust piirava sättena.[119] Kuna isikuandmetel ning ka muudel andmetel on majanduslik väärtus ning need on üldiselt ettevõtete majandustegevuses laialdaselt kasutuses, kuulub andmevoogudele piirangute seadmise õigus kaubandusklausli alusel Kongressile. Kongress, kui föderaalne institutsioon on kaubandusvaldkonnas andmekaitse reguleerimise aga ettevõtete iseregulatsiooni hoolde jätnud ja seda varem kirjeldatud liberaalmajanduslikel põhjustel. Kuna USA andmekaitseõiguses puudub initsiatiiv tagada isikuandmetele, mis riigi jurisdiktsioonist välja lähevad, vähemalt USA-ga samaväärne turvalisus, ei saa järeldada, et seal rakendatakse isikuandmetele kõrgetasemelist kaitset.

Seega on Ameerika Ühendriikides lähenemine andmekaitsele Euroopaga võrreldes vägagi erinev. USA-s puudub ühtne andmekaitse raamistik, selle asemel tegeletakse seal andmekaitsega valdkonniti. Ühendriikides reguleerivad andmekaitset mitmed erinevad föderaalsed ning osariikide seadused ning kaitset pakutakse vaid tähtsamatele isikuandmete liikidele. Pealgi on USA-s andmekaitsel hägune tähendus, sest see on vaid üks osa privaatsusõigusest. Samas ei leia seal ka privaatsusõiguse nii tugevat kaitset kui Euroopas.

Lisaks on USA-le omane, et kontrastselt eristatakse privaatsusõigust, mille alakategooriaks on andmekaitse, suhtes riik ja indiviid ning teised isikud ja indiviid. Leian, et selline tugev eristus tuleneb ameerikalikust liberaal-majanduslikust printsiibist, mille kohaselt on kõige paremini toimiv majandus riigi piirangutest vaba. Vaba turu konkurents on see, mis paneb ettevõtjaid käituma tarbijatele meelepäraseimal viisil. Andmetöötluses vaatepunktist tähendab see, et ettevõtted, kes ei austa isikute privaatsust andmete töötlemisel, kaotavad tarbija usalduse ning seeläbi ka oma positsiooni turul. Kui ettevõttel läheb hoolimata andmekaitse tavade järgimata jätmisest turul hästi, ei ole tarbijatele see oluline. Nii ongi kujunenud, et andmete töötlemisel ja

[116] J. Clark, K. Lucente; lk 492
[117] *Ibid*
[118] Ameerika Ühendriikide Konstitutsioon, artikkel 1 lõige 8; kättesaadav: https://www.archives.gov/founding-docs/constitution-transcript#toc-section-8- (01.05.2017)
[119] Cornell'i Ülikooli õigusteaduskonna õigusinformatsiooni instituut; *Commerce Clause*; kättesaadav: https://www.law.cornell.edu/wex/commerce_clause (01.05.2017)

privaatsusreeglite sätestamisel on peamiselt peetud silmas riigi omavoli piiramist ning kaubandussektoris on jäetud suures osas andmekaitse reeglite rakendamine ettevõtete enda kätte, kes soovi korral rakendavad ise-regulatsiooni.

1.3. Atlandiüleses andmevahetuse õiguslik raamistik

Eelpool esitatu tõendab, et USA õiguskord ei taga isikuandmete piisavat kaitset EL-i standardite järgi. Oluline on siinjuures tähelepanu pöörata asjaolule, et USA on föderaalriik, mille 50-le osariigile on USA konstitutsiooni kümnenda parandusega[120] garanteeritud teatud isevalitsemise õigus, mille kohaselt valdkonnad, mille reguleerimine ei ole antud föderaalsete institutsioonide kätte, kuuluvad osariikide pädevusse.[121] Seega võib USA Konstitutsioon välistada Kongressi õiguse rakendada üleriigilist EL-i tüüpi laiaulatuslikku andmekaitse reeglistiku, mis võimaldaks direktiiv 95/46 artikkel 25 alusel USA-sse isikuandmeid edastada. See aga tähendaks, et tulenevalt USA kui föderaalriigi põhiõiguskorrast ei ole USA-le tervikuna võimalik adekvaatsusotsust väljastada.

Teisest küljest, kui rõhutada isikuandmete majanduslikku tähtsust, võib jõuda ka seisukohale, et isikuandmete kasutamise reguleerimine kuulub Konstitutsiooni artikkel 1 lg 8 kohaselt justnimelt Kongressi pädevusse. Kuna andmekaitse ei ole kindlasti vaid kaubandusvaldkonna küsimus, ei saa ju unustada selle põhiõiguslikku mõõdet, eeldab andmekaitse piisava taseme saavutamine USA-s eesmärgipärast koostööd föderaalsel ning osariikide tasandil, mille saavutamine lähitulevikus on tõenäoliselt välistatud.

Digitaalmajanduse olulisuse tõttu on siiski mõlemal pool Atlandit prioriteediks hoida andmevood võimalikult vabad. Direktiivi artikkel 25(6) seda ka võimaldab, kui ebapiisava kaitsetasemega riik võtab omale rahvusvahelised kohustused, millega isikuandmete kaitse piisav tase siiski saavutatakse. Nagu näha järgenvast, just sellise tee USA ja EL valisidki.

Käesolevas alapeatükis on tähelepanu all Atlandiülese andmevahetuse õiguslik raamistik, mis sai alguse Komisjoni 26. juuli 2000. a. otsusega 2000/520/EÜ programmi *Safe Harbor* põhimõtete piisava andmekaitse taseme tagamise kohta ning asendus 12. juuli 2016

[120] USA konstitutsiooni kümnenda parandus sätestab: „Õigused, mida ei ole põhiseadusega Ameerika Ühendriikidele delegeeritud ning mis ei ole põhiseadusega osariikidele keelatud, kuuluvad vastavalt osariikidele ja rahvale.“

[121] Cornell University Law School, Legal Information Institution; *U.S. Constitution – Tenth Amendment*; kättesaadav: https://www.law.cornell.edu/anncon/html/amdt10_user.html#amdt10_hd4 (01.05.2017) USA konstitutsiooni kümnenda paranduse kohaselt kuuluvad õigused, mida ei ole põhiseadusega Ameerika Ühendriikidele delegeeritud ning mis ei ole põhiseadusega osariikidele keelatud, kuuluvad vastavalt osariikidele ja rahvale.

rakendusotsusega (EL) 2016/1250 andmekaitseraamistiku *Privacy Shield* piisavuse kohta. Lisaks annab autor ülevaate selle paradigmavahetuse põhjustanud kohtuasjast C-362/14 *Schrems*.

1.3.1. Safe Harbor ja kohtuasi C-362/14 *Schrems v. Data Protection Commissioner*

Läbirääkimised USA ning EL-i vahel andmekaitse küsimuse üle algasid 90nendate teisel poolel. Pärast 1995. aastal vastuvõetud direktiivi oli ilmne, et USA privaatsusreeglid ei taga direktiivile vastavat andmekaitse taset ning Atlandiülesele andmevoolule tähendas direktiivi jõustumine piirangute seadmist. Kui alguses väljendasid mõned EL-i ametnikud, et Euroopa Liitu rahuldab ainult see, kui USA võtab vastu ametliku andmekaitse regulatsiooni, mis tagaks andmesubjektidele direktiiviga võrreldes võrdset või piisavat kaitset, siis 1998. aasta esimeseks pooleks olid pooled jõudnud kokkuleppele, et andmevahetuspiirangute vältimiseks luuakse direktiivi artikkel 25(6) alusel raamistik kohustustest, mida USA andmetöötlejad eurooplaste andmete töötlemiseks järgima peavad ning mille täitmisele kohustub USA rakendama järelevalvet.[122]

Esimene ettepanek põhimõtetest, mis hiljem moodustasid *Safe Harbor*'i tuli samuti juba 1998. aastal USA kaubanduse aseministrilt David Aaronilt. Neid põhimõtteid oli seitse ning need adresseerisid kõiki direktiivis ning WP29 poolt esile tõstetud tagatisi andmesubjektile tema andmete töötlemisel. Nii USA kui EL näitasid üles lootust, et *Safe Harbor* kiidetakse kiiresti heaks ning peagi algab selle alusel Atlandiülene andmete vahetus. Nii see siiski ei läinud, mitmed liikmesriigid näitasid üles kahtlusi *Safe Harbor*'i pakutava turvalisuse taseme kohta. Järgnes 18 kuud keerulisi läbirääkimisi, mis lõppesid 31. mail 2000. aastal, kui liikmesriigid nõustusid printsiipidesse sisse viidud parandustega ning USA ja EL jõudsid *Safe Harbor* raamistiku sisus kokkuleppele.[123] 26. juulil järgnes kokkulepitud raamistiku osas Komisjoni adekvaatsusotsus 2000/520/EÜ.

Safe Harbor raamistik oma lõppkujul koosnes kolmest elemendist: andmetöötluspõhimõtted[124], korduma kippuvad küsimused[125] ning *Safe Harbor* programmi täitmise tagamise ülevaade.[126]

---

[122] H. Farrell; *Constructing the International Foundations of E-Commerce: The EU-U.S. Safe Harbor Arrangement*; International Organization, Vol. 57, Nr 2; Spring 2003; lk 285
[123] *Ibid*; lk 286
[124] Komisjoni otsus 2000/520/EÜ lisa 1 – Programmi *Safe Harbor* põhimõtted ;lk 122-125
[125] Komisjoni otsus 2000/520/EÜ lisa 2 – Kordama kippuvad küsimused; lk 126-138
[126] Komisjoni otsus 2000/520/EÜ lisa 3 – Ülevaade programmi *Safe Harbor* täitmise tagamisest – Föderaalsed ja osariikide volitused seoses kõlvatute tavade ja pettusega ja eraelu puutumatus; lk 139-143

Kokku lepiti seitsmes põhimõttes:[127]

1) Teatamise põhimõte – töötleja peab üksikisikutele teatama, millistel eesmärkidel ta kogub ja kasutab nende kohta käivaid andmeid, kuidas võtta töötlejaga ühendust päringute või kaebuste korral, missugust liiki kolmandatele osapooltele ta andmeid avaldab ning valikutest ja vahenditest, mida töötleja üksikisikutele andmete kasutamise ja avaldamise piiramiseks pakub.
2) Valikuvõimaluse põhimõte – töötleja peab pakkuma isikutele valida (*opt-out* valik), kas nende isikuandmeid a) avaldatakse kolmandatele osapooltele või b) kasutatakse muul eesmärgil kui see, milleks neid algselt koguti või milleks isik loa andis. Delikaatsete isikuandmete osas tuleb võimaldada kinnitav või selge valik (*opt-in* valik).
3) Edasise edastamise põhimõte – kui töötleja edastab isikuandmeid kolmandale osapoolele, peab ta järgima teatamise ning valikuvõimaluse põhimõtteid.
4) Turvalisuse põhimõte – isikuandmete töötlejad peavad rakendama abinõusid, mis tagaksid töödeldavate andmete turvalisuse.
5) Andmeterviklikkuse põhimõte – kooskõlas *Safe Harbor* põhimõtetega peavad isikuandmed vastama nende kasutusotstarbele. Isikuandmeid ei tohi töödelda viisil, mis ei vasta eesmärkidele, milleks need koguti või milleks andmesubjekt loa andis. Töötleja peab tagama, et isikuandmed, mida kasutatakse eesmärgi täitmiseks, on usaldusväärsed, täpsed, täielikud ja aktuaalsed.
6) Juurdepääsu põhimõte – andmesubjektile peab võimaldama juurdepääsu tema isikuandmetele, mis on töötleja käsutuses. Ta võib nõuda nende parandamist, muutmist, ja kustutamist, kui need on ebatäpsed.
7) Täitmise tagamise põhimõte – Tõhus isikuandmete kaitse peab hõlmama mehhanisme, mis tagaksid põhimõtete järgimise ja kaebuste käsitlemise võimaluse üksikisikutele, keda puudutavaid andmeid põhimõtete eiramine on mõjutanud, ning tagajärgi töötlejale, kes põhimõtteid ei järgi. Need mehhanismid peavad sisaldama minimaalselt: a) käepäraseid ja taskukohaseid sõltumatuid kaebuste käsitlemise mehhanisme, millega iga üksikisiku kaebusi ja vaidlusi uuritakse ja lahendatakse võrdluses põhimõtetega ning määratakse kahjutasu juhul, kui kohaldatav seadus või erasektori initsiatiiv seda ette näeb; b) kontrollimeetmed kinnitamaks, et tunnistused ja väited, mida töötlejad esitavad, vastavad tõele, ning endale võetud *Safe Harbor*'i kohustused on ellu rakendatud; ja c) kohustusi heastada põhimõtetele mittevastavusest tekkivad probleemid töötlejate poolt, kes on kohustunud põhimõtetest kinni pidama ning ka

[127] Komisjoni otsus 2000/520/EÜ lisa 1; lk 123-124

tagajärgi selliste töötlejate jaoks. Sanktsioonid peavad olema piisavalt ranged tagamaks printsiipide jälgimise.

Safe Harbor-i allakäik algas 2013. aastal, kui tollane CIA töötaja Edward Snowden paljastas inimõiguste seisukohast kahtlusi tekitava USA massluure programme käsitlevad dokumendid.[128] See motiveeris Euroopa Komisjoni läbi viima ulatuslikku kontrolli *Safe Harbor* programmi poolt pakutava isikuandmete kaitse piisavuse üle. Kontrolli tulemusel tegi Komisjon kindlaks mitmete puudujääkide esinemise[129] ning alustas Ühendriikidega läbirääkimisi uuema ja tugevama Atlandiülese raamistiku kokkuleppimiseks.

Samuti Snowdeni paljastustest lähtuvalt esitas 25. juunil 2013 Austriast pärit õigusteaduse tudeng Maximillian Schrems Iirimaa andmekaitsevolinikule kaebuse, milles ta palus keelata Facebook Ireland'il tema isikuandmeid edastada Ameerika Ühendriikidesse.[130] Schremsi sõnul tõestavad Snowdeni paljastused, et USA ei taga tegelikult piisaval tasemel eurooplaste isikuandmete kaitset ning seega tuleks andmete edastamine sinna keelata. Facebook Ireland nimelt, on sotsiaalvõrgustiku Facebook tütarfirma, millega on kõik Euroopas asuvad Facebooki kasutajad sõlminud lepingu. Facebook Ireland edastab Euroopast pärit kasutajate andmed kas osaliselt või täitelikut USA-s asuvatesse Facebooki serveritesse, kus neid andmeid töödeldakse.[131] Andmete edastamine kahe Facebooki vahel käis *Safe Harbor* programmi alusel.

Iiri andmekaitsevolinik keeldus Schremsi kaebuse läbivaatamisest, sest Schrems ei tõestanud, et tema isikuandmeid oleks USA luureprogrammid kuidagi puudutanud. Lisaks märkis volinik, et andmete edastamine Ühendriikidesse toimub adekvaatsusotsuse alusel ning seega on *Safe Harbor* programmi alusel tagatud isikuandmete piisav kaitse. Schrems esitas selle peale kaebuse Iiri Kõrgemale Kohtule (*Irish High Court*). Pea aasta pärast esialgse kaebuse esitamist tegi kohus otsuse, mis erines andmekaitsevoliniku seisukohast teravalt. Iiri Kohus leidis, et Schremsi kaebus on Snowdeni paljastuste valguses õigustatud, sest kuigi USA luureprogrammid teenivad avalikke huve, on föderaalasutused oma pädevust nende rakendamisel ulatuslikult ületanud ning andmesubjektil, kelle andmeid on Ühendriikidesse edastatud, puudub igasugune võimalus olla ära kuulatud, kui ta leiab, et tema isikuõigusi on rikutud. Lisaks leidis kohus, et isikuandmete riigipoolne kogumine peab olema seadustega

[128] A. Callahan-Slaughter; *Lipstick on a Pig: The Future of Transnational Data Flow Between the EU and the United States*; Tulane Journal of International & Comparitive Law; Vol 25, 2016; lk 249
[129] Euroopa Komisjon; *Komisjoni teatis Euroopa Parlamendile ja nõukogule usalduse taastamine ELi ja Ameerika Ühendriikide vaheliste andmevoogude vastu COM(2013) 846 final*; 27.11.2013, Brüssel ja Euroopa Komisjon; *Komisjoni teatis Euroopa Parlamendile ja Nõukogule, mis käsitleb programmi Safe Harbor toimimist ELi kodanike ja ELis asuvate äriühingute seisukohast COM(2013) 847 final*; 27.11.2013, Brüssel
[130] N. Loiden; *The End of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law*; Journal of Internet Law, Vol 19, nr 8; veebruar 2016, lk 9
[131] EK otsus asjas C-362/14 *Schrems* p-d 27-28

kooskõlas, proportsionaalne ning objektiivselt põhjendatud ja esitatud asjaoludest lähtudes esineb tugevaid kahtlusi, et USA riigiasutused neid põhimõtteid jälgisid. Vähemalt oleks andmekaitsevolinik pidanud Schremsi kaebuses esile toodud asjaolusid uurima ning läbi vaatamata jätmine oli ekslik. Kohus tundis ära, et vaidlus puudutab oluliselt Euroopa Liidu õiguse kohaldamist, sest sisuliselt vaidlustab Schrems oma kaebuses *Safe Harbor*'i adekvaatsusotsuse õiguspärasust, ja esitas seetõttu Euroopa Kohtule eelotsuse küsimused andmekaitsevoliniku volituste ulatuse kohta.[132]

EK leidski, et *Safe Harbor* ei taga isikuandmete piisavat kaitset USA-s ning tunnistas Komisjoni otsuse 2000/520 kehtetuks. Põhjuseks oli otsuse 200/520 lisa 1 neljas lõik, mis lubab USA andmetöötlejad riikliku julgeoleku, avaliku huvi või õiguskaitseliste vajaduste täitmiseks vajalikus ulatuses *Safe Harbor* põhimõtetest piiramatult kõrvale kalduda. EL-is peab liidu õigusakt, millega kaasneb sekkumine privaatsus- või andmekaitse põhiõigusesse sisaldama selgeid ja täpseid õigusnorme, mis reguleerivad meetme ulatust ja kohaldamist ning millega on kehtestatud miinimumnõuded, nii et isikutel oleks piisavad tagatised, mis võimaldavad nende andmeid tõhusalt kaitsta kuritarvitamise ohu ning ebaseadusliku juurdepääsu ja kasutamise eest.[133] *Safe Harbor* programmi alusel edastatavad eurooplaste isikuandmed võisid selle printsiipidega kooskõlas sattuda Ühendriikide föderaalsete ametiasutuste valdusesse, selliseid olukordi aga raamistik ei reguleerinud ning puudus ka vajalik järelevalve neis olukordades, mistõttu ei taganud *Safe Harbor* piisavat kaitset eurooplaste isikuandmetele direktiivi artikkel 25(6) tähenduses. Seega ei näinud EK vajadust *Safe Harbor*'i printsiipide sisuliseks hindamiseks.[134] Otsuse tegemisel kandis olulist kaalu Euroopa Komisjoni 2013. aastal tehtud järeldused teatistes COM(2013) 846 final[135] ja COM(2013) 847 final.[136] Nimelt tuvastas Komisjon, et *Safe Harbor* programmi alusel USA-sse edastatud isikuandmetele said USA ametiasutused tõepoolest piiramatu ligipääsu.[137]

Eelnevaga seoses soovib siinkirjutaja täiendavalt tähelepanu juhtida järgnevale. Kuna *Safe Harbor* programmiga liitumine oli iga USA andmetöötleja vaba voli ja seega sisuliselt tegemist ise-regulatsiooni rakendamisega, kuulus nende reeglite järgimise üle järelevalve teostamine Ühendriikide FTC pädevusse. Nii on ka *Safe Harbor* programmis sätestatud.[138] FTC tegevus laieneb ainult kaubandusalasele/ärilisele tegevusele, seega ei saa FTC rakendada järelevalvet

[132] *Ibid* p-d 29-36
[133] Otsus C-362/14, *Schrems*; punkt 91
[134] *Ibid*, punktid 86-88 ja 89-98
[135] Euroopa Komisjoni teatis COM(2013) 846 final
[136] Euroopa Komisjoni teatis COM(2013) 847 final
[137] Otsus C-362/14, *Schrems*; punktid 90-91
[138] Komisjoni otsus 2000/520/EÜ; preambuli punkt 5

nende andmete töötlejate üle, kes ei töötle andmeid ärilistel eesmärkidel. Siit algabki käesoleva töö autori hinnangul probleem, mis *Safe Harbor*'ile saatuslikuks sai. Nimelt on direktiivi kohaselt andmete töötlejaks nii füüsiline ja juriidiline isik, kui ka riigiasutus, esindus või muu organ. Kõik nemad on direktiivi kohaselt kohustatud isikuteks, kelle üle on kohalikel andmekaitse asutustel õigus rakendada järelevalvet. *Safe Harbor* on raamistik, mille eesmärgiks on võimaldada lihtsustatud korras ning piiranguteta eurooplaste isikuandmete edastamist ning töötlemist USA ettevõtetel ja seega võib tunduda, et on piisav, kui järelevalveasutuseks on kaubandusvaldkonna organ. Kuid raamistikuga on ettenähtud erandid, mille esinemisel töötleja ei pea *Safe Harbor* printsiipe järgima ning seega võivad isikuandmed sattuda FTC jurisdiktsioonist välja. Eelkõige mõtlen siin olukordi, kus töötleja peab isikuandmeid edastama valitsusele riikliku julgeoleku, avaliku huvi või õiguskaitseliste vajaduste täitmiseks või statuudi, valitsuse määruse või pretsedendiõiguse alusel, mis loovad vasturääkivaid kohustusi või annavad selleks otseseid volitusi. Nagu eelpool nägime (vt peatük 1.2.2.) rakendub USA föderaalorganite poolsele isikuandmete töötlemisele privaatsusseadus, mis garanteerib andmesubjektidele elementaarsed andmekaitseõigused. Andmesubjektid, kelle privaatsusõigusega USA föderaalvalitsus isikuandmete töötlemisel arvestama peab, on Privaatsusseaduse kohaselt ainult ameerika kodanikud ning õiguslikul alusel USA territooriumil resideeruvad isikud. Seega juba siit nähtub, et *Safe Harbor* ei pakkunud piisavat kaitset eurooplaste isikuandmetele olukorras, kus andmete töötlejaks osutus riigiasutus ning see oleks pidanud olema nähtav juba otsuse 2000/520 vastuvõtmisel. Alates 2014. aastast on olukord muutunud: President Obama piiras Presidentaalse direktiivi nr 28 (edaspidi „PPD-28" – *Presidential Policy Directive 28*) vastuvõtmisega USA luureametkonna tegevust välisriikide kodanike suhtes läbiviidava andmete kogumise osas.[139] PPD-28 nõuab, et kõiki isikuid tuleb teabe kogumisel kohelda austusega ning inimväärikalt, luureandmete kogumine võib toimuda vaid statuudi alusel või Presidendi loal ning see peab toimuma kooskõlas USA seaduste ja konstitutsiooniga, privaatsuse ning isikuõiguste tagamine peab olema prioriteet ning elektroonilise side kogumine peab garanteerima kõikide isikuandmete kaitsmise. Lisaks sätestab PPD-28, et elektroonilist sidet võib koguda vaid välisluure ja vastuluure eesmärgil ning see peab toimuma niivõrd kohandatuna, kui võimalik igast konkreetsest olukorrast lähtudes sobilike vahendite rakendamisel.[140]

[139] Valge Maja, Presidential Policy Directive/PPD-28, 17.01.2014, kättesaadav: https://fas.org/irp/offdocs/ppd/ppd-28.pdf (14.03.2017)
[140] Komisjoni rakendusotsus 2016/1250, punkt 68

Siinkirjutaja arvates oleks EK pidanud jõudma samale tulemusele, kui otsus oleks tehtud *Safe Harbor* printsiipidest lähtuvalt.

Esiteks ei ole *Safe Harbor* dokumentides käsitletud kolmandatele isikutele isikuandmete edastamist sisuliselt. Töötleja peab isikuandmete kolmandatele isikutele printsiipidega kooskõlas olevaks edastamiseks andmesubjekti teavitama vastava kolmanda osapoole liigist ning andma andmesubjektile võimaluse sellisest edastamisest keeldumiseks. Kolmanda osapoole poolt rakendatava andmekaitse taseme kohta ei ole ühtegi nõuet sätestatud.

Direktiivi järgse isikuandmete edastamise puhul saab andmesubjekt eeldada, et kolmas isik, kellele andmeid edastatakse, kuulub direktiivi alusel vastuvõetud seaduse või sellega võrdväärset kaitsetaset pakkuva jurisdiktsiooni alla ning seega on tema isikuandmete turvalisus tagatud. *Safe Harbor* printsiibid seda kindlust isikule ei võimaldanud. Andmesubjektile on küll antud võimalus andmete kolmandatele isikutele edastamisest keelduda, kuid autori arvates ei taga kolmanda osapoole liigist teadaandmine andmesubjekti piisavat informeerituse taset, et ta saaks langetada kaalutletud otsuse oma andmete edastamise kohta. Edasise edastamise põhimõte oleks võinud olla direktiiviga vastavuses, kui andmetöötlejal lasuks kohustus esitada isikule põhjalik ülevaade kolmandast isikust, kellele andmete edastamiseks ta nõusolekut küsib. Kindlasti oleks pidanud see informatsioon sisaldama ülevaadet kolmanda isiku tegevusest ning andmekaitsealastest meetmetest ning piirangutest, mida see isik oma tegevusele rakendab.

Kuna kolmandatele osapooltele isikuandmete edastamist *Safe Harbor* sisuliselt ei reguleerinud, oli täitmata ka direktiivi artiklist 11(1) tulenev nõue, mis sätestab, et kui andmed ei ole saadud andmesubjektilt, tuleb talle teada anda töötlemise eesmärk ning astutava töötleja andmed. *Safe Harbor* sätestas vaid kolmanda osapoole, kes samuti on töötleja, liigi kohta informatsiooni andmise kohustuse.

Lisaks tagab direktiivi artikkel 22 andmesubjektidele õiguse kasutada õiguskaitsevahendeid töötleja suhtes, kes tema isikuõigusi rikub. Näiteks Eesti Isikuandmete kaitse seadus annab sellisel juhul andmesubjektile õiguse nõuda kahju hüvitamist võlaõigusseaduse või riigivastutuse seaduse alusel ja korras.[141] Ka *Safe Harbor*'i dokumentides on sellisele võimalusele viidatud. Kahju hüvitamise aluseks pakub USA kaubandusministeerium (edaspidi „DoC" – *Department of Commerence*), mille vastav seisukoht on *Safe Harbor* programmi

[141] Isikuandmete kaitse seadus § 23, RT I, 06.01.2016, 10

ametlikuks osaks, esiteks, pettuse või väärinformatsiooni avaldamise ning teiseks, eraelupuutumatuse rikkumise.

Valeandmete esitamine või pettus on USA õiguse kohaselt kahju hüvitamise aluseks.[142] Rikkumine sellisel juhul seisneks selles, et töötleja, kes on *Safe Harbor* raamistikuga liitunud, on teinud ka vastavasisulise avalduse, milles ta kinnitab, et järgib andmete kogumisel ja töötlemisel vastavaid printsiipe.[143] Kui see töötleja neid printsiipe ei järgi, on ta teinud valeavalduse ning seega petnud andmesubjekti, kes töötleja avaldusele tugines. Eelduseks on andmetöötleja kuritahtlikus ehk ta teadvalt avaldas, et ta järgib *Safe Harbor* põhimõtteid, kuigi tegelikkuses ta seda ei teinud.[144] Ka lohakusest ehk hoolsuskohustuse rikkumisest tulenev valeväide võib olla kahju hüvitamise aluseks, kuid sellisel juhul on määratav kahjutasu piiratud konkreetse rahalise kahjuga, mida selline valeavaldus andmesubjektile põhjustas. Seega on valeandmete esitamise või pettuse alustel kahju hüvitamine pigem piiratud, sest pahatahtlikkuse tõendamine on keerukas ning konkreetset rahalist kahju ei pruugi isikuandmete õiguste rikkumisega kaasneda.[145]

Teisena pakub DoC välja kahju hüvitamise võimaluse printsiipidega tagatud õiguste rikkumise puhul privaatsushagi esitamisega.[146] Siiski, nagu alapeatükis 1.2.2. selgitatud, on siiani USA kohtud pigem eitanud võimalust andmekaitse alaste rikkumiste eest kahju hüvitamist nõuda.

Kahju hüvitamist võimaldavad nõuda ka mitmed osariikide õigusaktid, kui andmete töötleja rikub koos *Safe Harbor* põhimõttega mõne osariigi seadust, mis tema tegevusele kohaldub (see oleneb töötleja asukohast). Osariikide seadused reguleerivad andmete töötlemist valdkonniti ning erinevate osariikide andmekaitse ulatused on erinevad.[147] Seega ei näi ka sel teel olevat võimalik tagada, et printsiipide rikkumise tagajärjel avaneb kannatanule võimalus nõuda kahju hüvitamist.

Hoolimata eelnevast peab DoC tõenäoliseks, et neile, kes programmi *Safe Harbor* põhimõtete mittejärgimise tõttu kannatavad, mõistetakse rahaline hüvitis.[148] Tulenevalt eelnevast on siiski

---

[142] Federal Trade Commission Act (edaspidi FTCA) § 5, kättesaadav: https://www.ftc.gov/sites/default/files/documents/statutes/federal-trade-commission-act/ftc_act_incorporatingus_safe_web_act.pdf (14.03.2017)
[143] Komisjoni otsus 2000/520/EÜ, lisa 1, lõik 3
[144] Tuleneb FTCA §-st 5
[145] Vt alapeatükk 1.2.2.2.
[146] *Ibid*
[147] I. Jolly 2014/2015
[148] Komisjoni otsus 2000/520/EÜ; lk 146

kaheldav, kas *Safe Harbor*'i printsiipide rikkumisega tekitatud kahju hüvitamine oleks andmesubjektile olnud kättesaadav võrdväärselt nii *Safe Harbor*'i kui ka direktiivi alusel.

1.3.2. *Safe Harbor*'i lõpp ja *Privacy Shield'*i algus

Ajal mil EK *Safe Harbor* programmi kehtetuks tunnistas, võttis selle alusel isikuandmeid vastu üle 5000 ettevõtte teisel poolt Atlandit.[149] *Safe Harbori* kehtetuks tunnistamine tähendas, et sisuliselt päevapealt muutus selle programmi alusel isikuandmete edastamine ebaseaduslikuks.

Pärast EK otsust tegi WP29 avalduse, millega andis Komisjonile 2016. aasta jaanuari lõpuni aega USA ametiasutustega uue sobiliku lahenduse leidmiseks Atlandiüleseks andmevahetuseks. Selle tähtaja vastu eksimine oleks tähendanud, et EL-i andmekaitseasutused oleksid hakanud rakendama kõiki vajalikke ning asjakohaseid meetmeid, et tagada nõuete täitmine ning eurooplaste isikuandmete kaitse.[150] Kuigi WP29 avaldustel ning nõuannetel ei ole Komisjonile siduvat mõju, tähendas tähtaja seadmine seda, et liikmesriikide andmekaitse asutused võimaldasid ebaseadusliku *Safe Harbor* programmi alusel andmeid USA-sse edastada kuni nimetatud tähtajani. Kuni selle tähtajani nõustus WP29 *Safe Harbor*'i alusel andmete edastamisele piirangute seadmisest ning ettevõtetele sunnivahendite rakendamisest hoiduma kuni *Privacy Shield*'i adekvaatsusotsuse jõustumiseni.[151]

Avalduses märkis WP29, et kuigi *Safe Harbor*-'i alusel isikuandmete edastamine on keelatud, saab vahepeal andmete edastamise alusena kasutada andmekaitseasutuste poolt kinnitatud lepingutingimusi või kontserni sise-eeskirju.[152] Lisaks saab õiguspäraselt andmeid USA-sse edastada, kui esineb mõni direktiivi artiklist 26(1) tulenev erand.

2. veebruaril 2016 jõudsid USA esindajad ning Komisjon kokkuleppele uue transatlantilise andmete edastamise raamistikus, mis ristiti *Privacy Shield*'iks. Pressiteates väitsid Komisjoni esindajad, et „… uus raamistik kaitseb nende eurooplaste põhiõigusi, kelle andmed on edastatud Ameerika Ühendriikidesse, ning tagab ettevõtjatele õiguskindluse" ja asepresident Andrus

[149] N. Loiden; lk 1
[150] Artikkel 29 Töörühma 16.10.2015 avaldus; kättesaadav: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf (15.03.2017)
[151] Andmekaitse Inspektsioon; *Isikuandmete liigutamine Euroopa ja Ameerika vahel lihtsustub*; 09.02.2016; kättesaadav: http://www.aki.ee/et/uudised/pressiteated/isikuandmete-liigutamine-euroopa-ja-ameerika-vahel-lihtsustub (15.03.2017)
[152] Artikkel 29 Töörühma 16.10.2015 avaldus; lk 1

Ansip lisas, et nüüd võivad eurooplased „… olla kindlad, et nende isikuandmed on igati kaitstud*“.*[153]

Artikkel 29 Töögrupp tervitas seda kokkulepet ning luges selle tähtaegseks ja jäi ootama Privacy Shield programmi dokumentide avaldamist. Põhjus, miks Komisjonil õnnestus niivõrd kiiresti USA-ga sellise kokkuleppeni jõuda, oli selles, et pärast 2013. aasta teatiste avaldamist alustas Komisjon läbirääkimisi toonase *Safe Harbor* programmi parandamiseks, et kõrvaldada puudused, millele Komisjon oma teatistes tähelepanu suunas. Pärast EK otsust asjas C-362/14 *Schrems* need läbirääkimised hoogustusid ning arvesse võeti ka kohtu seisukohti kolmanda riigi või tema võetud rahvusvaheliste kohustustega pakutava andmekaitse taseme piisavuse hindamise kohta.[154]

29. veebruaril avaldas Komisjon *Privacy Shield* programmi dokumendid ning selle kohta koostatud adekvaatsusotsuse eelnõu. Eelnõu lisadena avaldati seitse dokumenti, mille hulgas olid *Privacy Shield* printsiibid ning mitmed kirjad koos kinnitustega USA riigisekretärilt, FTC esinaiselt, kaubandusministrilt ja teistelt, mis koos moodustavadki *Privacy Shield* programmi.[155]

Artikkel 29 Töögrupp võttis avaldatud adekvaatsusotsuse teadmiseks ning alustas direktiiv 95/46 artikkel 30(1c) alusel arvamuse koostamist adekvaatsusotsuse eelnõu kohta, mis avaldati 13. aprillil 2016.[156] Töögrupp leidis, et esitatud programmis esineb mitmeid murekohti, millega Komisjon peaks enne programmi jõustumist tegelema. Tõsisemaid probleem tuvastas töögrupp kolm: esiteks, ei kohusta *Privacy Shield* printsiibid senise sõnastuse kohaselt andmetöötlejaid kustutama isikuandmeid, mis ei ole neile enam vajalikud lepinguliste kohustuste täitmiseks, teiseks, näeb Töögrupp ikkagi probleeme USA luureasutuste poolse salajaste mass-luure programmide osas ning kolmandaks, pidades küll ombudsmani ametikoha sisseseadmist USA Riigidepartemangu juurde väga positiivseks sammuks, jääb esitatud dokumentidest ebakindlaks, kas ombudsmanil on efektiivseks funktsioneerimiseks piisavalt võimu.[157]

---

153 Euroopa Komisjoni pressiteade; Euroopa Liidu Komisjon ja Ameerika Ühendriigid leppisid kokku Atlandi-üleste andmevoogude uues andmekaitseraamistikus Privacy Shield; 02.02.2016

154 Komisjoni rakendusotsus (EL) 2016/1250; p 12

155 Euroopa Komisjon; *Commission decisions on the adequacy of the protection of personal data in third countries*, kättesaadav: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (15.03.2017)

156 Artikkel 29 Töögrupp arvamus 01/2016 EL-USA Privacy Shield adekvaatsusotsue eelnõu kohta, 13.04.2016; kättesaadav:http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf (15.03.2017)

157 *Ibid*, lk 57

Komisjon viis eelnõusse sisse parandused ning 8. juulil 2016 kiitis Artikkel 31 kommitee ehk liikmesriikide esindajatest koosnev organ parandused heaks ning *Privacy Shield* programmile anti roheline tuli.[158] 12. juulil võttis Komisjon *Privacy Shield* programmi osas vastu adekvaatsusotsuse (EL) 2016/1250.

Uus Atlandiülene isikuandmete edastamise raamistik on tekitanud palju vastuolu. Kohe pärast otsuse (EL) 2016/1250 eelnõu avaldamist lubasid mitmed privaatsusaktivistid selle vaidlustada Euroopa Kohtus, nende seas ka Max Schrems.[159] 16. septembril 2016 esitas Digital Rights Ireland Euroopa Kohtule hagi Komisjoni vastu, milles nõuab *Privacy Shield* adekvaatsusotsuse tühistamist.[160]

1.3.2.1. *Privacy Shield* õigusraamistik

Privacy Shield õigusraamistik on kooslus *Privacy Shield* dokumentidest – USA kaubandusministri Penny Pritzeri kiri ja selle seitse lisa, mis on adresseeritud Euroopa Komisjoni õigus- ja tarbijaküsimuste ning soolise võrdõiguslikkuse volinikule Vera Jourovale – ning Komisjoni rakendusotsusest 2016/1250. *Privacy Shield* dokumendid moodustavad USA DoC eestvedamisel kokku pandud programmi, millega liitnud USA andmetöötlejad võtavad omale kohustuse töödelda EL-ist edastatavaid isikuandmeid teatud viisil.[161] Teisest küljest, kuna *Privacy Shield* põhimõtetes on jäetud võimalus USA ametiasutustele rakendada USA siseriiklikust õigusest tulenevat volitust koguda USA isikuandmete töötlejatelt isikuandmeid teatud julgeolekulistel või avalikust huvist tulenevatel põhjustel, sisaldavad *Privacy Shield* dokumendid ka ülevaadet USA õiguskaitse- ja luureasutuste tegevust reguleerivatest dokumentidest.[162]

Seega on sisuliselt ka rakendusotsuse 2016/1250 puhul tuvastatavad kaks tasandit – esimese puhul hindab Komisjon *Privacy Shield* programmi, sealhulgas *Privacy Shield* põhimõtete poolt pakutava isikuandmete kaitse taseme vastavust EL-i omale ning teisel tasandil hindab Komisjon USA õiguskorra osa, mis võimaldab sekkumist *Privacy Sheild* programmi alusel USA töötlejatele edastatud isikuandmetesse vastavust EL-i õigusele.

---

[158] Euroopa Komisjoni teadanne *Statement by Vice-President Ansip and Commissioner Jourova on the occasion of the adoption by MemberStates of the EU-U.S. Privacy Shield*; 08.07.2016, Brüssel; kättesaadav: http://europa.eu/rapid/press-release_STATEMENT-16-2443_en.htm (15.03.2017)

[159] L. Hynes; *Privacy Shield – lipstick on a pig?*; 11.03.2016; kättesaadav: http://thoughtleadership.leman.ie/post/102d8f1/privacy-shield-lipstick-on-a-pig (15.03.2017)

[160] Euroopa Liidu Teataja, ELT C 410, 07.11.2016, lk 26

[161] Rakendusotsus 1250/2016 lisa 2

[162] *Ibid* lisad 6 ja 7

Privacy Shield dokumentide tuumiku moodustavad *Privacy Shield* põhimõtted, mida USA isikuandmete töötlejad peavad EL-ist saadavate isikuandmete töötlemisel järgima ning koopereerima oma isikuandmete töötlemist puudutavatesse juhenditesse ja poliisidesse. Neid põhimõtteid on kaht tüüpi – üldpõhimõtted (edaspidi „PS põhimõtted“) ja täiendavad põhimõtted (edaspidi „PS täiendavad põhimõtted“). Esimesed on andmetöötlemise põhimõtted, mis on analoogsed EL-i vastavate põhimõtetega ning teised omavad PS põhimõtete suhtes selgitavat ja toetavat funktsiooni.

Nagu *Safe Harbor* õigusraamistik enne seda, on ka *Privacy Shield* vabatahtlikul kinnitamise süsteemile ja isereguleerimise printsiibil põhinev programm, millega liitumiseks ja millest tulenevate soodsamate tingimuste saamiseks peab USA andmetöötleja ise oma andmetöötlustavad kooskõlla viima. Kui ettevõte on sellise pühendumuse teinud, allub ta FTC või transpordiministeeriumi järelevalve alla, mis kontrollivad ettevõtte tegevuse vastavust ettevõtte poolt avaldatud privaatsuspoliisidele. Selleks, et ettevõttele võimaldataks õigusraamistiku alusel ligipääsu eurooplaste isikuandmetele eelneb ettevõtte suhtes DoC poolt läbiviidav kontroll PS põhimõtetele vastavuse kohta.

Avalike organite töötlemist puudutavatest kinnitustest rääkides, sisaldavad *Privacy Shield* dokumendid esiteks USA justiitsministeeriumi esindaja selgitusi USA õiguse selle osa kohta, mis lubab õiguskaitse- ja kohtuasutustel õiguskaitselistel ja avalikust huvist tulenevatel eesmärkidel sekkuda andmesubjektide privaatsusesse, seal hulgas andmekaitseõigusesse.[163] Teiseks, riikliku julgeoleku kaalutlustel andmesubjektide isikuõigustesse sekkumise aluseid selgitab USA luureorganisatsioone koondava riikliku luurejuhi ameti esindaja.

Luureasutuste tegevuse suhtes on ettenähtud eraldi kontrollimehhanism, mille kaudu EL-i andmesubjektidele on võimaldatud rakendada kontrolli USA luureasutuste suhtes, kui ta leiab, et tema andmekaitseõigusi on rikutud. Selleks saab andmesubjekt läbi oma kohaliku andmekaitseorgani ühendust võtta *Privacy Shield* ombudsmaniga, kellele on võimaldatud laialdased uurimisvolitused USA luureasutuste tegevuse suhtes.[164]

[163] *Ibid* lisa 7
[164] *Ibid* lisa 3

2. Komisjoni rakendusotsuse 2016/1250 alusel toimuva isikuandmete edastamise järjepidevust ohustavad tegurid

Nagu täheldas EK otsuses C-362/14 *Schrems*, peab Komisjon pärast adekvaatsusotsuse tegemist regulaarselt kontrollima, kas järeldus kolmanda riigi tagatava andmekaitse piisava taseme kohta on jätkuvalt põhjendatud, sest kolmanda riigi tagatav kaitsetase võib ajas muutuda.[165] Lisaks tuleb kehtivuse kontrollimisel arvesse võtta ka pärast selle otsuse vastuvõtmist aset leidnud asjaolusid.[166] Kuna need kaks tähelepanekut on tehtud otsuse erinevates punktides, tuleb järeldada, et neil on ka mingil määral erinev tähendus. „Pärast otsuse vastuvõtmist aset leidnud asjaolud", kui laiema tähendussisuga määratlus hõlmab seega asjaolusid, mis jäävad väljapoole kolmanda riigi tagatavat kaitsetaset.

Privacy Shield programmis on korduva kontrolli põhimõte sätestatud artiklis 4.[167] Vastavalt artiklile 4 hindab Komisjon igal aastal *Privacy Shield* programmi poolt pakutava kaitsetaseme piisavust ning esitab vajadusel meetmete eelnõu *Privacy Shield* programmi dokumentide muutmiseks, peatamiseks või kehtetuks tunnistamiseks.[168] Esimene selline iga-aastane kontroll toimub suvel 2017.[169]

Seega, kui eeldada, et *Privacy Shield* tagas rakendusotsuse 2016/1250 vastuvõtmise ajal 12. juulil 2016 eurooplaste isikuandmete kaitse piisava taseme (olgugi et juba paar kuud hiljem esitati rakendusotsuse vaidlustamiseks hagi, mis sellega ei nõustu) võib edaspidi nimetatud hindamiste teel selguda, et programmiga tagatud kaitse on siiski ebapiisav USA-st tulenevatest põhjustest, aga ka muudest, näiteks EL-ist endast tulenevtest põhjustest. Võttes arvesse pärast otsuse 2016/1250 vastuvõtmist toimunud asjaolusid on ilmselt suurima tähelepanu all USA värske presidendi Donald J. Trumpi administratsiooni poolt tehtud reformide ettepanekud ning rakendatud seadlused ja nende mõju USA õiguskorrale andmekaitse vaatevinklist üldiselt ja kitsamalt *Privacy Shield* programmiga eelmise administratsiooni poolt antud lubatuste täitmisele.

---

[165] Otsuse C-362/14, *Schrems*, punkt 76
[166] *Ibid* punkt 77
[167] Komisjoni rakendusotsus (EL) 2016/1250 artikkel 4
[168] *Ibid* artikkel 4(4) ja artikkel 4(6)
[169] Euroopa Komisjon; *Daily news 19/12/16*; 19.12.2016, Brüssel; kättesaadav: http://europa.eu/rapid/press-release_MEX-16-4463_en.htm (17.03.2017)

Aastal 2018 aga leiavad EL-i enda sees aset andmekaitse seisukohalt olulised muutused, millel on eelduslikult oluline mõju *Privacy Shield* programmile. Nimelt rakendub kevadel 2018 Euroopa Liidu andmekaitsereformi raames vastuvõetud õigusakt GDPR. Kuna GDPR muudab kehtetuks ning hakkab asendama direktiivi 95/46, muutub ka adekvaatsusotsuste õiguslik alus.

GDPR-i artikkel 45(1) kohaselt võib isikuandmeid kolmandale riigile või rahvusvahelisele organisatsioonile edastada, kui on olemas eelnev Komisjoni adekvaatsusotsus vastavas sihtpunktis rakenduva isikuandmete kaitse piisava taseme kohta. Sisuliselt ei lisa GDPR-i V peatükk, mis reguleerib isikuandmete edastamist EL-i jurisdiktsioonist välja poole, direktiivi 95/46 järgsele õiguskorrale isikuandmete kolmandatesse riikidesse edastamise kohta midagi fundamentaalselt uut, selles osas GDPR lihtsalt deklareerib mõningaid praktikas väljakujunenud seisukohti ja sõnastab reegleid varasemast detailsemalt.[170] Kuna andmekaitse reformi üheks eesmärgiks on tugevdada õigust eraelu puutumatusele[171], tõstab GDPR üldisemalt aga EL-i andmekaitse taset. Seega on GDPR-il ka otsene mõju rakendusotsusele 2016/1250, mis tunnistas *Privay Shield* programmi piisavat kaitset tagavaks lähtudes direktiivist 95/46.[172] Seega on *Privacy Shield* programmi osas tehtud adekvaatsusotsuse kehtivuse tagamiseks pärast kevadet 2018 oluline seda uuendada.

Algavas peatükis pöördub autor käesoleva töö põhiküsimuse lahendamise juurde ning võtab eesmärgiks kaardistada ning esile tuua küsimused ning probleemid ja osutada asjaoludele, mis vajalikke muudatusi rakendamata tingiksid edaspidi *Privacy Shield* programmi käsitleva adekvaatsusotsuse tühisuse pakutava andmekaitse taseme ebapiisavuse tõttu. Esimeses alapeatükis on tähelepanu raskuskese pärast otsuse 2016/1250 vastuvõtmist toimunud muudatustel, mis on tingitud USA-st ning millele peaks Komisjon eelseisval suvel toimuva kontrolli raames tähelepanu pöörama, et oleks tagatud *Privacy Shield* programmi käsitleva adekvaatsusotsuse järjepidevus. Teine alapeatükk kujutab endast detailsemat käsitlust *Privacy Shield* programmi pakutava andmekaitse taseme ebapiisavusest andmekaitse reformi kontekstis, täpsemalt analüüsib autor *Privacy Shield* põhimõtete ehk nimetatud programmiga liitunud USA ettevõtete poolsele isikuandmetele kohalduva andmetöötlusreeglite vastavust GDPR-ile. Läbivaks küsimuseks, millele autor kahes alapeatükis vastust otsib on: millised asjaolud seavad ohtu rakendusotsuse 2016/1250 järjepidevuse.

---

[170] T. Bräutigam; *The Land of Confusion: International Data Transfers between Schrems and the GDPR*; Helsinki 2016; Helsinki Ülikooli Õigusõppe Uurimustööde Seeria, nr 46; kättesaadav: https://ssrn.com/abstract=2920181 (17.03.2017); lk 149

[171] Euroopa Komisjon – Pressiteade; 25.01.2012, Brüssel; kättesaadav: http://europa.eu/rapid/press-release_IP-12-46_et.htm (18.03.2017)

[172] Komisjoni rakendusotsus (EL) 2016/1250 preambuli punkt 137 kohaselt tagab *Privacy Shield* sisuliselt samaväärse isikuandmete kaitsetaseme, nagu on tagatud direktiiviga 95/46

2.1. USA uus administratsioon, kui pärast otsuse 2016/1250 vastuvõtmist esinenud USA-st tulenev oluline asjaolu *Privacy Shield* programmi jätkuva piisava kaitse taseme tagamise positsioonilt

2.1.1. Avalike organite kinnitused *Privacy Shield* programmi käsitleva adekvaatsusotsuse eeldustena

Privacy Shield programmis on oluline osa USA erinevate ametiasutuste kinnitustel. Jälgides programmi sisulist struktuuri, mille esimese osa moodustab põhimõtete kogum, mida Atlanditagused ettevõtted peavad oma andmetöötlusele rakendama, et saada *Privacy Shield* programmist tulenevaid eeliseid ning teise osa moodustab reeglite kogum, mis rakendub USA ametiasutustele, kelle käsutusse võivad samuti EL-ist edastatavad isikuandmed teatud juhtudel jõuda, on neil kinnitustel suurem roll teise variandi kontekstis. *Privacy Shield* põhimõtete rakendamine ettevõtjate poolt on see, milles lasub küll kogu raamistiku tuum, kuid võttes arvesse eelmises peatükis selgitatut, allutavad ettevõtted, mis avalikult deklareerivad oma kasutustingimustes või privaatsuspoliisides teatud standardi järgimist oma klientide andmete töötlemisel, end FTC või transpordiministeeriumi järelevalve alla ning seega lasub neil avaliku deklareerimise tulemusel seadusest tulenev kohustus neist põhimõtetest kinni pidada igal juhul. Seega ei lisa *Privacy Shield* USA õiguskorda andmetöötleja positsioonilt midagi uut. Võime ju ka ettekujutada, et ettevõte, millel ei ole *Privacy Shield* programmiga mingit seost, avaldab andmetöötluspõhimõtted, mis on palju rangemad kui EL-i vastavad reeglid, avaldamise tõttu peab ta aga kohalikust õigusest tulenevalt neid standardeid oma tegevuses ka rakendama. Seega eksisteerivad USA õigussüsteemis *Privacy Shield* programmis mainitud järelevalve mehhanismid ning toimivad analoogsetel põhimõtetel ka ilma Komisjonile antud kinnitusteta. *Privacy Shield* ettevõtete üle toimub küll intensiivsem kontroll[173] DoC ja vastavate ametiasutuste poolt, kuid sisuliselt rakendavad nad kontrolli käigus USA õigust. *Privacy Shield* programmi teise osa puhul on kinnituste tähendus erinev.

Privacy Shield programmi raames USA-sse edastatavad andmed võivad programmi põhimõtetega kooskõlas jõuda ka USA ametiasutuste valdusesse. Selline võimalus on sätestatud adekvaatsusotsuse 2016/1250 2. lisa II lisa I osa punktis 5 ning PS täiendavate põhimõtete punktis 16.[174] Nimelt võivad ettevõtted *Privacy Shield* põhimõtetest kõrvale kalduda riikliku julgeoleku, avaliku huvi või õiguskaitseliste vajaduste täitmiseks vajalikus

[173] Rakendusotsuse 2016/1250 preambuli punktid 30-37
[174] Rakendusotsus 2016/1250, lk 49 ning lk 66-67

ulatuses.[175] *Privacy Shield* dokumentidest nähtuvalt kohalduvad nimetatud erandid siis, kui vastav ametiasutus esitab isikuandmeid töötlevale ettevõttele vastava korralduse ning sisuliselt tähendab see töödeldavate isikuandmete üleandmist korralduse teinud ametiasutusele.[176] „Riikliku julgeoleku" vajaduse täitmiseks saab korralduse esitada USA riiklikusse luurekogukonda kuuluv asutus[177], avaliku huvi vajaduse täitmiseks tsiviilvaldkondade ja reguleerivad asutused[178] ning õiguskaitseliste vajaduste täitmiseks riigiprokurörid ja föderaalsed uurimisasutused ning õigusmõistmisega seotud asutused (näitekst FBI, vandemeeste kogud, kohtud, föderaalsed kriminaalmenetluse asutused jne).[179]

Luurekogukonda puututavatel kinnitustel lasub eriline tähelepanu, sest 2013. aastal kinnitas Komisjon, et *Safe Harbor* programmi raames edastatud isikuandmed võivad valimatult ning vastuolus EL-i andmekaitse põhimõtetele sattuda USA luureasutuste kätte.[180] Selle teadmise valguses oli eriti oluline asjaolu, et USA õigus välistas isikutele, kes ei ole USA kodanikud või seaduslikud residendid kaitsemeetmed luureasutuste poolse privaatsusõiguse rikkumise vastu.[181] Eelnev oli ühtlasi ka üks põhjendustest, mida EK *Safe Harbor* programmi puudutava adekvaatsusotsuse tühistamisel kasutas.[182]

Kui meenutada Edward Snowden'i 2013. aasta paljastusi, siis pälvisid enim tähelepanu USA luureasutuste kaks jälgimisprogrammi - PRISM ja *Upstream*.[183] Esimest kasutati USA ettevõtete valduses oleva internetiliikluse (k.a. isikuandmed) saamiseks ning teine oli programm, mille raames luureametkonnad kogusid internetiliiklust otse allikast ehk ookeaneid läbivatest optilistest kaablitest.[184] EK *Schrems*'i otsuses ja Komisjoni 2013. aasta teatistes[185] käsitleti luureametite tegevust *Safe Harbor* ettevõtetelt isikuandmete saamisel ehk sisuliselt PRISM programmi rakendamist USA-s, *Upstream* programmi ei käsitletud. Seda autori arvates ka õigustatult, sest *Safe Harbor* programmi (ja ka *Privacy Shield* programmi) põhisisu peitub erasektori poolse isikuandmete töötlemisele standardite seadmisel ning riikliku luure või spionaaži korraldamine kuulub riigi suveräänsus- ja enesekaitse õiguse alla.

---

[175] *Ibid*
[176] Rakendusotsuse 2016/1250 lisa VI ja lisa VII
[177] Rakendusotsuse 2016/1250 lisa VI, lk 91
[178] Rakendusotsuse 2016/1250 lisa VII, lk 209
[179] *Ibid*, lk 111
[180] Euroopa Komisjoni teatis COM(2013) 846 final punkt 2
[181] Euroopa Komisjoni teatis COM(2013) 847 final punkt 7.2.
[182] EK otsus C-362/14, *Schrems* punkt 90
[183] C. Timberg; *NSA slide shows surveillance of undersea cables*; 10.07.2013; The Washington Post; kättesaadav: https://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html (30.03.2017)
[184] Free Snowden; *Surveillance programs*; kättesaadav: https://edwardsnowden.com/surveillance-programs/ (30.03.2017)
[185] Euroopa Komisjoni teatised COM(2013) 846 final ja COM(2013) 847 final

Privacy Shield dokumentides sisalduv Riikliku luurejuhi ameti õigusnõuniku kinnitused vajavad seega erilist tähelepanu, sest kõigest kolm aastat varem puudusid USA õigusest aktid, mis oleks kohustanud ametiasutusi välismaalaste privaatsusõigust austama.

EK rõhutas otsuses C-362/14 *Schrems* juba korduvalt kohtu praktikas kinnitust leidnud seisukohta, et õigusakt, millega kaasneb sekkumine isiku privaatsus ja andmekaitseõigusesse peab sisaldama „… selgeid ja täpseid õigusnorme, mis reguleerivad meetme ulatust ja kohaldamist ning millega on kehtestatud miinimumnõuded, nii et isikutel, kelle isikuandmed on asjassepuutuvad, on piisavad tagatised, mis võimaldavad nende andmeid tõhusalt kaitsta kuritarvitamise ohu ning ebaseadusliku juurdepääsu ja käsitamise eest.“[186] Ning lisas, et eelkõige nõuab eraelu puutumatuse põhiõiguse kaitse, et isikuandmete kaitse erandid ja piirangud piirduksid rangelt vajalikuga.[187] Kuna *Privacy Shield* põhimõtted, nagu ka *Safe Harbor* raamistik enne seda, võimaldavad andmesubjekti põhiõigusesse sekkumist, on *Privacy Shield* programmi koostamisel püütud EK juhiseid silmas pidada. Luurekogukonda esindava õigusnõuniku kinnituste alusel on Komisjon leidnud, et riikliku julgeoleku erandi rakendumisel on Euroopa Kohtu eelnimetatud kriteeriumid USA õiguskorras tagatud.

Riikliku luurejuhi ameti kinnitused on sisuliselt selgitused kolme USA õigusakti – vastuluure ja jälitustegevuse seadus (edaspidi „FISA“), USA Vabaduse Seadus (USA Freedom Act) ja PPD-28 – rakendamisest ning nende pakutavast kaitsest eurooplaste isikuandmete luureametite poolsele töötlemisele. Kuigi luurejuhi amet ei tunnista ega välista *Upstream* programmi laadsete luureprogrammide kasutamist riikliku luure teostamisel, kinnitab luurejuhi ameti õigusnõunik, et kogu luuretegevus, isegi kui see hõlmab selliseid meetodeid, juhindub nimetatud aktidest.[188]

Kui esimesed kaks nimetatut on USA kongressi, kui USA kõrgeima seadusandliku organi[189] poolt vastu võetud õigusaktid, siis PPD-28 on president Barack Obama poliitikasuunis 2014. aastast ehk USA kõrgeima täidesaatva võimu ametniku ja riigipea poolt antud täidesaatva võimu organite tegevust kujundav akt.[190] Arvestades seadusandliku organi aktide esmasust täidesaatva organi analoogide ees[191] ja samas PPD-28 olulisemalt suuremat rolli FISA ja USA *Freedom Act*’i ees riikliku luurejuhi ameti kinnitustes *Privacy Shield* dokumentides, on oluline

[186] EK otsus asjas C-362/14, *Schrems* punkt 91
[187] *Ibid* punkt 92
[188] Rakendusotsuse 2016/1250 lk 92
[189] USA konstitutsioon artikkel 1 lõige 8
[190] T. Moe ja W. Howell; *The Presidential Power of Unilateral Action*; Aprill 1999; Journal of Law, Economics & Organization, Vol 15, Nr 1; lk 133
[191] V. Chu ja T. Garvey; *Executive Orders: Issuance, Modification and Revocation*; Aprill 2014; USA Kongressi uuringute teenistus; lk 1-2

käesoleva alapeatüki kontekstis täpsemalt analüüsida PPD-28 õiguslikku järjepidavust USA uue administratsiooni valguses.

2.1.1.1. PPD-28 roll *Privacy Shield* programmis

PPD-28 sätestab põhimõtted, mis kohalduvad kogu USA luureasutuste signaalluurele ning kõikide inimeste isikuandmete suhtes, sõltumata nende rahvusest või asukohast.[192]

Näiteks sätestab PPD-28, et signaalluuret võib teostada vaid statuudi, korralduse või presidendi muu direktiivi alusel ja kooskõlas seaduste ja konstitutsiooniga[193], signaalluure teostamisel on privaatsus- ja põhiõiguslikud kaalutlused alati arvestatud[194] ning signaalluure peab alati olema teostatud niivõrd kohandataval kujul kui võimalik ja nii kogutud andmeid saab kasutada vaid kindlatel eesmärkidel.[195]

Signaalluure teel kogutud andmete kasutamine on PPD-28 kohaselt võimalik vaid piiratud juhtudel riikliku ning liitlaste huvides, julgeoleku tagamise ja rahvusvahelise kuritegevuse tõkestamise eesmärkidel.[196]

Eraldi sisaldab PPD-28 personaalse informatsiooni kaitsmisele pühendatud paragrahvi, mis sätestab kohustuse signaalluure teostajatele järgida andmete kvaliteedi, minimeerimise, andmete turvalisuse ja juurdepääsu põhimõtteid.[197]

Seega on PPD-28-l väga oluline roll USA riiklike luureasutuste signaalluure tegevusele piiride seadmisel. Kusjuures, tegemist on ainukese õigusliku instrumendiga USA õiguses, mis luuretegevusele, lähtudes muu hulgas andmesubjektide põhiõigustest, ulatuslikke piiranguid seab.

EK on pidanud liidu õigusega vastuolus olevaks õigusakte, mis võimaldavad andmesubjektide vastu korraldatavat piiranguteta signaalluuret ehk massandmekogumist[198], seega näib PPD-28 roll luurejuhi ameti kinnitustes olevat demonstreerida, et USA õiguses tagab PPD-28 signaalluure rakendamise vaid rangelt vajalikus ulatuses. Enne PPD-28 rakendamist võimaldas USA õiguskord sinna Euroopast edastatud isikuandmetele juurdepääsu USA ametiasutustele

[192] PPD-28, lk 1
[193] PPD-28 artikkel 1(a)
[194] PPD-28 artikkel 1(b)
[195] PPD-28 artikkel 1(d)
[196] PPD-28 artikkel 2
[197] PPD-28 paragrahv 4
[198] EK otsus liidetud kohtuasjades C-293/12 ja C-594/12 *Digital Rights Ireland*

ulatuses, mis oli suurem, kui otseselt vajalik ja proportsionaalne riikliku julgeoleku kaitsmise eesmärgist lähtudes.[199]

Käesoleva töö autori eesmärk ei ole seada kahtluse alla Komisjoni järeldust PPD-28 poolt pakutavate tagatiste vastavuse kohta EL-i andmekaitseõiguses ettenähtule ehk vastata küsimusele, kas PPD-28 tagab signaalluure rakendatavuse vaid rangelt vajalikus määras. Nagu ülal märgitud, lähtub autor eeldusest, et rakendusotsus 2016/1250 oli selle vastuvõtmise hetkel vastavuses EL-i õigusega. Samas puudub rakendusotsuse dokumentides analüüs USA presidendi poliitikasuunitluste õigusliku tähenduse kohta, mis on rakendusotsuse 2016/1250 järjepidevuse seisukohast oluline, eriti võttes arvesse, et otsuse preambuli punktis 69 kinnitab Komisjon, et PPD-28 on USA luureasutustele siduv, kuid lisab, et PPD-28 „… jääb kehtima kuni USA valitsuse vahetumiseni.“[200]

Tänaseks on USA-l uus president ning valitsus. Seega on üleskerkinud küsimus PPD-28 õigusliku tähenduse kohta uue administratsiooni kontekstis. Selleks vaatleb autor järgnevalt USA presidentide seadusandliku aktide õiguslikku tähendust.

2.1.1.2. Presidentaalsed seadusandlikud aktid USA õiguses

USA konstitutsiooni artikkel 2 loetleb USA presidendi volitused. Näiteks nimetab see artikkel üldistatult, et presidendile kuuluvad täidesaatva võimu volitused.[201] Seadusandlike aktide andmist selles artiklis nimetatud ei ole. Sellegipoolest on vägagi tavaline, et USA presidendid väljastavad erinevaid presidentaalseid akte, millel on riigi täidesaatva võimu ametnikele ja organitele siduv tähendus. Praktikas on presidendi selline tegevus, olgu siis täidesaatvate korralduste (*executive order*), memorandumite (*presidentaal memorandum*) või direktiivide (*presidentaal directive*) kaudu, aktsepteeritud ning sisuliselt on sellisena võimaldatud USA presidendile piiratud seadusandlik võim, mille ulatus võib praktikas olla üpriski lai.[202]

Kuna president rakendab konstitutsiooni kohaselt kogu täidesaatvat võimu, peab tal olema võimu teostamiseks võimalus anda administratsioonile juhiseid oma poliitika elluviimiseks.[203] Samas on rõhutatud, et president ei saa rakendada neid akte valdkondades, mis konstitutsiooni

[199] Komisjoni teatis COM(2013) 847 final punkt 7.1.
[200] Rakendusotsus 2016/1250 lk 14
[201] USA Konstitutsioon artikkel 2(1), kättesaadav: https://www.law.cornell.edu/constitution/articleii (01.04.2017)
[202] T. Moe ja W. Howell, lk 133
[203] *Ibid*, lk 138

kohaselt talle ei kuulu või kuuluvad kongressile või kohtule.[204] Presidentaalsed aktid, mis lähevad seadusega vastuollu, ei oma algusest peale mingit õiguslikku jõudu.[205]

Tähtsaimaks ja tugevaima õigusjõuga presidentaalseks aktiks peetake täidesaatvaid korraldusi – nad meenutavad vormilt seadusi ja on ametnikele kohustuslikud ning kohalduvad otse, kohe alates avaldamisest.[206] Presidentaalsed poliitikasuunised, nagu ka PPD-28, omavad täidesaatvate korraldustega samaväärset õiguslikku jõudu.[207]

Kuna presidentaalsete aktide väljaandmine käib lahutamatult USA presidendi õiguse juurde oma poliitikat kujundada, ei saa need aktid olla ka kuigi stabiilsed. Iga president võib vabalt oma korraldusi muuta, kehtetuks tunnistada, teiste aktidega asendada ning sama teha ka oma eelkäijate presidentaalsete aktidega.[208] Seega on vägagi päevakorras ka küsimus PPD-28 staatusest president Donald Trumpi valitsusajal, eriti arvestades tema senist praktikat president Obama presidentaalsete aktide kehtetuks tunnistamisel ning nendega vastuolulise poliitika rakendamisel.[209]

2.1.1.3. PPD-28 õiguslik tähendus tänases USA-s

PPD-28 omab *Privacy Shield* dokumentides kahtlemata olulist rolli. Kui meenutada *Shcrems*'i lahendit, oli rakendusotsuse 2000/520/EÜ tühistamise peamiseks põhjuseks asjaolu, et *Safe Harbor* programmi põhimõtetega kooskõlas võisid edastatud isikuandmed vastutava töötleja käest jõuda USA ametiasutuste kätte, kuid Komisjon ei olnud rakendusotsuse vastuvõtmisel analüüsinud sellisel juhul USA ametiasutustele kohalduvaid isikuandmete töötlemise reegleid.[210] Muu hulgas leidis kohus, et tegelikult USA õiguskord, mis lubab piiranguteta signaalluuret teostada välisriiki andmesubjektide suhtes, ei taga EL-iga võrdväärset isikuandmete kaitset, sest USA õiguskord võimaldas sekkumist andmesubjektide eraellu ulatuses, mis ületas rangelt vajalikku.[211] PPD-28 roll peakski olema sätestada piirangud signaalluure kasutamisele, et luureasutustele oleks võimaldatud signaalluure teostamine vaid ulatuses, mis on rangelt vajalik riigi julgeoleku eesmärkide saavutamiseks.

---

[204] V. Chu ja T. Garvey, lk 1
[205] *Ibid*
[206] *Ibid*
[207] USA justiitsministeeriumi õigusbüroo seisukoht *Legal effectiveness of presidentaal directive, as compared to an executive order*; 29.01.2000; kättesaadav: https://fas.org/irp/offdocs/predirective.html (01.02.2017)
[208] V. Chu ja T. Garvey, lk 7
[209] Valge Maja; *Presidential Executive Order on the Revocation of Federal Contracting Executive Orders*; 27.03.2017 – tegemist on täidesaatva korraldusega, millega president Trumpi tunnistati kehtetuks kolm president Obama korraldust
[210] EK otsus asjas C-362/14 *Schrems*, p 87-88
[211] *Ibid*, p 91

Direktiiv 95/46 artikkel 25(6) kohaselt võib kolmas riik tagada isikuandmete piisava kaitsetaseme endale võetud rahvusvaheliste kohustustega või oma siseriikliku õigusega. Kui tulla tagasi *Privacy Shield* programmi struktuuri juurde, nähtub programmi esimesest osast (*Privacy Shield* põhimõtted ning DoC poolt antud kinnitused), et peamiselt on artikkel 25(6) mõttes tegemist USA rahvusvaheliste kohustustega, mis tagavad isikuandmete kaitse piisava taseme. Programmi teine osa aga koosneb USA ametkondade kinnitustest selle kohta, et USA õiguskord sätestab konkreetsed piirangud ja õigused olukorras, kus ametiasutus töötleb andmesubjektide (k.a. välismaallastest andmesubjektide) isikuandmeid avalikes huvides, riikliku julgeoleku kaalutlustel või õiguskaitselistel vajadustel. Seega on sisuliselt ka Komisjoni rakendusotsusest võimalik tuvastada kaks eritasandit: ühel juhul hindab Komisjon kas *Privacy Shield* põhimõtted ja nende tagamise kinnitused DoC poolt on USA ametivõimude poolt võetud piisavad isikuandmete kaitset pakkuvad rahvusvahelised kohustused; ja teisel juhul, kas USA õiguskord, mis käsitleb avalikes huvides ja riikliku julgeoleku eesmärkidel isikuandmete töötlemist, pakub EL-i õigusega samaväärset kaitset samaväärsetes olukordades.

EK ütles *Shcrems*'i lahendis, et kolmanda riigi siseriiklik õigus tagab isikuandmete piisava kaitsetaseme, kui see on sisuliselt samaväärne sellele, mis on tagatud EL-is.[212] Lisaks on Kohus Euroopa Liidu õiguse kontekstis öelnud, et põhiõiguste kaitse nõuab, et isikuandmete kaitse erandite ja piirangute puhul tuleb piirduda rangelt vajalikuga ning lisanud, et selle nõude täitmiseks peab õigusakt, mis võimaldab sekkumist isiku põhiõigustesse, sätestama piisavate tagatiste olemasoluks selged ja täpsed reeglid meetmete ulatuse ja kohaldamise kohta ning kehtestama miinimumnõuded.[213]

USA elektroonilise välisluure õiguslikuks aluseks on FISA[214], mis on USA Kongressi vastuvõetud seadus. PPD-28 on õigusakt, mis USA õiguses seab piirangud signaalluurele selliselt, et luureasutuste poolt teostatav tegevus, mis sekkub julgeoleku kaalutlustel andmesubjektide andmekaitseõigusesse, piirduks vaid rangelt vajalikuga (annab juhised FISA rakendamiseks, selliselt et luureasutused järgiksid signaalluure teostamisel rangelt vajalikkuse põhimõtet).

Seega nähtub siit autori arvates tähelepanuväärne ebakõla, sest õigusakt, mis seab signaalluurele olulised piirangud ja teeb USA luurasutuste signaalluure teostamise Komisjoni hinnangul EL-i õiguse lähtekohast vastuvõetavaks, on normihierarhiliselt oluliselt nõrgem

[212] EK otsus asjas C-362/14 *Schrems*, p 73
[213] EK otsus liidetud kohtuasjades C-293/12 ja C-594/12 *Digital Rights Ireland*, p-52-54
[214] Rakendusotsuse 2016/1250 Lisa IV, lk 98; U.S. Code § 1802(a)(1), kättesaadav: https://www.law.cornell.edu/uscode/text/50/1802 (03.04.2017)

õigusaktist, mis signaalluuret võimaldab. Arvestades PPD-28 kui presidentaalse seadusandliku akti õiguslikku tähendust USA õiguses, nähtub et tegemist on õigusaktiga, mille jätkuv kohaldamine uue administratsiooni võimu ajal on sisuliselt uue presidendi poliitiline otsus. Samas ei ole presidentaalsetel seadusandlikel aktidel siduvat tähendust ka selle väljastanud presidendile endale, sest poliitikasuunised võivad nii maailma, kui ka sisepoliitilistest sündmustest lähtuvalt muutuda. Seega on USA õiguses isiku andmekaitseliste õiguste tagamine luureasutuste poolt tagatud normihierarhiliselt väga nõrga õigusliku instrumendiga, samal ajal kui EL-is on samad õigused isikule tagatud põhiõigusena, ELPH-s sätestatuna ja seega osana EL-i primaarõigusest.

Euroopa Kohtu sõnul peab isikuõiguste riivet võimaldav EL-i õigusakt sätestama ka piirangud, mis tagavad sekkumise vaid rangelt vajalikus ulatuses. Seega nähtub kohtupraktikast, et riivet piiravad sätted peavad omama vähemalt võrdväärset õiguslikku jõudu sätetega, mis riivet võimaldavad. See tingimus ei ole täidetud USA õiguses signaalluuret võimaldava ning sellele piiranguid seadvate õigusaktide vahel.

Kuna PPD-28 jätkuv kehtivus on piltlikult öeldes USA uue administratsiooni kätes, peab Komisjon edaspidi tegema olulisi samme selleks, et saada Trumpi administratsioonilt selge kinnitus PPD-28 reeglite jätkuva järgmise kohta. Kuid edaspidise õiguskindluse kaalutlusel on siiski oluline, et PPD-28 leiaks USA õiguses kinnistamist seadusandliku võimu poolt vastuvõetud seadusena.

2.1.1.4. Eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon (PCLOB) ja *Privacy Shield* ombudsman

Direktiivi 95/46 artikkel 28 kohaselt näeb iga liikmesriik ette ühe või mitu riigiasutust, et teostada järelevalvet direktiivi sätete kohaldamise üle. Otsuses C-362/14 *Schrems* märkis EK, et eelotsust küsinud Iiri kohus tuvastas *Safe Harbor*'i puudujäägina asjaolu, et USA-s teostatakse järelevalvet luureteenistuste tegevuse üle salastatud menetluses, mis ei ole võistlev ning liidu kodanikel ei ole mingit tegelikku õigust olla ära kuulatud.[215]

Direktiivi artiklist 28 nähtuvalt peab järelevalve asutus olema riigiasutus (täidesaatva võimu organ), mis on oma ülesannete täitmisel täiesti sõltumatu. Sellisel asutusel peavad olema uurimisvolitused, sekkumisvolitused ning kohustus menetleda andmesubjektide avaldusi.

[215] EK otsus asjas C-362/14 *Schrems*, p 31

Privacy Shield programmis rõhutatakse luuretegevuse mitmekülgset järelevalvet.[216] Täidesaatva võimu tasandil teostavad järelevalvet mitmed Riikliku luurejuhi ameti haldusala ametnikud ja organid[217], otse presidendi haldusalas töötav Eraelu puutumatuse ja kodaniku vabaduste järelevalve komisjon (edaspidi „PCLOB“)[218] ning PPD-28 alusel spetsiaalselt *Privacy Shield* programmi tarbeks eurooplaste avalduste menetlemiseks loodud ombudsman.[219]

Artikkel 28 kriteeriumeid ei rahulda esimesena nimetatud järelevalve instants, sest puudub täieliku sõltumatus – kontroll toimub nende samade organite sees, mis luuretegevust teostavad. PCLOB ja ombudsman koosvaadatuna võiks neid kriteeriume rahuldada. PCLOB on luureasutustest eraldiseisev, täitevvõimu osaks olev sõltumatu organ, mille seitsmeliikmelise koosseisu määrab ametisse president senati heakskiidul.[220] PCLOB ülesandeks on järelevalve teostamine USA täidesaatva võimu tegevuse üle, mida teostatakse riikliku julgeoleku huvides eesmärgiga tagada isikute privaatsus- ja põhiõiguste kaitse.[221] *Privacy Shield* dokumentidest ning PCLOB enda poolt avaldatud informatsioonist nähtuvalt on PCLOB-l laialdased uurimisvolitused, kuid asjaomastest allikatest nähtuvalt puuduvad komisjonil sekkumisvolitused. Sekkumisvolitusi saab pidada kaudseteks, sest PCLOB koostab raporteid ning teavitab uurimistel selgunud mittevastavustest senati vastavaid komisjone, ministeeriumeid ja muid täidesaatvavõimu kõrgemaid organeid, kellel sekkumisõigus on olemas.[222]

Privacy Shiled ombudsmani kohustusi täidab USA riigisekretäri otseses haldusalas tegutsev rahvusvahelise infotehnoloogiaalase diplomaatia vanemkoordinaator (*Senior Coordinator for International Information Technology Diplomacy*). See ametikoht loodi PPD-28 alusel kontaktisikuks välisriikide valitsuste jaoks, mis tunnevad muret USA signaalluurealase tegevuse kohta.[223] *Privacy Shield* ombudsmani ülesannetega vanemkoordinaator on ametiisik, kes menetleb ja uurib andmesubjektide kaebusi USA luuretegevuse suhtes.[224]

Uue administratsiooni kontekstis ei pea aga *Privacy Shield* dokumentides antud kinnitused PCLOB ja ombudsmani järelevalve tegevuse kohta paika. Nimelt on USA Riigidepartemangu

[216] Rakendusotsus 2016/1250 punkt 95, lisa VI lk 96, lisa III lisa A lk 72
[217] Riikliku luurejuhi ameti kinnituste kohaselt teostab iga luureühendusse kuuluv organ ise järelevalvet ning ka riikliku luurejuhi ameti enda juures töötab vastav büroo
[218] Rakendusotsus 2016/1250 lisa VI lk 96
[219] Ombudsmani mehhanismi sätestab rakendusotsuse 2016/1250 lisa III lisa A
[220] Rakendusotsus 2016/1250, punkt 98;
[221] Privacy and Civil Liberties Oversight Board; *about the Board*; kättesaadav: https://www.pclob.gov/about-us.html (08.04.2017)
[222] Rakendusotsus 2016/1250 punktid 99-102
[223] PPD-28 paragrahv 4d
[224] Rakendusotsus 2016/1250 punkt 117

juures tegutseva ning ombudsmani kohustusti täitva ametiisiku positsioon käesoleva töö koostamise seisuga täitmata kolm kuud.[225] Ka PCLOB liikmete arv ei ole seitse, nagu väidab Rakendusotsuse 2016/1250 punkt 98, vaid kuni jaanuarini 2017 oli neid neli ning alates veebruarist vaid üks.[226] Seega on ka PCLOB poolsete ülesannete kohane täitmine suure küsimärgi all nagu ka *Privacy Shield* programmi poolt pakutav piisav andmekaitse tase.

Kuna ombudsmani kohuseid täitev ametikoht Riigidepartemangu juures on loodud PPD-28 alusel, kohaldub ka siin eelmises alapeatükis PPD-28 kohta järeldatu.

Eelnevast tulenevalt on *Privacy Shield* programmi raames USA ametiasutuste poolt antud kinnitustest rakendusotsuse 2016/1250 järjepidevuse tagamiseks oluline, et uus administratsioon teeks täiendavaid ning eelneva administratsiooni seisukohti kinnitavaid avaldusi. Kuna ombudsmani positsioon on hetkel tühi ning PCLOB komisjon samuti oluliselt kärbitud, peaks Komisjoni esmane prioriteet eelseisvatel *Privacy Shield* programmi kohase ülevaatuse raames olema nimetatud institutsioonide vastavusse saamine *Privacy Shield* dokumentidega.

2.1.2. President Trumpi 25. jaanuari täidesaatev korraldus ja selle mõju *Privacy Shield'*ile

Pärast ametivande andmist 20. veebruaril 2017[227], alustas president Trump tormiliselt oma poliitika elluviimist, kuulutades välja oma ametiaja esimese kümne nädalaga üle seitsmekümne presidentaalse akti, nende hulgas 23 täidesaatvat korraldust.[228]

Kindlasti kõige enam tekitas kõneainet tema 27. jaanuari täidesaatev korraldus[229], millega peatati sisseränne teatud moslemienamusega riikidest.[230] Andmekaitsega seotud ringkondades

[225] USA Riigidepartemang; *Alphabetical List of Bureaus and Offices – Other Senior Officials: Coordinators*; kättesaadav: https://www.state.gov/r/pa/ei/rls/dos/1718.htm?MobileOptOut=1 (01.05.2017)
[226] Privacy and Civil Liberties Oversight Board; *Board Members*; kättesaadav: https://www.pclob.gov/about-us/board.html (09.04.2017)
[227] Valge Maja; *The Inaugural Address*; kättesaadav: https://www.whitehouse.gov/inaugural-address (23.03.2017)
[228] Valge Maja; *Presidential actions*; kättesaadav https://www.whitehouse.gov/briefing-room/presidential-actions (08.04.2017)
[229] Valge Maja; *Executive Order: Protecting the nation from foreign terrorist entry into the United States*; 27.01.2017; kättesaadav: https://www.whitehouse.gov/the-press-office/2017/01/27/executive-order-protecting-nation-foreign-terrorist-entry-united-states (08.04.2017)
[230] A. Yuhas ja M. Sidahmed; *Is this a Muslim ban? Trump's executive order explained*; The Guardian, 31.01.2017; kättesaadav: https://www.theguardian.com/us-news/2017/jan/28/trump-immigration-ban-syria-muslims-reaction-lawsuits (08.04.2017)

saabus kerge paanikalaine aga mõned päevad varem[231], pärast korralduse „Ameerika Ühendriikide sisese avaliku turvalisuse suurendamine“ avaldamist.[232]

Kuigi nimetatud korraldus on peamiselt suunatud ebaseadusliku immigratsiooni tõkestamisele, sisaldab see ka paragrahvi 14, mis mõne asjatundja sõnul seab kahtluse alla õigusraamistiku *Privacy Shield* kehtivuse. Paragrahv 14 sätestab kõigile USA täidesaatva võimu asutustele korralduse jätta kohaldamata välismaallaste suhtes USA *Privaacy Act*-ist tulenevad tagatised.

Paanikalaine sai alguse Euroopa Parlamendi kodanikuvabaduste, justiits- ja siseasjade komisjoni aseesimehe Jan Phillipp Albrechti[233] sotsiaalmeedia Twitter kontol avaldatud säutsust, milles parlamendiliige kuulutas, et paragrahv 14 tõttu tuleks koheselt *Privacy Shield* raamistiku alusel isikuandmete edastamine lõpetada ning USA suhtes sanktsioone rakendada.[234]

Jan Albrechti tähelepaneku järel mitmete ajakirjanike ühispöördumise peale kinnitas Euroopa Komisjoni esindaja, et Komisjon on teadlik Trumpi täidesaatvast korraldusest, kuid ei näe selles vastuolu *Privacy Shield* programmiga, sest *Privacy Act*'il ei ole programmiga puutumust.[235]

Nagu peatükis 1.2.2. mainitud pakub *Privacy Act* kaitset föderaalsete ametiasutuste valduses olevatele isikute andmetele, võimaldades andmesubjektidel nende privaatsusõiguste rikkumisel riigiasutustest andmetöötleja vastu esitada kohtule kahju hüvitamise ning isikuõiguste rikkumistest hoidumise nõudeid. Seega, juhindudes ELPH artiklist 47 ning Euroopa Kohtu otsuse C-362/14 *Schrems* punktist 95, tuleks tõepoolest järeldada, et juhul kui Presidendi 25. jaanuari täidesaatev korraldus välistab eurooplaste isikuandmete kaitse õiguse kohtute poolse kaitse, tuleb rakendusotsus 2016/1250 kehtetuks tunnistada, sest *Privacy Shield* võimaldab teatud olukordades USA riigiasutustele ligipääsu edastatud isikuandmetele.

Tegelikkuses ei ole *Privacy Act Privacy Shield* programmiga üldsegi seotud. Õigused, mida *Privacy Act* USA andmesubjektidele tagab, on *Privacy Shield* programmis samaväärselt tagatud

---

[231] M. Burgess; *New presidential order could wreck US-EU Privacy Shield*; Wired, 27.02.2017; kättesaadav: http://www.wired.co.uk/article/trump-privacy-shield-data (08.04.2017)

[232] Valge Maja; *Executive Order: Enhancing Public Saftey in the Interior of the United States*, 25.01.2017; kättesaadav: https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united (08.04.2017)

[233] Euroopa Parlament; *Parlamendiliikmed – Jan Philipp Albert*; kättesaadav: http://www.europarl.europa.eu/meps/et/96736/JAN+PHILIPP_ALBRECHT_home.html (08.04.2017)

[234] J. P. Albert; 26.01.2017 säuts; Twitter; kättesaadav: https://twitter.com/JanAlbrecht/status/824553962678390784?ref_src=twsrc%5Etfw&ref_url=http%3A%2F%2Fwww.wired.co.uk%2Farticle%2Ftrump-privacy-shield-data (08.04.2017)

[235] N. Lomas; *Trump order strips privacy rights from non-U.S. citizens, could nix EU-US data flows*; TechCrunch, 26.01.2017; kättesaadav: https://techcrunch.com/2017/01/26/trump-order-strips-privacy-rights-from-non-u-s-citizens-could-nix-eu-us-data-flows/ (08.04.2017); L. Kayali; 26.01.2017 säuts; Twitter; kättesaadav: https://twitter.com/LauKaya/status/824674537803550721 (08.04.2017)

õigusaktidega FISA, *Computer Fraud and Abuse Act, Electronic Communications Privacy Act, Right to Financial Privacy Act, Freedom of Information Act, Wiretap Act, Federal Torts Claim Act* ja *Fair Credit Reporting Act*.[236] Nende seaduste järgi on õigustatud isikuteks kõik kahjustatud isikud, hoolimata nende kodakondsusest ja asukohast.[237] Seega tuleb nõustuda Komisjoniga ning Euroopa Parlamendi liikme Albrecht hinnang jätta tähelepanuta.

Pealegi, kui meelespidada presidentaalsete täidesaatvate korralduste õiguslikku mõju, selgub, et presidentaalsed korraldused ei kuulu kohaldamisele ulatuses, mis läheb vastuollu mõne Kongressi poolt kehtestatud seadusega. Siinkohal omab tähtsust peatükis 1.2.2.1. käsitletud JRA, mille kohaselt siiski laienevad *Privacy Act*'i sätted teatud välisriigi kodanikele. Euroopa Liidust pärit isikud kuuluvad *Privacy Act* on kaetud JRA artikkel 2(d)(1)(A) ja 2(d)(1)(B) alusel.

2.1.3. Vahekokkuvõte

Käesoleva peatüki eesmärgiks oli kaardistada ning tähelepanu suunata olulistele USA-st tulenevatele asjaoludele, mis pärast rakendusotsuse 2016/1250 vastuvõtmist on aset leidnud ning millel võib olla oluline mõju *Privacy Shield* programmi järjepidevale toimimisele. USA-st tulenevatest muutustest on kindlasti olulisim uue presidendi ja administratsiooni ametisse astumine jaanuaris 2017. Kuna *Privacy Shield* programmi kinnitas eelmine administratsioon ning programmis on läbivalt oluline roll USA ametiasutuste poolsetel kinnitustel, mille paikapidavus uue administratsiooni ajal ei ole autori arvates iseenesestmõistetav, on oluline saada USA uuelt administratsioonilt täiendavaid kinnitusi *Privacy Shield* programmiga antud lubadustest kinnipidamise kohta.

Arvestades PPD-28 õiguslikku tähendust presidentaalse direktiivina ning selle üliolulist rolli USA luureasutuste poolt teostatava signaalluure piiramisel ja seega ka *Privacy Shield* programmi kehtivuse tagamisel, võib olla oluline vähemalt täiendavate kinnituste saamine USA uuelt administratsioonilt PPD-28 jätkuva rakendamise kohta. Sellised täiendavad kinnitused võiksid *Privacy Shield* programmis olla esitatud näiteks USA rahvusvaheliste kohustustena EL-i ees. Kui PPD-28 sätted oleksid lisatud *Privacy Shield* programmi sellisena, et Komisjon saaks hinnata neid kui USA rahvusvahelisi kohustusi, mitte osana USA õigussüsteemist, oleks adekvaatsusotsuses võimalik võtta seisukoht, mille kohaselt Komisjon möönaks, et USA luuretegevusele kohalduv õigus küll ei taga isikuandmete kaitse taset EL-iga samaväärselt, kuid

[236] Rakendusotsus 2016/1250 lisa VI, lk 102-103 ja lisa VII, lk 32
[237] *Ibid*

koos *Privacy Shield* programmis sisalduvate kinnitustega saab kaitse taset siiski piisavaks lugeda.

Sellegipoolest, õiguskindluse mõttes oleks tähtis leida võimalus, et PPD-28-s sätestatud reeglid leiaksid kajastamist ka USA seadustes, sest rahvusvahelise kohustusena PPD-28 reeglite sätestamine *Privacy Shield* programmis vajaks ka järelevalve mehhanismide kohaldamist, mis võib osutuda keeruliseks, arvestades luureasutuste tegevuse rolli riigi suveräänsusõiguse teostamisel.

Lisaks on USA uus administratsioon jätnud täitmata *Privacy Shield* programmi tähenduses olulised luureasutuste üle järelevalvet teostavad ametikohad – PCLOB komisjonis on tänase seisuga vaid üks liige, mitte seitse, nagu kinnitatud *Privacy Shield* dokumentides ning täitmata on *Privacy Shield* ombudsmani positsioon.

2.2. *Privacy Shield* programmi põhimõtete vastavus GDPR-ile

Algavas alapeatükis käsitleb autor *Privacy Shield* programmi tuumiku, ehk raamistikuga liitunud ettevõtjatele kohustuslike isikuandmete töötlemise põhimõtete ühilduvust 2018. aasta kevadel rakenduvate GDPR-i põhimõtetega ning soovib identifitseerida selles lähtuvalt puudujäägid *Privacy Shield* programmi põhimõtetes.

GDPR vahetab välja direktiivi 95/46[238] ja seega muutub ka adekvaatsusotsuste alus. Direktiivis 95/46 on adekvaatsusotsuste õiguslik alus artikkel 25(6), mille kohaselt võib komisjon vastava otsusega tunnistada kolmanda riigi andmekaitse taseme artikli 25(2) tähenduses piisavaks. GDPR-is annab adekvaatsusotsuste tegemiseks Komisjonile volituse artikkel 44(3), kui hinnatav riik, territoorium või rahvusvaheline organisatsioon tagab piisava kaitse taseme artikli 44(2) tähenduses. Eelduslikult tähendab uus andmekaitse reeglistik vajadust ümberhinnata ka kõik varasemad adekvaatsusotsused lähtudes GDPR-is toodud õiguslikust alusest. Sama kehtib ka rakendusotsuse 2016/1250 suhtes.

Käesolevas peatükis lähtub autor peamiselt eeldusest, et rakendusotsus 2016/1250 on kooskõlas liidu õigusega, ehk *Privacy Shield* raamistik tagab isikuandmete kaitse tasemel, mis on sisuliselt samaväärne EL-i andmekaitse tasemega. Käesolevas alapeatükis kätkeb see eeldus endas ka usaldust USA vastavate ametiasutuste tegevuse suhtes programmis antud kinnitustest kinnipidamise osas. Seega ka eeldust, et *Privacy Shield* programmi ametlikul kodulehel

[238] GDPR artikkel 94(1)

avaldatud nimekirjas olevate ettevõtete[239] isikuandmete töötlemine on kooskõlas PS põhimõtetega.

Selline eeldus võimaldab autoril PS põhimõtete GDPR-ile vastavuse analüüsimisel tugineda ning tuua näiteid *Privacy Shield* ettevõtete poolt *Privacy Shield* programmi alusel vastuvõetud ja avaldatud privaatsus- ja teenusetingimustest. Näidete toomisel tugineb autor konkreetsemalt Google Inc.[240] poolt avaldatud Google'i teenusetingimustele[241] ja privaatsuseeskirjadele[242] ning Facebook Inc.[243] poolt avaldatud *Privacy Shield* programmiga liitumise teatisele[244], töötlemise põhimõtetele[245] ja teenusetingimustele. [246]

Nimetatud ettevõtteid on kasutatud näidetena, sest tegemist on rahvusvahelises digitaalmajanduses oluliste töötlejatega. Lisaks on andmetöötlejatel Facebook ja Google EL-i andmekaitseõiguses märgiline tähendus kohtu asjade *Schrems* ja *Google Spain* tõttu ning seega omab nende andmetöötlusreeglite analüüsimine käesolevas töös ka sümboolset tähendust.

Facebookil on Euroopas tütarfirma Facebook Ireland Ltd, kellega sõlmivad andmesubjektid Facebook'i teenuste kasutamisel vastava lepingu ja mis asub Iirimaal.[247] Kuna Facebook Ireland edastab kõik kasutajate isikuandmed kas täielikult või osaliselt Facebook Inc.-ile[248], käsitleb autor Facebook'i puudutavate näidete puhul eeldusest, nagu isikuandmed edastataks otse USA Facebookile.

Sarnasest eeldusest lähtub autor ka Google Inc. teenuste osutamise analüüsimisel. Kuna iga Google'i teenuse kasutaja nõustub Google Inc. tingimustega, tekib tal suhe otse USA-s asuva Google Inc.-ga ning seega lähtub autor ka siin eeldusest, et isikuandmete edastamine toimub otse USA-sse.[249]

---

[239] *Privacy Shield* programmiga liitunud ettevõtete nimekiri USA Kaubandusministeeriumi hallataval veebilehel https://www.privacyshield.gov/list (12.04.2017)
[240] Google Inc. *Privacy Shield* programmiga liitumise kinnitus, kättesaadav: https://www.privacyshield.gov/participant?id=a2zt000000001L5AAI&status=Active (19.04.2017)
[241] Google Inc., *Google'i teenusetingimused*; kättesaadav: https://www.google.ee/intl/et/policies/terms/regional.html (19.04.2017)
[242] Google Inc., *Privaatsuseeskirjad*; kättesaadav: https://www.google.ee/intl/et/policies/privacy/ (19.04.2017)
[243] Facebook Inc. *Privacy Shield* programmiga liitumise kinnitus, kättesaadav: https://www.privacyshield.gov/participant?id=a2zt0000000GnywAAC&status=Active (12.04.2017)
[244] Facebook Inc. *Facebook Inc. and the EU-U.S. Privacy Shield*, kättesaadav: https://www.facebook.com/about/privacyshield (19.04.2017)
[245] Facebook; *Data Policy*; kättesaadav: https://www.facebook.com/policy.php (12.04.2017)
[246] Facebook; *Statement of Rights and Resposibilities*; kättesaadav: https://www.facebook.com/legal/terms (12.04.2017)
[247] Facebook Inc. *Facebook Inc. and the EU-U.S. Privacy Shield*
[248] EK otsus asjas C-362/14 *Schrems*, punkt 27
[249] Google'i teenusetingimused

2.2.1. Töötlemise põhimõtted

Selleks, et *Privacy Shield* programm oleks GDPR-iga vastavuses, peaksid kummagi sätestatud põhimõtted ning neist andmesubjektidele tulenevad õigused olema sisuliselt samaväärsed, et tagatud oleks piisav isikuandmete kaitse tase pärast GDPR-i rakendumist. Selle kontrolli läbiviimiseks on autor jaganud analüüsi viieks osaks lähtuvalt GDPR-is sisalduvatest üldistest andmekaitse põhimõtetest. GDPR-i III peatükis sätestatud andmesubjekti õigused on kategoriseeritud vastava põhimõtte alla ning analüüsitud PS põhimõtete valguses. Autor tõdeb, et GDPR-is sätestatud andmesubjekti õigused võivad kuuluda korraga mitme põhimõtte alla ning all toodud liigitus ei ole kindlasti ainuvõimalik. Käesolevas peatükis on liigitamise eesmärgiks luua vastavale GDPR-i andmekaitse põhimõttele piirid, et oleks võimalik PS põhimõtteid neile kõrvutada ning kompaktselt välja selgitada nende põhimõtete üksteisele vastavus.

PS põhimõtted on nimetatud rakendusotsuse 2016/1250 2. lisa II lisas väljaantuna USA DoC poolt. Programmis on loetletud 7 põhimõtet, millele lisanduvad 16 PS täiendavat põhimõtet. PS täiendavad põhimõtted on PS põhimõtete suhtes toetavad ning suurem osa neist ei oma järgneva analüüsi seisukohast tähtsust.

PS põhimõtetes on eraldi välja toodud definitsioonid mõistetele „isikuandmed“, „töötlemine“ ja „vastutav töötleja“.[250] *Safe Harbor* põhimõtetes neid eraldi ei deklareeritud. Kõik kolm mõistet vastavad direktiivis 95/46 artiklile 2. GDPR selles osas ei erine direktiivist. Isikuandmete definitsioon on küll pisut täpsem, nimetades eraldi asukohateabe, võrguidentifikaatorid, isiku füüsilised, geneetilised, vaimsed, majanduslikud, kultuurilised ja sotsiaalsed tunnused[251] isikuandmetena, kuid sisuliselt kätkevad nimetatud ka direktiivis ja seega ka PS põhimõtetes. PS põhimõtetest leiab ka tundlike andmete definitsiooni[252], mis vastab GDPR artikkel 9(1) toodud eriliiki isikuandmetele. Definitsioonide lisamine PS põhimõtete hulka on kindlasti oluline, sest see tagab siin ja sealpool Atlandit teostatavatele töötlemistele ühtse raamistiku, eriti arvestades, et USA õiguses sellised klassifikatsioonid puuduvad.

Kui proovida identifitseerida *Privacy Shield* programmi alusel toimuva isikuandmete edastamise ketis vastutavad töötlejad, volitatud töötlejad ja muud GDPR artiklis 4 nimetatud isikud, on autori arvates võimalik tuvastada vähemalt kolm olukorda.

[250] Rakendusotsus 2016/1250 lisa 2 II lisa, punkt 8; lk 49
[251] GDPR artikkel 4(1)
[252] Rakendusotsus 2016/1250 lisa 2 II lisa; *täiendavad põhimõtted – Tundlikud andmed*; lk 52

Esiteks edastamine EL-is asuva vastutava töötleja poolt, USA-s asuvale volitatud töötlejale. Põhimõtteliselt oleks tegu olukorraga, kus vastutav töötleja on kogunud hulga isikuandmeid ja saadab need kokkuleppe alusel USA-sse töötlemiseks, kuid töötlemise eesmärgid on paika pandud vastutava töötleja poolt. Sellisel juhul võib vastutavaks töötlejaks olla ka EL-i andmesubjekt ise. Näiteks olukord, kus andesubjekt soovib teha isikuliku veebilehe USA veebimajutusettevõtte juures ning veebimajutaja ei välju töötlemisel andmesubjekti poolt antud juhistest.

Teiseks, olukorrad, kus USA-s võtab isikuandmed vastu vastutav töötleja otse andmesubjektilt, teiselt vastutavalt töötlejalt või volitatud töötlejalt, kes vastutava töötleja jaoks isikuandmeid kogub. Autori hinnangul saab otse andmesubjektilt isikuandmete kogumist käsitleda edastamisena EK otsuse C-101/01 *Lindqvist* valguses. Kuigi nimetatud kohtuasja üks peamisi küsimusi oli, kas isikuandmete avaldamine avalikul veebisaidil, kuhu pääsevad ligi isikud üle Maa, on käsitletav isikuandmete edastamisena kolmandasse riiki, sisaldas see ka analüüsi üksik isiku poolt andmete edastamise kohta serverisse. Kohus käsitles isikuandmete sisestamist veebilehele, edastamisena.[253]

Kolmandaks, eelneva kahe segu, kus USA andmetöötleja on nii vastutav, kui ka volitatud töötleja. Sellised suhted on tavalised, näiteks sotsiaalmeedia teenuse pakkujate ja andmesubjektide vahel. Ühest küljest valib andmesubjekt mida ta oma sotsiaalmeedia kontole üles laeb, ehk milliseid isikuandmeid avalikustab ja selles aspektis on sotsiaalmeedia teenuse pakkuja lihtsalt platvorm, mis töötlemise eesmärkidesse ega vahenditesse ei puutu, näiteks Facebook pakub andmesubjektile platvormi isikuandmete üleslaadimiseks ehk oma profiili koostamiseks – andmesubjekt määrab töötlemise eesmärgid ja vahendid ning seega on ta vastutav töötleja. Teisest küljest võib see sotsiaalmeedia teenuse pakkuja kasutada üleslaetud isikuandmeid iseenda eesmärkidest ja vahenditest lähtuvalt, kui tal on selleks andmesubjekti nõusolek või ta teeb seda lepingust lähtudes.

Selles kontekstis on Facebook küllaltki huvitav nähtus. Facebook'i poolt avaldatud *Privacy Shield* teavituses klassifitseerib Facebook end eranditult volitatud töötlejaks, mis siinkirjutaja hinnangul ei pruugi olla tõene. Ilmselt peitub Facebooki loogika selles, et andmesubjekti nähakse vastutava töötlejana, kellel on absoluutne kontroll oma isikuandmete üle. Tehes postitusi või kasutades muid Facebook'i teenuseid, edastab andmesubjekt küll Facebook'ile isikuandmeid, kuid eesmärgid, milleks neid töödelda saab on andmesubjekt ise oma privaatsusseadmetes paika pannud. Facebook'i privaatsuspoliisi kohaselt kasutab Facebook

[253] EK otsus asjas C-101/01 *Bodil Lindqvist*; p 71

isikuandmeid, mida kasutajatelt kogutud, muu hulgas oma teenuste arendamiseks, parandamiseks ja pakkumiseks.[254] Kasutustingimustes on märgitud, et kõiki andmeid kogutakse andmesubjektidelt nende endi nõusolekul.[255] Arvestades, et nõusolekut saab anda ettepanekule isikuandmeid töödelda mingil eesmärgil ning Facebooki teenuste parandamine ja arendamine ei toimu andmesubjektide poolt ega ole võimalik nende otsesel osalusel, ei saa Facebooki enesemääratlusega, kui isikuandmete volitatud töötleja, kuidagi nõustuda.

2.2.1.1. Töötlemise seaduslikkus, õiglus ja läbipaistvus

Iga õiguspärase isikuandmete töötlusprotsessi eelduseks on kindel seaduses toodud alus. Tegemist on ühtlasi ka ühe olulisema EL-i andmekaitse põhimõttega – töötlemine peab olema seaduslik.[256] GDPR-i kohaselt on seadusliku töötlemise aluseid kuus[257], mis sisuliselt ei erine direktiivis nimetatud alustest. Seega peab ka *Privacy Shield* raamistiku alusel teisel pool Atlandit toimuv isikuandmete töötlemised lähtuma vähemalt ühest neist.

Privacy Shield dokumentides puudub otsene viide töötlemise seaduslikkuse põhimõttele. Arvestades, et *Privacy Shield* programm on ülesseatud direktiivi 95/46 artikkel 26 alusel (GDPR-i puhul artikkel 45(1)) selleks, et isikuandmete edastamisel USA-sse säiliks sihtriigis nende töötlemisel EL-iga samaväärne kaitse, on esmane töötlemistoiming, mis teisel pool Atlandit isikuandmetega toimub, vastuvõtmine, säilitamine või dokumenteerimine või muu taoline toiming. Vastuvõtmine eeldab aga edastamist, mis analüüsitaval juhul saab lähtuda vaid EL-ist.

Iga töötlemise eelduseks on ligipääs vastavatele isikuandmetele ja ligipääsu saab *Privacy Shield* ettevõttele võimaldada vaid EL-i töötleja või andmesubjekt ise. Kui edastaja on töötleja, rakendub temale EL-i andmekaitse reeglistik, mis tagab, et töötlemine toimub õiguspärastel eesmärkidel ja nii kandub töötlemise õiguspärasus edasi USA ettevõttele. Kui isikuandmeid edastab andmesubjekt ise, saab eeldada andmesubjekti ja töötleja vahel mingisugust kokkulepet või vähemalt andmesubjekti nõusolekut tema isikuandmete töötlemiseks, sest isikuandmete edastamine on eelduslikult teadlik tegevus.

Seega on ilmselt kõige asjakohasemad GDPR artiklis 6 nimetatud õiguslikest alustest töötlemine andmesubjekti nõusolekul (GDPR artikkel 6(1a)) ja andmesubjekti osalusel sõlmitud lepingu täitmiseks (GDPR artikkel 6(1b)). GDPR artikkel 6(1c) oleks töötlemise

[254] Facebook; *Data Policy – How do we use thi information?*
[255] Facebook; *Statement of Rights and Resposibilities*
[256] Direktiiv 95/46 artikkel 7; GDPR artikkel 5(1a) ja artikkel 6
[257] GDPR artikkel 6

aluseks näiteks olukorras, kus USA ettevõte saab avalikult organilt korralduse andmete edastamiseks. Sellise korralduse saamisel PS põhimõtted ettevõttele ei kohaldu.[258]

Siiski vajab andmete edastamine otse andmesubjekti poolt töötlemise seaduslikkuse kontekstis pisut põhjalikumat analüüsi. Andmesubjektil, kui andmekaitseõiguse subjektile, ei lasu iseenda isikuandmete töötlemisel, näiteks edastamisel, mingeid kohustusi. Peamiselt seetõttu, et direktiiv 95/46 artikkel 3(2) ja GDPR artikkel 2(2c) kohaselt ei kohaldata andmekaitse reegleid kui füüsiline isik töötleb isikuandmeid eranditult isiklike või koduste tegevuste käigus, kuid ka seetõttu, et iseenda andmete töötlemist, kui aktiivse tegevuse eelduseks on nõusolek. Andmesubjekti nõusoleku alusel (direktiiv artikkel 26(1a) ja GDPR artikkel 49(1a)) isikuandmete edastamise korral *Privacy Shield* ettevõttele, peab ettevõte samuti järgima PS põhimõtteid.[259]

Kui isikuandmeid võtab vastu ehk töötleb *Privacy Shield* ettevõte, on ettevõttel tulenevalt teavitamise põhimõttest kohustus teatada andmesubjekti milliseid isikuandmeid kogutakse ja millistel eesmärkidel neid kogutakse ja kasutatakse.[260] Eesmärgi piiramise põhimõttest tulenevalt peavad kogutud isikuandmed olema piiratud sellega, mis on töötlemise eesmärke arvesse võttes asjakohane ning andmeid ei tohi töödelda viisil, mis ei vasta neile eesmärkidele.[261] Võib argumenteerida, et seaduslikkuse põhimõte on eelviidatud kohustuste täitmisel samuti täidetud, sest alati andmete kogumisel avaldatakse andmesubjektile eesmärgid ja põhjused isikuandmete kogumiseks ja kui andmesubjekt jätkab pärast eesmärkidega tutvumist teenuse kasutamist või isikuandmete edastamist, on töötlemise aluseks andmesubjekti nõusolek (direktiiv 95/46 artikkel 7(a) ja GDPR artikkel 6(1a)). Lisaks, arvestades, et valdavalt on andmetöötlejate poolt pakutavate teenuste kasutamiseks sätestatud kasutustingimused, millega andmesubjekt teenuste kasutamisel nõustub, võib töötlemise aluseks pidada andmesubjekti osalusel sõlmitud lepingu täitmist (direktiiv 95/46 artikkel 7(b) ja GDPR artikkel 6(1b)). Selliste lepingute puhul nähakse tihtipeale andmesubjekti aktseptina andmesubjekti poolt teenuse kasutamist.

Siiski ei vasta eelkirjeldatud nõusolek GDPR-is sätestatud nõusoleku tunnustele. GDPR-kohaselt on nõusolek vabatahtlik, konkreetne, teadlik ja ühemõtteline tahteavaldus, millega andmesubjekt kas avalduse vormis või selget nõusolekut väljendava tegevusega nõustub tema

[258] Rakendusotsus 2016/1250 lisa 2 II lisa, lk 49; *Ibid; Täiendavad põhimõtted – Juurdepääsutaotlused riigiasutuste poolt*; lk 66-67
[259] Rakendusotsus 2016/1250 preambuli punkt 16, lk 4
[260] Rakendusotsus 2016/1250 lisa 2 II lisa; *Põhimõtted – teade*; punktid iii ja iv; lk 49-50
[261] Rakendusotsus 2016/1250 lisa 2 II lisa; *Põhimõtted – andmete terviklikkus ja eesmärgi piiramine*; punkt a; lk 51

kohta käivate isikuandmete töötlemisega.[262] Nõusoleku vabatahtlikkuse hindamisel tuleb võtta arvesse, kas teenuse osutamise tingimuseks on nende isikuandmete töötlemiseks nõusoleku andmine, mida teenuse osutamiseks või lepingu täitmiseks vaja ei lähe.[263] Lisaks kohustab GDPR töötlejaid vajadusel tõendama, et andmesubjekt on töötlemisega nõustunud.[264] Alla 16-aastase lapse nõusolek on kehtiv vaid siis, kui lapse esindaja on sellega päri.[265] Lisaks on positiveeritud andmesubjekti õigus võtta oma nõusolek igal ajal tagasi.[266]

Privacy Shield programm ei täpsusta sisuliselt mõistet „nõusolek". Kasutatud on termineid „selgesõnaline nõusolek" (*opt in*)[267] ja „valik" (*opt out*)[268], kuid eraldi ei ole sätestatud, kriteeriumeid, millele õiguspärane nõusolek peaks vastama, et selle alusel isikuandmete töötlemine toimuda saaks. Veelgi enam, PS põhimõtete kohaselt peavad andmetöötlejad võimaldama andmesubjektidele võimaluse loobuda (*opt out*) isikuandmete kolmandatele isikutele avaldamisest ning isikuandmete kasutamisest eesmärkidel, mis on erinevad sellest, milleks neid algselt kasutatakse ehk vaikimisi eeldatakse selleks andmesubjekti nõusolekut.[269]

Eelnevast nähtuvalt on PS põhimõtetega kooskõlas olukord, kus ettevõte avaldab andmesubjektile nimekirja kogutavatest isikuandmetest ning hulga eesmärke, milleks neid kogutakse ja töödeldakse ning kui andmesubjekt alustab teenuse kasutamist, annab ta justkui nõusoleku kõikide väljatoodud isikuandete töötlemiseks väljatoodud eesmärkidel. Lähtudes EK otsusest liidetud kohtuasjades C-92/09 ja C-93/09 *Volker und Markus Schecke GbR* leiab autor, et sellistes olukordades isikuandmete töötlemine ei toimu andmesubjekti nõusoleku alusel, sest kõigest isikuandmete töötlemise eesmärkidest teavitamine ei loo automaatselt võimalust järeldada andmesubjekti nõustumist, kui pärast teavitamist alustab andmesubjekt vastava teenuse kasutamist.[270] Eriti, kui kogutavad isikuandmed ning töötlemise eesmärgid on andmesubjektile esitatud kogumis ning nõustumine on teenuse kasutamise eelduseks.

Eelkirjeldatud lähenemine on nähtav ka Google Inc. teenuse- ja privaatsustingimustest. Google'i teenuste puhul kogub Google isikuandmeid tihtipeale otse andmesubjektilt, tavaliselt andmesubjekti ja Google Inc. vahel sõlmitud lepingu alusel ja selle täitmiseks ning teenuse

[262] GDPR artikkel 4(11)
[263] GDPR artikkel 7(4)
[264] GDPR artikkel 7(1)
[265] GDPR artikkel 8
[266] GDPR artikkel 7(3)
[267] Rakendusotsuse 2016/1250 lisa 2 II lisa; *Põhimõtted – valikuvõimalus*; punkt c, lk 50
[268] Rakendusotsuse 2016/1250 lisa 2 II lisa; *Põhimõtted – valikuvõimalus*; punkt a, lk 50
[269] *Ibid*
[270] EK otsus liidetud kohtuasjades C-92/09 ja C-93/09 *Volker und Markus Schecke GbR, Hartmunt Eifert v Land Hessen*; p 61-64

osutamise eeldusena.[271] See leping, üldnimetusega teenusetingimused, kohaldub ka siis, kui andmesubjekt lihtsalt kasutab mõnda Google'i teenust, ilma kasutajana sisse logimata. Teenusetingimustest nähtuvalt eeldab Google andmesubjekti nõustumist teenusetingimustega, sealhulgas privaatsuseeskirjadega.[272] Privaatsuseeskirjades on üldsõnaliselt loetletud isikuandmete grupid, mida Google kasutab ning eesmärgid, milleks andmeid kogutakse.[273] Arvestades, et mõned nimetatud eesmärkidest ei puutu otseselt andmesubjekti, vaid teenindavad Google Inc. huvisid, näiteks teenuste täiustamine ja uute teenuste arendamine, on Google Inc töödeldavate isikuandmete suhtes vastutav töötleja, kelle poolne töötlemine ei eelda andmesubjekti konkreetset, vabatahtlikku ja teadlikku nõusolekut. Teenuste täiustamine ega uute teenuste arendamine ei ole ka eesmärgid, mille saavutamiseks Google'i poolne isikuandmete töötlemine on vajalik andmesubjektiga sõlmitud lepingu täitmiseks, kui lugeda teenusetingimusi poolte vaheliseks lepinguks, olukorras kus andmesubjekt kasutab näiteks Google Maps rakendust.

Eelnevast nähtuvalt ei pruugi PS põhimõtete alusel isikuandmete töötlemise korral olla alati tagatud GDPR-iga samaväärne isikuandmete kaitse seadusliku töötlemise põhimõttele nõrga esindatuse tõttu. Probleeme tekitab tõsiasi, et PS põhimõtetes ei ole eraldi sätestatud ammendatud nimekirja tingimustest, mis on eelduslikud õiguspärasele isikuandmete töötlemisele, nagu on GDPR-i artiklis 6(1). Lisaks puudub eraldi termini „nõusolek" määratlus, mis vastaks GDPR-is sätestatule ning nõusolekuna nähakse nii loobumist (*opt-out*), valimist (*opt-in*), kui ka sõnaselget nõusolekut.

Samas tõusetub eelneva põhjal ka õigustatud küsimus, kas PS põhimõtted on üldsegi kooskõlas kehtiva EL-i andmekaitse tasemega, sest sisuliselt ei lisa seaduslikkuse põhimõttele ega õiguspärase nõusoleku tingimustele GDPR võrreldes direktiivis 95/46 sätestatule kuigi palju sisulist juurde. Kuna see küsimus langeb väljapoole käesoleva töö ulatust, hoidub autor sellel põhjalikumalt vastamisest.

Õiguspärane töötlemine toimub läbipaistvalt. Läbipaistvuse tagamiseks on GDPR-is sätestatud andmetöötlejatele kohustus esitada andmesubjektile töötlemise kohta teavet aga teavitama andmesubjekti ka tema seadusest tulenevatest õigustest.[274] Läbipaistvuse põhimõte eeldab, et andmesubjektile on lihtsalt kättesaadav kogu tema isikuandmete töötlemisega seotud teave.[275]

[271] Google teenusetingimused ja privaatsuseeskirjad
[272] Google'i teenusetingimused – *Tere tulemast Google'isse!* ja *Privaatsus ja autoriõiguste kaitse*
[273] Google'i privaatsuseeskirjad – *Teave, mida kogume* ja *Kuidas kasutame kogutud teavet*
[274] GDPR artikkel 12(1)
[275] GDPR põhjenduse p 39

Kuna andmekaitse tagab sisuliselt isiku õigust informatsioonilisele enesemääratlusele[276], peab tal olema võimalik säilitada kontroll informatsiooni ja andmete üle, mida andmetöötlejad subjektid tema kohta omavad. See on ka eelduseks, et andmesubjekt saaks oma andmekaitse õigusest tulenevaid konkreetseid nõudeõigusi rakendada, sest kui isik ei tea, kes tema andmeid töötleb ja milliseid tema andmeid töödeldakse, pole tal võimalik ka kontrolli teostada ega õigusi maksma panna.[277]

Autor eristab GDPR-is läbipaistvust tagavatest õigustest andmesubjekti õiguse saada ning töötleja kohustuse anda teatavat informatsioon töötlemise ja töötleja kohta[278] ning andmesubjekti õiguse tutvuda isikuandmetega, mis on töötleja käes.[279] Lisaks on läbipaistvuse põhimõtte garandina võimalik käsitleda artiklist 19 tulenevat nõuet, et andmetöötleja teavitab andmesubjekti tema isikuandmete parandamise, kustutamise või töötlemise piiramise kohta.

PS põhimõtetes on läbipaistvus tagatud kahe põhimõtte kaudu – teade[280] ja juurdepääs.[281] Teate põhimõttel on *Privacy Shield* raamistikus lisaks läbipaistvusele ka teine eesmärk – oma tegevuse USA FTC või Transpordiministeeriumi järelevalvele allutamine. USA ettevõte peab andmesubjekti teavitama näiteks sellest, et ta järgib PS põhimõtteid ning ta tunnustab USA täidesaatva võimu volitusi uurimise läbiviimiseks ja sunni rakendamiseks.[282] Mäletavasti muudab USA õiguse kohaselt tarbijale nimetatud asjaolude deklareerimine PS põhimõtted talle kohustuslikuks ja annab täidesaatva võimu organitele õiguse tema suhtes järelevalvet teostada.

GDPR-is on konkreetne teave, mida vastutav andmetöötleja andmesubjektile edastama peab, mitmekesisem võrreldes PS põhimõtetes sätestatust. Näiteks on GDPR-i kohaselt töötleja kohustuseks avaldada ajavahemik, mille jooksul isikuandmeid säilitatakse või selle ajavahemiku määramise kriteeriumid[283]. PS põhimõtetes on küll sätestatud töötleja kohustus reeglina mitte säilitada kauem kui see on andmete kogumise eesmärkide täitmiseks vajalik,[284] kuid säilitamise perioodi kohta teavet andmesubjektile esitada ei ole kohustuslik. Lisaks on GDPR-i kohaselt vajalik teavitada mõningatest konkreetsetest elementidest ja nende rakendamisest, mida *Privacy Shield* programmi andmetöötlejatele programmiga ettenähtud ei

[276] E. Tikk ja A. Nõmper; lk 37
[277] EK otsus asjas C-553/07 *College van burgemeester ne wethounders van Rotterdam v M. E. E. Rijkeboer* p 51-57
[278] GDPR artiklid 13 ja 14
[279] GDPR artikkel 15
[280] Rakendusotsus 2016/1250 lisa 2 II lisa; *Põhimõtted – teade*; lk 49-50
[281] *Ibid*; lk 51-52
[282] *Ibid*, punktid i, iii, x
[283] GDPR artikkel 13(2a)
[284] Rakendusotsus 2016/1250; lisa 2 II lisa; *Põhimõtted – andmete terviklikkus ja eesmärgi piiramine*; punkt b, lk 51

ole – näiteks andmekaitseametniku kontaktandmed ja profiilianalüüsi puudutav info.[285] Kuna need elemendid on pigem uued ka EL-i andmekaitseõigusele, analüüsib autor neid eraldi allpool.

Osa teabest, mida *Privacy Shield* ettevõte andmesubjektile esitama peab, tuleneb konkreetselt sellest, et tegemist on *Privacy Shield* programmi alusel andmete töötlejaga – näiteks informatsioon vahekohtule, mis lahendab andmesubjekti ja andmetöötleja vahel tekkivaid vaidlusi, mis puudutavad PS põhimõtete täitmist.[286] GDPR-i puudub sellise teabe avaldamiseks vajadus, sest vaidluste lahendamisega tegeleb vastava liikmesriigi kohus.

GDPR artikkel 15 kohaselt on andmesubjektil õigus nõuda vastutavalt töötlejalt kinnitust tema andmete töötlemise kohta ning tutvumist nende andmetega. PS põhimõtetes on selline õigus tagatud juurdepääsu põhimõttega[287], mille osana on sätestatud ka andmesubjekti õigus nõuda parandamist, muutmist või kustutamist, kui andmed on ebatäpsed või neid on töödeldud vastuolus PS põhimõtetega.

Seega on eelnevast analüüsist nähtav, et PS põhimõtted on vastavuses GDPR-i läbipaistvuse põhimõttega. Ettevõttele, kes PS põhimõtetega eurooplaste isikuandmeid töötleb, on ettenähtud laialdane teavitamise kohustus, mis tagab töötlemise läbipaistvuse samaväärselt EL-i andmekaitseõigusega GDPR-i rakendumise ajal. Lisaks on põhimõtetesse lisatud täiendav osa teavitamise kohustusest, mis on oluline USA õiguse seisukohast, et vastavad järelevalve asutused saaksid järelevalvet teostada.

2.2.1.2. Eesmärgipärane töötlemine ja eesmärk kui töötlemist piirav element

GDPR-i artiklis 1 on sätestatud kolm põhimõtet, mis autori hinnangul on sisuliselt võimalik kokku võtta ühe põhimõttena – eesmärgipärasuse põhimõte. Määruses on need sätestatud kui eesmärgi piirangu põhimõte[288], võimalikult väheste andmete kogumise põhimõte[289] ehk minimeerimise põhimõte ja õigsuse põhimõte.[290] Kõik nimetatud deklareerivad andmetöötleja kohustust isikuandmete töötlemisel mitte väljuda eesmärkidest, milleks andmed algselt koguti ja tunnustavad andmesubjekti õigust isikuandmete kogumise eesmärgi vastu eksiva töötlemise keelamist nõuda. Kokkuvõtlikult võiks seda põhimõtet väljendada järgmiselt: Isikuandmeid

[285] GDPR artikkel 13(1b), 13(2f), 14(1b) ja 14(2g)
[286] Rakendusotsus 2016/1250 lisa 2 II lisa; *Põhimõtted – teade*; punktid ix, xi; lk 50
[287] Rakendusotsus 2016/1250 lisa 2 II lisa; *Põhimõtted – juurdepääs*, lk 51
[288] GDPR artikkel 5(1b)
[289] GDPR artikkel 5(1c)
[290] GDPR artikkel 5(1d)

võib koguda ja töödelda vaid täpselt ja selgelt kindlaksmääratud ning õiguspäraste eesmärkide saavutamise ulatuses ning neid ei töödelda hiljem viisil, mis on nende eesmärkidega vastuolus. Sellest tuleneb ka otseselt kohustus hoida isikuandmed õiged ja ajakohastatud ning rakendada meetmeid, mis tagaksid eesmärgi seisukohast ebaõigete isikuandmete kustutamise ja parandamise (ehk õigsuse põhimõte).

Eesmärgipärasuse põhimõtte tagamiseks on GDPR-is sätestatud andmesubjektile õigus nõuda andmete parandamist (artikkel 16), kustutamist (artikkel 17) ning isikuandmete töötlemise piiramist (artikkel 18).

PS põhimõtetes on eesmärgipärasuse põhimõte esindatud andmete terviklikkuse ja eesmärgi piiramise põhimõttes ning juurdepääsu põhimõttes. Neist nähtuvalt peavad töödeldavad isikuandmed olema piiratud ulatusele, mille eesmärgiks need koguti või milleks isik hiljem loa andis. Eesmärkidest lähtuvalt peab töötleja võtma mõistlike meetmeid tegemaks et isikuandmed on kavatsetud kasutamiseks usaldusväärsed, täpsed, täielikud ja ajakohased.[291] Juurdepääsu põhimõte kohustab töötlejat andma andmesubjektile võimalus andmeid parandada, muuta ja kustutada, kui need on ebatäpsed või neid on töödeldud vastuolus põhimõtetega.[292] PS täiendavate põhimõtetega on sätestatud eraldi tingimused, kuidas juurdepääsu põhimõtet rakendama peaks.[293]

PS põhimõtetes on andmete parandamise, kustutamise, muutmise ja andmetega tutvumise õigus sätestatud ühe põhimõtte all sellisena, et töötlejal on õigus keelduda kõigi nimetatud alustel esitatud nõuete täitmistest samadel alustel. Esiteks on sätestatud, et nimetatud nõudeid saab andmesubjekt esitada, kui tema isikuandmed on ebatäpsed või neid on töödeldud vastuolus PS põhimõtetega. Juurdepääsu võimaldamisest võib keelduda, kui see on ebaproportsionaalselt tülikas või kulukas või kui juurdepääs rikuks teiste isikute õigusi. Tülikus ja kulukus on olulised tegurid, mida tuleks arvesse võtta vaid siis, kui need ei ole otsustavad tegurid juurdepääsu võimaldamise mõistlikkuse üle otsustamisel.[294]

Selline väljendusviis PS põhimõtetes ei vasta GDPR-is sätestatule seetõttu, et vastavad andmesubjekti õigused on määruses sätestatud eraldi ning ka andmetöötlejatele on ettenähtud erinevad võimalused vastavatest nõuetest keeldumiseks. Näiteks andmete parandamise õigus peaks olema sätestatud universaalselt, ehk olukorras, kus andmesubjekt saab teada, et tema

[291] Rakendusotsus 2016/1250 lisa 2 II lisa; *Põhimõtted – andmete terviklikkus ja eesmärgi piiramine*; punkt a; lk 51
[292] Rakendusotsus 2016/1250 lisa 2 II lisa; *Põhimõtted – juurdepääs*; lk 52
[293] Rakendusotsus 2016/1250 lisa 2 II lisa; *Täiendavad põhimõtted – juurdepääs*; lk 57
[294] Rakendusotsus 2016/1250 lisa 2 II lisa; *Põhimõtted – juurdepääs; lk 52*

isikuandmed, mis on töötleja valduses, on ebaõiged, peaks töötleja andmesubjekti nõudmise korral andmeid parandama tingimusteta.

PS täiendavates põhimõtetes on pühendatud mitme leheküljeline osa juurdepääsu põhimõtte rakendamisele, kuid sealt nähtuvalt käsitletakse peamiselt vaid isiku õigust oma andmetega tutvumiseks ehk täiendavates põhimõtetes on juurdepääsu põhimõttel PS üldistes põhimõtetes sätestatust kitsam tähendus. Selles mõttes on GDPR artiklist 15 tulenev andmesubjekti õigus oma andmetega tutvuda samaväärne PS põhimõtetes ja PS täiendavates põhimõtetes sätestatuga, kuid parandamise, kustutamise ja töötlemise piiramise õigus on jäänud laiemalt avamata.

Selline ebatäpsus võib tipneda andmetöötlejate poolt andmesubjektide esitatud kustutamise, parandamise ja töötlemise piiramise nõuete täitmisest keeldumisega alustel, mis GDPR-i kohaselt on keeldumise aluseks vaid juurdepääsu nõude täitmisest.

Google'i privaatsustingimustes nähtubki, et Google jätab endale õiguse vale teabe muutmisest või kustutamisest keeldumiseks, kui teabe valel kujul säilitamiseks on ettevõttel „seaduslikud ärilised või õiguslikud" eesmärgid.[295] Kuna Google Inc. on USA äriühing, ei ole andmesubjektidele ettenähtav, millised nimetatud seaduslikud ärilised ja õiguslikud eesmärgid olla võivad. Veelgi enam, seaduslikud ärilised eesmärgid võivad osutuda äärmiselt laiaks määratluseks, näiteks võiks selle alla liigitada ettevõtlusvabaduse vms õigused. Autori hinnangul on EL-i andmekaitseõigusest ja täpsemalt GDPR artiklist 16 tulenev õigus valede isikuandmete parandamiseks kategooriline andmesubjekti õigus, mille tunnustamata jätmine võib andmesubjektile kaasa tuua olulist kahju, kuna mõjutab oluliselt isiku enesemääratlusõigust ja võib soodustada näiteks laimu levitamist.

GDPR artiklis 17 sätestatud õigus andmete kustutamisele on oluline täiendus EL-i andmekaitseõiguse positiivses õiguses, mis osati on deklareeritud määruses just võrgukeskkonnas toimuvat isikuandmete töötlemist silmas pidades,[296] seda tüüpi töötlemine *Privacy Shield* programmi puhul on küllaltki asjakohane.

PS põhimõtete kohaselt on andmesubjektil õigus nõuda kustutamist siis, kui andmed on ebatäpsed või neid on töödeldud PS põhimõtetega vastuolus. Nagu nähtus käesoleva töö alapeatükist 2.2.1.1.1 on teatud juhtudel võimalik, et *Privacy Shield* ettevõte töötleb andmesubjekti isikuandmeid ilma seadusliku aluseta. Kui selline töötlemine lähtub isikuandmete kogumise eesmärkidest, ei ole võimalik andmesubjektil seega nõuda andmete

[295] Google'i privaatsuseeskirjad – *Juurdepääs isiklikule teabele ja selle värskendamine*
[296] GDPR preambuli punkt 66

kustutamist, nagu GDPR-i artikkel 17(1d) seda võimaldab. Kuna PS põhimõtted ei käsitle eraldi lapse isikuandmete töötlemist, ei ole võimalik isikuandmete kustutamist nõuda, kui lapse esindaja seda nõuab, nagu võimaldab GDPR artikkel 17(1f). Seega ei võimalda PS põhimõtted andmesubjektile GDPR-is sätestatuga võrdväärset isikuandmete kustutamise õigust.

GDPR artikkel 18 kohaselt on andmesubjektil õigus teatud õigustatud huvi olukordades nõuda töötlejalt isikuandmete töötlemise piiramist. Näiteks isikuandmete õigsuse vaidlustamise korral võib andmesubjekt nõuda töötlemise piiramist, kuniks vaidlustus on lahendatud, ka võib ta nõuda, et töötleja ei kustuta andmeid kui töötleja neid enam töötlemise eesmärkide täimiseks ei vaja, kui subjektil on neid andmeid vaja õigusnõude koostamiseks, esitamiseks või kaitsmiseks jne.[297] Selline nõudeõigus ei ole PS põhimõtete osaks.

2.2.1.3. Säilitamise piiramise põhimõte

Säilitamise piiramise põhimõte kohaselt säilitatakse isikuandmeid kujul, mis võimaldab andmesubjekti tuvastada vaid seni, kuni see on vajalik eesmärgi täitmiseks, milleks isikuandmeid töödeldakse.[298] GDPR-i preambulis on selle põhimõtte sisustamiseks muu hulgas märgitud, et selle põhimõtte tagamiseks peaks vastutav töötleja kindlaks määrama tähtajad andmete kustutamiseks või perioodiliseks läbivaatamiseks.[299]

GDPR artikkel 25(2) kohaselt peab säilitamise piiramise põhimõtte tagamiseks vastutav töötleja rakendama asjakohaseid tehnilisi ja korralduslike meetmeid.

PS põhimõtetes on nimetatud põhimõte deklareeritud sisuliselt samaväärselt GDPR-iga – isikuandmeid võib säilitada kujul, mis identifitseerib või võimaldab andmesubjekti identifitseerida ainult nii kaua kuni see on vajalik töötlemiseks isikuandmete kogumise eesmärkidest lähtuvalt.[300] Samaväärselt on sätestatud ka erandid mille puhul võib nimetatud põhimõttest teha kõrvalekaldeid: pikem säilitamine on võimalik avalikust huvist lähtudes, näiteks ajakirjanduslikel, kunsti- või teaduseesmärkidel.

GDPR-i preambulis nimetatud nõue määratud tähtaegade tagant andmeid kustutada või läbi vaadata näib kaudselt olevat kaetud PS täiendavates põhimõtetes sätestatud kontrollimise kohustusega.[301] Nimelt peavad PS ettevõtted ette nägema kontrollimeetmed, et tõendada PS

[297] GDPR artikkel 18
[298] GDPR artikkel 6(1e)
[299] GDPR preambul punkt 39
[300] Rakendusotsus 2016/1250; lisa 2 II lisa; *Põhimõtted – andmete terviklikkus ja eesmärgi piiramine*; punkt b, lk 51
[301] Rakendusotsus 2016/1250 lisa 2 II lisa; *Täiendavad põhimõtted – kontrollimine*; lk 56-57

põhimõtetega kooskõlas olevate ja andmesubjektidele avaldatud töötlemistavadest kinnipidamist kinnipidamist, need kontrollimeetmed peaksid olema rakendatud enesehindamistena või välise kontrolli kaudu. Kui ettevõte rakendab enesekontrolli, peab ta perioodiliselt teostama objektiivsest kontrolli. Objektiivse ehk välise kontrolli puhul kontrollitakse samuti vastavust PS põhimõtetele ja seega ka kohustust säilitada isikuandmeid identifitseeritaval kujul vaid nii kaua kuni see on vajalik töötlemiseks isikuandmete kogumise eesmärkidest lähtuvalt. Seega peaksid perioodilised välised ja objektiivsed kontrollid tagama ka isikuandmete säilitamise piiramise põhimõttest kinni pidamise ehk vajadusel mitte asjakohaste isikuandmete kustutamise.

2.2.1.4. Turvalisuse põhimõte

Isikuandmeid töödeldakse viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kaotamise, hävitamise või kahjustamise eest, kasutades asjakohaseid tehnilisi või korralduslike meetmeid.[302] PS põhimõtetes sisaldub turvalisuse põhimõtte definitsioon on sisuliselt samaväärne eeltooduga GDPR-ist, mis annab turvalisuse põhimõtte üldtähenduse. Lisaks on GDPR-is sätestatud turvalisuse põhimõtet täpsustav säte, mis on konkreetsem võrreldes direktiivi artikliga 17 ja ka PS põhimõtete turvalisuse põhimõttega.

Turvalisuse põhimõtet avab GDPR-i artikkel 32, tuues välja avatud nimekirja konkreetsetest meetmetest, mida turvalisuse tagamiseks vastutav töötleja vastavalt vajadusele peaks rakendama. Näiteks on nimetatud isikuandmete krüpteerimise ja pseudonümiseerimise meede ja tehniliste ja korralduslike meetmete tõhususe korrapärasuse testimine ja hindamine töötlemise turvalisuse tagamiseks.[303]

GDPR artikkel 32 on olemuselt pigem nõuandva funktsiooniga säte, millest otseseid kohustusi vastutavale töötlejale välja lugeda ei saa. Oluline, mida turvalisuse põhimõte GDPR-is ette näeb, on kohustus suhtuda isikuandmete töötlemisse hoolsusega ja rakendada praktikas, olenevalt isikuandmete töötlemise asjaoludest, piisavaid abinõusid, et isikuandmed ei satuks pahatahtlike kolmandate isikute töötlemise objektiks ning vältida vastutava töötleja hooletusest tingitud töötlemist (nt tahtmatu kustutamine, kadumine jne). Selles osas on PS põhimõtetes ja GDPR-is sätestatu vahel kattuvus olemas.

[302] GDPR artikkel 5(1f)
[303] GDPR artikkel 32(1a) ja 32(1d)

2.2.1.5. Andmesubjekti kontroll oma andmete üle

Kuna andmesubjekti kontroll oma isikuandmete üle on isiku informatsioonilise enesemääratlusõiguse olulisem element, peaks PS põhimõtted ning GDPR sisuliselt samaväärse isikuandme kaitse taseme korral pakkuma andmesubjektile võrdväärselt õigusi oma isikuandmete üle kontrolli teostamiseks. Jättes kõrvale andmesubjekti õiguse tutvuda oma andmetega, neid kustutada , parandada ja töötlemist piirata, mida autor juba eelpool käsitlenud, on GDPR-is sätestatud andmesubjekti õigus isikuandmeid üle kanda.[304]

Andmete ülekandmise õigus annab andmesubjektile võimaluse saada vastutavalt töötlejalt teda puudutavad isikuandmed struktureeritud, üldkasutatavas vormingus ning masinaloetaval kujul ning need andmed teisele vastutavale töötlejale edasi anda, ilma, et vastutav töötleja andmesubjekti takistada saaks. Selle õiguse kasutamise eelduseks on, et isikuandmeid üleandev vastutav töötleja töötleb andmeid andmesubjekti nõusoleku või lepingu alusel ning töötlemine toimub automatiseeritult.[305] Siia juurde käib ka andmesubjekti õigus nõuda andmete ülekandmist otse uuele vastutavale töötlejale.[306]

Tegemist on õigusega, mis on EL-i andmekaitseõiguses täiesti uus. Kuna see õigus annab andmesubjektile sõnaõiguse, kes ja kui kaua tema isikuandmeid töötleb, suurendab see oluliselt andmesubjekti informatsioonilist enesemääratlusõigust.[307]

Lisaks võib sellel uuel põhimõttel olla oluline mõju digitaalmajandusse üldiselt, sest andmesubjektid ei ole enam „lõksus“ ühe teenusepakkuja juures, vaid nad saavad vabalt oma isikuandmetega liikuda teenusepakkujate vahet. Nii ei piirdu andmete ülekandmise õiguse positiivne mõju ainult andmekaitseõigusele, vaid soodustab ka konkurentsi teenusepakkujate vahel.[308]

PS põhimõtetest loomulikult andemete ülekandmise õigusele sarnast õigust ei leia, mis omab otsest ja olulist mõju PS põhimõtete poolt pakutavale andmekaitse tasemele, kui seda võrrelda GDPR-i omaga. Kuna nimetatud õigusel on oluline mõju isiku informatsioonilisele enesemääratlemise õigusele ehk andmekaitse olulisemale põhiõiguslikule eesmärgile[309], on

[304] GDPR artikkel 20
[305] GDPR artikkel 20(1)
[306] GDPR artikkel 20(2)
[307] E. Fialova; *Data Portability and Informational Self-Determination*; Masaryk University Journal of law and Technology; 2014, vol 8(1); lk 47
[308] B. Engels; *Data portability among online platforms*; Internet Policy Review; 2016, vol 5(2); lk 14
[309] *Ibid*, lk 50

pärast GDPR-i rakendamist kevadel 2018 isikuandmete ülekandmise õigus eelduseks igale õiguskorrale, mida GDPR-i artikkel 45 alusel piisava andmekaitse taseme valguses hinnatakse.

Oluline täiendus GDPR-is võrreldes varasema andmekaitse reeglistikuga, mis samuti suurendab isiku kontrolli oma isikuandmete üle on „profiilianalüüsi" defineerimine ning andmesubjekti õiguste kasutamise selgitamine profiilianalüüsi kontekstis.

GDPR artikkel 4(4) kohaselt on profiilianalüüs igasugune isikuandmete automatiseeritud töötlemine, mis hõlmab isikuandmete kasutamist füüsilise isikuga seotud teatavate isiklike aspektide hindamiseks, eelkõige selliste aspektide analüüsimiseks või prognoosimiseks, mis on seotud asjaomase füüsilise isiku töötulemuste, majandusliku olukorra, tervise, isiklike eelistuste, huvide, usaldusväärsuse, käitumise, asukoha või liikumisega. Sellest sõnastusest nähtub, et „profiilianalüüsi" toomine GDPR-i on märgatavalt seotud sellise tehnoloogia laia levikuga, mis võimaldab võrgu kasutajatele suunata kohandatud sisu, näiteks reklaami, lähtuvalt andmesubjekti käitumisest võrgus.

Profiilianalüüsi teostamise korral on vastutaval töötlejal kohustus sellest andmesubjekti teavitada ning avaldada teave sellise töötlemise tähtsusest ja prognoositavatest tagajärgedest andmesubjekti jaoks.[310] Lisaks peab andmesubjektile olema võimaldatud profiilianalüüsi teostamise kohta esitada vastuväiteid ning vastutav töötleja peab sel juhul sellise töötlemise lõpetama, eriti kui profiilianalüüsi teostatakse otseturunduse eesmärgil.[311]

Kuna ka profiilianalüüsi kui andmetöötluse eraldi kategooria sätestamine GDPR-is on olulise positiivse mõjuga meede andmesubjekti põhiõiguste tagamisel, mida PS põhimõtetest ei leia, on PS põhimõtete alusel korraldatav isikuandmete töötlemine oluliselt piiravama mõjuga andmesubjekti õigusele informatsioonilisele enesemääratlusele võrreldes GDPR-iga.

2.2.2. Vahekokkuvõte

Tulenevalt eelnevast analüüsist on selge, et alates GDPR-i rakendamisest kevadel 2018 ei taga *Privacy Shield* programm selles sätestatud põhimõtete puudulikkuse tõttu enam USA ettevõtete poolt teostatava isikuandmete töötlemise suhtes andmekaitse taset, mis on sisuliselt samaväärne EL-iga.

[310] GDPR artikkel 13(2f) ja 12(2g)
[311] GDPR artikkel 21(1) ja (2) ja artikkel 22

Autorile üllatuseks esineb *Privacy Shield* põhimõtetes oluline puudujääk isikuandmete töötlemise seaduslikkuse tagamisel. Kuna GDPR-is ei ole seda põhimõtet sisuliselt võrreldes kehtiva seaduslikkuse põhimõttega täiendatud, tõusetub sellest puudujäägist oluline küsimus rakendusotsuse 2016/1250 kehtivuse kohta, sest töötlemise seaduslikkus on EL-i andmekaitse õiguses sätestatud kategooriliselt. Iseenesest ei ole selle puudujäägi kõrvaldamine suureks probleemiks, kui PS põhimõtetes oleks eraldi deklareeritud GDPR-ile vastav seaduslikkuse põhimõte. Oluline on sel juhul lisada PS põhimõtetesse ka kindel ja üldine definitsioon „nõusoleku“, sealhulgas lapse nõusoleku, kohta.

Eesmärgipärasuse põhimõttest ning seda põhimõtet tagavates andmesubjekti õigustest rääkides, selgub et PS põhimõtetes sätestatud juurdepääsu põhimõtte ebaselge väljendusviis võimaldab vastutaval töötlejal keelduda andmesubjekti esitatud parandamise ja kustutamise nõude täitmisest alustel, mis on GDPR-i kohaselt keeldumiseks vaid andmetega tutvumise õigusest keeldumiseks. Selle puudujäägi korvamiseks piisaks viimati nimetatud õiguste selgemast ja eraldiseisvast määratlusest. Ka isikuandmete töötlemise piiramise õigus puudub PS põhimõtetes.

GDPR-iga võrreldes on PS põhimõtetega tagatud isiku kontrolliõigus oma andmete üle tunduvalt kitsam. Andmete ülekandmise õigus on GDPR-is oluline positiivne tagatis isiku informatsioonilise enesemääratlusõigusele. Samasugune mõju on ka profiilianalüüsi, kui isikuandmete töötlemise eriliigi, sissetoomisel GDPR-i. Kuna eelnevad suurendavad isiku enesemääratlusõigust, kõrgendavad nad ka EL-i andmekaitse taset ning PS põhimõtted sellele vasta.

KOKKUVÕTE

Käesoleva töö eesmärgiks oli tuvastada ning juhtida tähelepanu pärast rakendusotsuse 2016/1250 jõustumist aset leidnud ning aset leidvatele olulistele muutustele USA ja EL-i õiguskorras, mille adresseerimata jätmine ning mille suhtes ennetava tegevuse teostamata jätmine võib taaskord kulmineeruda Atlandiülest vaba isikuandmete edastamist võimaldava rakendusotsuse kehtetuks tunnistamisega EK poolt. Autor piiritles analüüsitavad muutused kahest olulisest sündmusest lähtuvalt: USA uus administratsioon kui *Privacy Shield* programmis sisalduvate USA ametiasutuste kinnituste jätkuvat paikapidavust mõjutav faktor ja GDPR, kui tulevane alus adekvaatsusotsuste väljastamiseks ja piisava andmekaitse taseme hindamise lähteregulatsioon.

Eelnevast tulenevalt püstitas autor käesoleva töö uurimusküsimuse: kas *Privacy Shield* programm käesoleval kujul tagab EL-i andmekaitseõigusega sisuliselt samaväärse isikuandmete kaitse taseme USA uue administratsiooni kontekstis ning pärast GDPR-i kohaldamist mais 2018. Hüpoteesina püstitas autor seisukoha, et *Privacy Shield* programmi poolt tagatav isikuandmete kaitse tase ei vasta käesoleval hetkel USA-st tulenevate muutuste tõttu EL-i andmekaitse tasemele ja PS põhimõtted ei vasta GDPR-i poolt pakutavale isikuandmete kaitse tasemele. Uurimusküsimuse teise osa puhul oli autori eesmärgiks tuvastada konkreetsed puudujäägid *Privacy Shield* põhimõtetes võrreldes GDPR-is sätestatud andmetöötlus põhimõtetega.

Tööd alustas autor sissejuhatava peatükiga Atlandiülese isikuandmete edastamise, kui EL-i andmekaitseõiguse valdkonna eelduste, kujunemise ja hetkeseisu kirjeldamisega.

Esimesest peatükist nähtus, et EL-i andmekaitseõigus lubab isikuandmeid edastada kolmandatesse riikidesse, nagu seda on ka USA, kolmel juhul: kui esineb mõni artiklis 26(1) nimetatud erand, andmetöötlejad rakendavad isikuandmete edastamisele piisavaid tagatisi (näiteks lepingulisi tüüptingimusi või kontsernisiseseid eeskirju) või isikuandmete edastamise sihtriigi andmekaitse tase on Komisjoni poolt tunnistatud piisavaks. Nimetatutest viimane on isikuandmete töötlejate jaoks kõige mugavam ning digitaalmajandusele vähim piiranguid seadev variant.

Selleks, et Komisjon saaks kolmanda riigi suhtes adekvaatsusotsuse teha, peab see oma siseriikliku õigusega ja kohaldava praktikaga tagama andmekaitse taseme, mis on sisuliselt samaväärne EL-iga. USA siseriiklik õiguse osas sellist adekvaatsusotsust teha ei saa.

USA andmekaitseõigus on fragmentlik, pakkudes kaitset ainult teatud liiki isikuandmetele. Selline lähenemine isikuandmete kaitsele ei vasta EL-i kõrgetasemelisele andmekaitsele. Samas välistab EL-i tüüpi andmekaitsereeglistiku rakendamise USA kohalikus õiguses valitsev liberaal-majanduslik printsiip, konstitutsioonilised piirangud ning üldine arusaam isikuandmete töötlemisest kui pigem majanduse ning ettevõtlusvabaduse valdkonda, kui isiku põhiõiguste sfääri kuuluvast tegevusest.

Kuna USA ja EL-i vahelise piiranguteta isikuandmete liikumine on mõlemale poolele majanduslikest kaalutlustest lähtuvalt oluline, on USA ja EL alates direktiivi 95/46 algusaastatest saadik näinud vajadust õigusraamistiku järele, mis siiski võimaldaks USA ettevõtetel Euroopast edastavaid isikuandmeid vabalt töödelda. Aastal 2000 loodi õigusraamistik *Safe Harbor,* mille kohta andis Komisjon välja adekvaatsusotsuse. Oktoobris 2015 tunnistas EK otsusega C-362/14 *Schrems* selle otsuse kehtetuks, sest EK hinnangul ei taganud *Safe Harbor* isikuandmete piisavat kaitset. Juulis 2016 asendati *Safe Harbor* õigusraamistikuga *Privacy Shield,* mille Komisjon hindas piisavat kaitset tagavaks.

Teise peatüki vältel vastas autor uurimisküsimusele ning täitis töös püstitatud eesmärgi, juhtides esmalt tähelepanu pärast rakendusotsuse 2016/1250 vastuvõtmist USA-st tulenevatele asjaoludele, millele Komisjon suvel 2017 toimuva *Privacy Shield* kontrolli raames tähelepanu peab pöörama ja mille osas USA uuelt administratsioonilt täiendavaid kinnitusi saama. Vastasel juhul jääks kõrvaldamata mittevastavus *Privacy Shield* programmi ja EL-i andmekaitse tasemete vahel ning isikuandmete edastamine rakendusotsuse 2016/1250 alusel tuleks lõpetada.

USA administratsiooni vahetamise tähenduses tekitas *Privacy Shield* programmis sisalduvatest kinnitustest erilist tähelepanu presidentaalne direktiiv PPD-28, mis on USA õiguses sätestatud eesmärgiga piirata USA luureasutuste poolt teostatavat signaalluurealast tegevust, pannes kohustuseks tegevuse teostamisel arvestada kõikide andmesubjektide isikuõigustega.

Sealjuures tuleb tähele panna, et PPD-28 ning muude *Privacy Shield* programmis nimetatud USA luuretegevusele kohalduvate piirangute puhul esitab USA luurejuhi ameti esindaja ülevaate USA õiguses olevatest riiklikku luuret reguleerivatest õigusaktidest ning seega hindab sisuliselt Komisjon rakendusotsuses 2016/1250 USA õiguskorras luuretegevust reguleerivate õigusaktide vastavust EL-i õigusele, mitte USA võetud rahvusvaheliste kohustuste vastavust EL-i õigusele, nagu PS põhimõtete puhul.

PPD-28-ga seoses tuvastas autor järgneva probleemkoha:

EL-i õiguses kehtib põhimõte, mille kohaselt peab õigusakt, millega kaasneb sekkumine isiku privaatsus- ja andmekaitseõigusesse, sisaldama selgeid ja täpseid õigusnorme, mis reguleerivad sekkumise meetme ulatust ja kohaldamist ning võimaldama sekkumist kõigest ulatuses, mis on rangelt vajalik.

PPD-28 ei ole aga seadusandliku organi poolt antud õigusakt, nagu aktid, mis loovad USA luureasutustele õigusliku aluse isikute privaatsusesse sekkumiseks. Presidentaalsed direktiivid on USA presidendi seadusandlikud aktid, mille järgimine ei ole järgnevatele presidentidele kohustuslik. Iga president võib eelneva presidendi poolt vastuvõetud direktiivid ning korraldused vabalt kehtetuks tunnistada ja nendega vastuolus olevaid otsuseid vastu võtta ja kohaldumisele kuulub valitseva presidendi õigusakt. Euroopa Kohtu sõnul peab isikuõiguste riivet võimaldav EL-i õigusakt sätestama ka piiranguid, mis tagavad sekkumise vaid rangelt vajalikus ulatuses. Seega nähtub kohtupraktikast, et riivet piiravad sätted peavad omama vähemalt võrdväärset õiguslikku jõudu sättega, mis riivet võimaldab. See tingimus ei ole täidetud PPD-28 puhul, mille jätkuv rakendamine on piltlikult öeldes president Trumpi kätes. Kuigi nimetatud puudujääk ei ole tingitud USA administratsiooni vahetusest, vaid oleks pidanud üles kerkima juba Komisjoni rakendusotsuse tegemise ajal, on USA uuel administratsioonil võimalik see puudujääk kõrvaldada, kui PPD-28-le vastavad normid sätestataks USA seadustes või lisataks *Privacy Shield* programmi täiendavad kinnitused luuretegevusele kohalduvate piirangute kohta, mis oleksid käsitletavad USA rahvusvaheliste kohustustena EL-i ees.

Peale selle tuvastas autor, et *Privacy Shield* dokumentides nimetatud USA luureasutuste üle järelevalvet teostatava PCLOB komisjoni ning *Privacy Shield* ombudsmani ametikohad on puudulikult täidetud – PCLOB kohustuslikust 7 liikmest tegutseb ainult üks ning ombudsmani ametikohustusi täitva ametiisiku positsioon on täitmata. Sellised ebakõlad Obama administratsiooni poolt antud kinnituste ning Trumpi administratsiooni tegevuse vahel on oluliseks murekohaks rakendusotsuse 2016/1250 jätkuva kehtivuse küsimuses.

Privacy Shield ombudsman on programmi kohaselt ametiisik, kelle kaudu saavad Euroopa andmesubjektid enda andmekaitseõigusi teostada, kui isikuandmete töötlejaks on USA luureasutus. PCLOB on USA luuretegevuse järelevalve teostamisel oluline organ ning ka ombudsmanile tema ametikohustuse täitmisel üheks olulisemaks vahendiks. Seega tuleb järeldada, et vastavate ametipositsioonide täitmata jätmine president Trumpi poolt on põhjustanud olukorra, kus USA luuretegevuse üle teostatav järelevalve on oluliselt langenud

ning ei vasta enam eelneva administratsiooni poolt kinnitatud tasemele. Kuna varasemate kinnituste järgimine USA ametiasutuste poolt oli rakendusotsuse 2016/1250 tegemise eeldusteks, tuleb asuda seisukohale, et *Privacy Shield* programmiga ei ole tagatud isikuandmete kaitse piisav tase, kui isikuandmed satuvad USA luureasutuste valdusesse.

Kolmandaks analüüsis autor president Trumpi 25. jaanuari täidesaatvat korraldust, mis sätestas, et kolmandate riikide kodanike suhtes ei rakendata USA *Privacy Act*'is tulenevaid õigusi ja kohustusi. Korralduse väljakuulutamise järel tekitas see andmekaitseringkondades rahulolematust, sest väideti, et korraldus on põhjustanud rakendusotsus 2016/1250 kehtetuse. Kuna 2015. aastal kehtima hakanud JRA kohaselt rakendatakse *Privacy Act*'i ka EL-i kodanike suhtes ning presidentaalsed seadusandlikud aktid devalveeruvad seadusandliku organi poolt vastuvõetud seaduste ees, ei olnud nimetatud kahtlustel tegelikkuses alust.

Lisaks hinnatavast kolmandast riigist, ehk siinkohal USA-st, tulenevatele põhjustele, mis adekvaatsusotsuse kehtivust võivad mõjutada, võivad kehtivust mõjutada ka EL-ist endast tulenevad muutused. Kuna kevadel 2018 rakendub GDPR, muutub adekvaatsusotsuste andmise õiguslik alus ning piisava andmekaitse taseme hindamise lähtekoht ehk kõrgeneb EL-i andmekaitse tase. Selleks, et vältida rakendusotsuse 2016/1250 kehtetust, on oluline täiendada *Privacy Shield* programmi enne 2018. aasta maid selliselt, et see vastaks kõrgenenud andmekaitse tasemele.

Peatükis 2.2. analüüsis autor sellest lähtudes PS põhimõtete vastavust GDPR-is sätestatud andmekaitse põhimõtetele ja andmesubjektidele tagatud õigustele. Analüüsist nähtus, et PS põhimõtetega tagatud andmekaitse tase on GDPR-iga tagatuga võrreldes puudulik ning PS põhimõtteid täiendamata tuleks rakendusotsus 2016/1250 tühistada, sest *Privacy Shield* programm ei taga pärast 2018. aasta mai enam andmekaitse taset, mis on sisuliselt samaväärne EL-i andmekaitse tasemega.

Esiteks leidis autor, et PS põhimõtete alusel töötlemise korral ei pruugi olla tagatud GDPR-iga samaväärne isikuandmete kaitse seadusliku töötlemise põhimõtte nõrga esindatuse tõttu PS põhimõtetes. GDPR, nagu ka direktiiv 95/46, sätestab piiratud hulga õiguslikke aluseid, mille esinemine on seadusliku töötlemise eelduseks. Probleeme tekitab tõsiasi, et PS põhimõtetes ei ole eraldi sätestatud ammendatud nimekirja tingimustest, mis on eelduslikud õiguspärasele isikuandmete töötlemisele, nagu on sätestatud GDPR-i artiklis 6(1). See võib tekitada olukordi, kus USA andmetöötleja, kogudes isikuandmeid otse andmesubjektilt, töötleb neid ilma õigusliku aluseta. Seda peamiselt seetõttu, et PS põhimõtetes puudub ühtne ja läbiv „nõusoleku" määratlus – nõusolekuna nähakse nii loobumist (*opt-out*), valimist (*opt-in*), kui ka

sõnaselget nõusolekut. Ebamäärane termini „nõusolek“ definitsioon võimaldab töötlejatel teatud olukordades eeldada andmesubjekti nõusolekut mõningatel eesmärkidel isikuandmete töötlemise suhtes. Eelnev ei vasta GDPR-is sätestatud „nõusoleku“ mõistele ja seega võimaldavad PS põhimõtted USA töötlejatele töödelda EL-ist edastatud isikuandmeid ilma õigusliku aluseta.

Sellega seoses märkis autor, et GDPR-is ei ole seadusliku töötlemise aluseid sisuliselt võrreldes kehtivate alustega oluliselt muudetud ja seega tõusetub oluline küsimus rakendusotsuse 2016/1250 üldise kehtivuse kohta, sest töötlemise seaduslikkus on EL-i andmekaitseõiguses sätestatud kategooriliselt.

Läbipaistvuse põhimõtte esindatuse analüüsimisel PS põhimõtetes, liigitas autor selle alla teate ja juurdepääsu põhimõtted PS põhimõtetes sätestatud kujul. Teate põhimõttel on *Privacy Shield* raamistikus lisaks läbipaistvusele ka teine eesmärk – oma tegevuse USA FTC või Transpordiministeeriumi järelevalvele allutamine. GDPR-is on konkreetne teave, mida vastutav andmetöötleja peab andmesubjektile edastama võrreldes PS põhimõtetega mitmekesisem. Seda põhjusel, et GDPR sisaldab mõningaid uusi elemente, mida kehtivas EL-i andmekaitseõiguses ei ole ning kohustuse neist ka andmesubjekti teavitada. Osa teabest, mida *Privacy Shield* ettevõte andmesubjektile esitama peab, tuleneb konkreetselt sellest, et tegemist on *Privacy Shield* programmi alusel isikuandmete töötlejaga.

Eesmärgipärasuse põhimõttest ning seda põhimõtet tagavates andmesubjekti õigustest rääkides, selgub et PS põhimõtetes sätestatud juurdepääsu põhimõtte ebaselge väljendusviis võimaldab vastutaval töötlejal keelduda andmesubjekti esitatud parandamise ja kustutamise nõude täitmisest alustel, mis on GDPR-i kohaselt keeldumiseks vaid andmetega tutvumise õigusest keeldumiseks. See asjaolu nähtub ka ettevõtte Google Inc., mis on *Privacy Shield* programmiga liitunud ettevõte, vastavatest privaatsusreeglitest. PS täiendavates põhimõtetes on küll pühendatud mitme leheküljeline osa juurdepääsu põhimõtte rakendamisele, kuid sealt on juurdepääsu põhimõttel PS üldistes põhimõtetes sätestatust kitsam tähendus. Seega leidis autor, et GDPR artiklist 15 tulenev andmesubjekti õigus oma andmetega tutvuda on samaväärne PS põhimõtetes ja PS täiendavates põhimõtetes sätestatuga, kuid parandamise, kustutamise ja töötlemise piiramise õigus on jäänud laiemalt avamata, mistõttu ei võimalda PS põhimõtted andmesubjektil teostada õigust isikuandmeid parandada või kustutada GDPR-ile vastavas ulatuses.

Eesmärgipärasuse põhimõtte mittevastavuse GDPR-ile on võimalik kõrvaldada andmesubjekti õigusega nõuda andmete parandamist ja kustutamist eraldi sätestamisega ja käsitlemisega PS põhimõtetes.

GDPR-is säilitamise piiramise põhimõtte kontekstis sätestatud kohustus määratud tähtaegade tagant isikuandmeid kustutada või läbi vaadata näib kaudselt olevat tagatud PS täiendavates põhimõtetes sätestatud kontrollimise kohustusega. *Privacy Shield* programmiga liitunud ettevõtted peavad rakendama kontrollimeetmeid, et tõendada PS põhimõtetega kooskõlas olevate ja andmesubjektidele avaldatud töötlemistavadest kinnipidamist. Need kontrollimeetmed peaksid olema rakendatud enesehindamistena või välise kontrolli kaudu. Kui ettevõte rakendab enesekontrolli, peab ta perioodiliselt teostama ka objektiivsest kontrolli. Objektiivse ehk välise kontrolli puhul kontrollitakse samuti vastavust PS põhimõtetele ja seega ka kohustust säilitada isikuandmeid identifitseeritaval kujul vaid nii kaua, kuni see on vajalik töötlemiseks isikuandmete kogumise eesmärkidest lähtuvalt. Seega peaksid perioodilised välised ja objektiivsed kontrollid tagama ka isikuandmete säilitamise piiramise põhimõttest kinni pidamise ehk vajadusel mitteasjakohaste isikuandmete kustutamise.

Andmekaitseõigus on oluliselt seotud isiku õigusega end informatsiooniliselt määratleda ning seega on andmekaitseõiguse oluline funktsioon anda isikule kontroll oma isikuandmete üle. GDPR-iga võrreldes on PS põhimõtetega tagatud isiku kontrolliõigus oma andmete üle tunduvalt kitsam. Andmete ülekandmise õigus on GDPR-is oluline positiivne tagatis isiku informatsioonilisele enesemääratlusõigusele. Samasugune mõju on ka profiilianalüüsi, kui isikuandmete töötlemise eriliigi sissetoomisel GDPR-i. Kuna eelnevad suurendavad isiku enesemääratlusõigust, tõstavad nad ka EL-i andmekaitse taset ning PS põhimõtted sellele tasemele ei vasta.

Andmete turvalisuse põhimõte on GDPR-is sätestatud pigem nõuandva eesmärgiga, millest ei saa välja lugeda töötlejale kohalduvaid konkreetseid kohustusi. Oluline, mida turvalisuse põhimõte GDPR-is ette näeb, on kohustus suhtuda isikuandmete töötlemisse hoolsusega ja rakendada praktikas, olenevalt isikuandmete töötlemise asjaoludesid, piisavaid abinõusid, et isikuandmed ei satuks pahatahtlike kolmandate isikute töötlemise objektiks ning vältida vastutava töötleja hooletusest tingitud töötlemist (nt tahtmatu kustutamine, kadumine jne). Selles osas on PS põhimõtetes ja GDPR-is sätestatu vahel kattuvus olemas.

Eelnevast nähtuvalt leidis käesolevas töös kinnitust autori poolt esitatud hüpotees, mille kohaselt ei vasta *Privacy Shield* programm käesoleval hetkel USA-st tulenevate muutuste tõttu EL-i andmekaitse tasemele ja PS põhimõtted ei vasta GDPR-i poolt pakutavale isikuandmete

kaitse tasemele. Olulised eeldused selliseks järelduseks tulenevad esiteks asjaolust, et PPD-28 ei võimalda oma normihierarhilise positsiooni tõttu pakkuda samaväärset kontrolli luureasutuste tegevuse üle, kui EL-i õigus ning PS põhimõtetes esineb olulisi puudujääke selleks, et pakkuda andmesubjektidele GDPR-is sätestatud andmekaitse põhimõtetele vastavat kaitset

Töös jõuab autor järeldusele, et *Privacy Shield* programmi on oluline lähiajal põhjalikult täiendada, selleks et saaks programmi pidada piisavat andmekaitse taset tagavaks. Esimesed muudatused peaksid aset leidma juba eeloleval suvel, kui Komisjon alustab kontrolli õigusraamistiku toimise üle ning sel puhul on oluline adresseerida mõningaid USA administratsiooni vahetusest tulenevaid asjaolusid, aga juhtida tähelepanu ka järgmisel aastal GDPR-i kaudu EL-i õiguse kõrgenenud andmekaitse tasemele ning PS põhimõtted GDPR-iga kooskõlla viia.

Significant Developments in law and legislation of the United States and European Union from the perspective of validity of the Commission implementing decision (EU) 2016/1250

Summary

The role played by personal data in the digital economy cannot be underestimated. Controllers collect data subject's data as a prerequisite to providing them services, but also use it for personal objectives such as predicting consumer behaviour and selling it to other controllers. Since personal data of the consumers have a great value to businesses, it can happen that the person behind these data is just reduced to the object of the data. This raises concerns from the perspective of fundamental privacy rights of the data subjects.

Although states are more-or-less unanimous when it comes to the necessity of protection of the personal data, the approach on the depth and form of appropriate protection is divided. Different paths taken in the regulation of data protection by the United States and European Union (hereinafter "EU") is the main starting point of this work.

EU's data protection law is based on the directive 95/46/EC, which is often considered the most influential data protection instrument out there. By providing a thorough regulation on processing of personal data, whereas the terms "personal data" and "processing" have a broad scope within the directive, and restricting transmissions of personal data to states that don't guarantee adequate data protection level, the EU presents an example of implementation of high level of personal data protection. The significance of personal data protection and privacy rights for the Europeans is also apparent from the fact that the right to data protection has been elevated to the level of fundamental right by the Charter of Fundamental Rights of the European Union.

In U.S. legislation, data protection is an inherent part of right to privacy and there it is rather referred to as data or information privacy. Information privacy takes a different approach on protecting personal data than EU's corresponding regulation. One can't find such broadly defined terms in U.S. legislations to "processing" and "personal data" as one could in EU. Information privacy covers only few types of personal data such as finance data or medical data etc. Such a fragmented approach to protection of personal data doesn't meet EU standards and therefore, according to current EU law, personal data transmissions to the U.S. without sufficient safeguards is prohibited.

However, taking account the economic importance of free flow of data between EU and U.S., the parties find it essential to keep transatlantic data flows as restriction-free as possible. Namely because the trade between these two makes up more than a half of the world's GDP and the percentage of digital economy takes up a bigger part of by year. In the context of modern free trade, it is important to ensure that transatlantic data flows stay as free as possible.

With that objective in mind, U.S. and EU have concluded a legal framework that allows U.S. companies to receive personal data sent from EU, if they fulfil certain prerequisites. Currently operational framework is called Privacy Shield and it is second of its kind concluded between the two. Legal basis for transatlantic personal data transmissions is provided with the European Commission's (hereinafter "Commission") implementing decision (EU) 2016/1250 (hereinafter "decision 2016/1250") that deems that personal data transmitted to the companies of the U.S. in accordance with the Privacy Shield enjoy an adequate level of personal data protection.

Privacy Shield and decision 2016/1250 are updated versions of their predecessors Safe Harbor and implementing decision 2000/520/EC (hereinafter "decision 2000/520"). European Court of Justice (hereinafter "ECJ") found in the decision C-362/14 *Schrems v Data Protection Commissioner* (hereinafter "C-362/14") of October 6th 2015 that Safe Harbor didn't provide an adequate level of personal data protection to the data transmitted to the U.S. and announced decision 2000/520 invalid.

Without evaluating the principals stipulated in the Safe Harbor, the ECJ's concerns were concentrated on the fact that Safe Harbor did not foresee any safeguards for the personal data of the Europeans when these happened to be processed by the U.S. intelligence agencies in accordance with U.S. forgein intelligence programs. Since these programs were implemented by the U.S. government after the decision 2000/520 was passed by the Commission, ECJ saw it necessary to emphasize the need to conduct regular check-ups on the Commission adequacy decisions to reassure their continual validity. It was pointed out by the advocate general Bot, who was assigned to case C-362/14, that the invalidity of Commission adequacy decisions, unlike most other type of decisions passed by the Commission, could be caused by factors that weren't apparent on the time of implementing of that decision. As an adequacy decision is essentially an assessment of a legal system from the perspective of EU data protection law at a given time, the invalidly of it could be resulted by events occurring after the making of the decision. These impact-having events could originate from the third country, in case of drop of its level of data protection, but also from other subsequent events.

These remarks have been noted by the Commission when drafting the decision 2016/1250, as it stipulates that the Commission is obliged to perform annual check-ups on the level of data protection provided by Privacy Shield. In addition, articles 4(2) and 4(3) of the decision 2016/1250 establish an obligation to the member states to notify the Commission about circumstances that indicate to the possible non-compliance of the data protection level provided by Privacy Shield to EU law.

Since due to the economic importance of consistently easy and unrestricted personal data transmissions from EU to U.S. is important to both parties, it is also important to identify and eliminate any problems as soon as possible that, when left unsolved, would result in invalidity of the decision 2016/1250 and therefore cessation of free transatlantic personal data transmissions.

Main objective of this work is to draw attention to important issues and changes in U.S. and EU legislation that have occurred and will occur after the implementation of the decision 2016/1250 and which, when left unaddressed, could result in another invalidation of the transatlantic personal data transmission enabling framework by the ECJ.

When talking about possible issues and changes in the U.S. and EU legislation, the author sees two important ones in the given context: first, the change in U.S. administration and the effect of the rule of president Trump on the confirmations given by the former administration in the documents of Privacy Shield program and secondly, the replacement of the directive 95/46 with the General Data Protection Regulation (hereinafter "GDPR") in May of 2018.

Following the structure of the Privacy Shield program, these developments have an influence on different levels of the program – first, since the executive branch of the U.S. is guided from the worldview and policies of the president, the change in administration could have an effect on the confirmations given by the former administration in Privacy Shield documents. Secondly, GDPR will replace the legal ground for adequacy decisions announced by the Commission, but also it will change the level of data protection granted for EU data subjects in the EU. This means that the data protection level provided by Privacy Shield principles, will not meet the level of data protection in the EU after May of 2018, even though it would correspond to the level provided by the directive 95/46.

Guided from the previous, the research question of this work is formulated thusly: does the Privacy Shield program ensure the data protection level that is essentially equivalent to EU law in the context of new U.S. administration and after implementation of the GDPR in May of 2018. As a hypothesis, the author stipulated that answers to both of the questions are negative.

In order to provide answers to the research questions, the author has divided the work into two chapters. First chapter has an introductory purpose and gives an overview of the subfield of EU's data protection law that considers transatlantic personal data transmission, its legal background, formation and necessity. In the second chapter the author turns to the research questions to provide answers to them in separate subchapters.

The first chapter showed that there are three possible legal bases for transmitting personal data to third countries under EU law, most important of which, within the meaning of this paper, is transmitting personal data under adequacy decision issued by the Commission about a third country. Adequacy decisions, conjointly, provides for the most comfortable and least restricting alternative for the controllers.

Since the data privacy laws of the U.S. make up a fragmented patch-work type regulation, it couldn't be considered a country that provides equal level of data protection to the one that EU legislation does. Therefore, Commission adequacy decisions are ruled out in respect to U.S. domestic law. Due to the ruling liberal-economic principle, constitutional restrictions and general understanding of data processing as something that rather falls in the scope of entrepreneurial freedom than personal privacy, implementing data protection rules similar to EU's in the U.S. is not an option. Former dictates, that restriction free personal data transmissions to U.S. processors and controllers could only be achieved through legal frameworks like Safe Harbor and Privacy Shield that leave it up to companies to implement stricter rules on their personal data processing for an exchange of being able to receive personal data from EU without restrictions.

In the first subchapter of chapter 2, the author analyzed the effect of the change in administration to the confirmations given in the Privacy Shield documents by the previous administration. Most significant effects were identified in the context of confirmations given about the activities of U.S. intelligence agencies. The author took notice of the fact that there are two separate levels identifiable in the decision 2016/1250. In the first one, the Commission has assessed the adequacy of the data protection provided by the Privacy Shield principles and U.S. authorities' obligations to EU about ensuring the operation of the Privacy Shield framework. The second one is essentially an assessment of the U.S. national legislation on the foreign intelligence activities carried out by the intelligence community. As Privacy Shield provides for a legal basis for the intelligence agencies to collect personal form Privacy Shield companies who have received it from the EU, appendix 6 of the decision 2016/1250 constitutes an overview of U.S. national legislation that provides legal basis for conducting intelligence activities and restrictions that apply on intelligence gathering.

First point of interest to the author concentrated on the presidential directive PPD-28 issued by president Obama, that provides restrictions on the signals intelligence activities carried out by U.S. intelligence agencies. PPD-28 establishes policies and procedures governing the safeguarding of personal information collected from signals intelligence activities.

According to EU law, EU legislation interference with rights such as privacy or data protection must lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data.

Legal basis for conducting intelligence activities is granted to intelligence communities by congressional laws. Aforementioned restrictions on intelligence activities are provided with PPD-28, which isn't a congressional law, but a presidential legislative act. Presidential act such as presidential policy directives can be freely revoked, changed and conflicted by subsequent presidents and their presidential legislative acts (executive orders, policy directives etc.). Since the court practice of the ECJ demands that the legislations that provides restrictions to interference is situated at least on the same level on the hierarchy of norms as the legislation that provides the basis for the interference, it must be concluded that PPD-28 doesn't fails to secure the level of data protection that is essentially equivalent to the one provided by EU law.

Furthermore, the author ascertained that the supervision conducted on the U.S. intelligence agencies is inadequate because the members of the supervisory board PCLOB have been left vacant by president Trump. Currently PCLOB has only one member. The author also discovered that the Privacy Shield ombudsperson's position has been vacant for months. Therefore, it must be concluded that oversight exercised on U.S. intelligence authorities is unsatisfactory and doesn't correspond to the factual situation that was apparent when Privacy Shield was announced adequate by the Commission.

Thirdly, the author analysed president Trump's executive order from January 25th 2017, that directed U.S. authorities to ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information. This clause of executive order was claim to make decision 2016/1250 invalid by some privacy activists. As the author found out, these accusations held no ground, since Judicial Redress Act of 2015 granted these rights to Europeans.

In the second subchapter of chapter 2 the compatibility of Privacy Shield principles with the data processing principles provided by the GDPR was analysed. The author concluded that data

protection level granted by Privacy Shield principles is inadequate when compared to GDPR and that would necessitate thorough reformation of the Privacy Shield, in order to maintain lawful personal data transmission under the adequacy decision after May of 2018.

First, it was identified that the principle of legality as it is stipulated in the GDPR is not fully covered by Privacy Shield principles. The author discovered that PS principles allow unlawful processing of personal data in some cases where data is gathered directly form the data subject. GDPR and directive 95/46 lay down a confined list of legal basis for lawful processing, Privacy Shield doesn't. Former doesn't automatically refer to incompatibility with GDPR, since other Privacy Shield principles or circumstances inherent to the transfer could ensure that every processing carried out by the Privacy Shield company. However, this isn't always the case in Privacy Shield. "Consent" in Privacy Shield principles doesn't have an unambiguous meaning and distinctive scope. Therefore, when personal data is gathered from the data subject, this shortcoming allows for processing of the personal data what could seem as processing based on the data subject's consent, but according to EU's current and future law, it isn't.

This raises further questions on whether decision 2016/1250 could even have been passed by the Commission according to EU law, as it seems that the principles therein don't actually provide an adequate level of data protection. Since the mentioned fell out of the scope of this work, the author refrained from analysing the validity of decision 2016/1250 further.

The principles of purposeful processing is also not fully ensured by the Privacy Shield principles. The author has concluded that vague and indistinct formulation of the access principal in Privacy Shield allows processors to refuse data subjects to exercise the right to erasure and right to rectification on the grounds that only allow refusal to provide access to the data subject's personal data in GDPR. This could result in situations where processors refuse to erase or rectify data that are false or inadequate on basis that in GDPR only allow to refuse from providing access to personal data.

Data protection law is strongly tied to the person's right to informational self-determination and therefore the function of the data protection laws should be to ensure as big of a control for the data subject over his or her personal data as feasible. When comparing the control over the personal data grated to the data subject by GDPR and Privacy Shield, GDPR prevails. The right to data portability, as it is provided in the GDPR, is a new positive instrument for data subjects to ensure their right to informational self-determination. Stipulation of profiling as a sub-category of processing in the GDPR also contributes to this purpose. Since these are new instruments in the EU data protection law, they are absent from Privacy Shield principles.

Considering the effect on the data subjects' control over their personal data and right to informational self-determination, these are great examples of the heightened level of data protection resulted in application of GDPR and therefore, it is crucial that these aspects are added to the Privacy Shield prior to the date of implementation of GDPR. Otherwise, the privacy Shield would have to share the fate of its predecessor Safe Harbour.

In conclusion, the research hypothesis proposed in the thesis was confirmed, as the listed shortcomings prove that the data protection level provided by the Privacy Shield doesn't correspond to the level that is provided with EU legislation due to U.S. administration change. Even if the problems pointed out in the chapter 2.1. are resolved, the invalidity of the decision 2016/1250 will be apparent as soon as the GDPR takes effect in May 2018. The shortcomings of Privacy Shield processing principles in the context of GDPR were pointed out.

Lühendid

EK	Euroopa Kohus
EL	Euroopa Liit
ELPH	Euroopa Liidu Põhiõiguste Harta
FISA	*Foreign Intelligence Act* – USA välisluuret reguleeriv seadus
FTC	*Federal Trade Commission* – USA Kaubandusministeeriumi juures tegutsev tarbijate õigustega ja konkuretsi rikkumistega tegelev järelevalve organ
FTCA	*Federal Trade Commission Act* – FTC tegevust reguleeriv õigusakt USA õiguses
GDPR	Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiiv 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)
JRA	*Judicial Redress Act of 2015* – USA õigusakt, mis laiendab teatud välisriikide kodanikele *Privacy Act*'ist tulenevaid õigusi
DoC	USA Kaubandusministeerium
PCLOB	*Privacy and Civil Liberties Oversight Board* – iseseisev USA täidesaatva võimu tegevuse üle andmesubjektide põhiõiguste järgimise kohta järelevalvet teostav komisjon, mille liikmed nimetab ametisse USA president
PPD-28	*Presidetial Policy Directive nr 28* – USA luureasutuste teostatava signaalluureele piiranguid seadev presidentaalne seadusandlik akt
PS põhimõtted	Rakendusotsuse 2016/1250 lisa 2 II lisas sätestatud isikuandmete töötlemise põhimõtted
PS täiendavad põhimõtted	Rakendusotsuse 2016/1250 lisa 2 II lisas sätestatud põhimõtted, mis täiendavad PS põhimõtteid ning annavad juhiseid PS põhimõtete rakendamiseks
WP29	Artikkel 29 Töörühm

Kasutatud kirjandus

1. Brandeis L., Warren S.; The Right to Privacy – R. Wacks; Privacy: The International Library of Essays in Law and Legal Theory. Volume II: Privacy and the Law; Dartmouth Publishing Company Limited; 1993; lk 3-30
2. Burke J.; Kohtuniku roll Ameerika õigussüsteemis; Juridica, 1993, nr 3, lk 59-60
3. Bräutigam T.; The Land of Confusion: International Data Transfers between Schrems and the GDPR; Helsinki 2016; Helsinki Legal Studies Research Paper 46; kättesaadav: https://ssrn.com/abstract=2920181 (01.05.2017)
4. Callahan-Slaughter A.; Lipstick on a Pig: The Future of Transnational Data Flow Between the EU and the United States; Tulane Journal of International & Comparitive Law; Vol 25, 2016, lk 239-258
5. Chu V., Garvey T.; Executive Orders: Issuance, Modification and Revocation; Aprill 2014; USA Kongressi uuringute teenistus; lk 1-10
6. Clark J., Lucente K.; Data Protection Laws of the World – Full Handbook; DLA Piper, 2017
7. Diorio S.; Data Protection Laws: Quilts versus Blankets; Syracuse Journal of International Law and Commerce; Vol 42, Nr 2; 2015; lk 485-513
8. Engels B.; Data portability among online platforms; Internet Policy Review; 11.06.2016, vol 5 nr 2; DOI: 10.14763/2016.2.408
9. Euroopa Liidu Põhiõiguste Amet ja Euroopa Nõukogu Euroopa Inimõiguste kohus. Euroopa andmekaitse käsiraamat; Luxembourg: Euroopa Liidu Väljaannete Talitus 2015
10. Farrell H.; Constructing the International Foundations of E-Commerce: The EU-U.S. Safe Harbor Arrangement; International Organization, Vol. 57 nr 2; Spring 2003; lk 276-306
11. Fialova E.; Data Portability and Informational Self-Determination; Masaryk University Journal of law and Technology; 2014, vol 8 nr 1; lk 45-55
12. Fuster G.; The Emergence of Personal Data Protection as a Fundamental Right of the EU; Springler: Cham, 2014
13. Gregory Voss W.; The Future of Transatlantic Data Flows: Privacy SHield or Bust; Journal of Internet Law; vol 19 nr 11; may 2016; lk 9-19

14. Hoofnagle C.; Comparative study on diferent approaches to new privacy challanges in particular in the light of technological developments – country studies- United States of America; Mai 2010, Euroopa Komisjoni uurimus, lk 23-24 ja 29, kättesaadav: http://ec.europa.eu/justice/data-protection/document/studies/index_en.htm (14.04.2017)
15. Howell W., Moe T.; The Presidential Power of Unilateral Action; Aprill 1999; Journal of Law, Economics & Organization, Vol 15, Nr 1; lk 131-179
16. Jolly I.; Data protection in United States: Overview; kättesaadav: http://uk.practicallaw.com/6-502-0467?q=*&qp=&qo=&qe= (13.03.2017)
17. Ku R., Shih R.; Data Privacy as a Civil Right: The EU Gets it?; Kentucky Law Journal, Vol 103 nr 3; 2014/2015; lk 391-404
18. Kuner C.; Transborder Data Flow Regulation and Data Privacy Law; Oxford University Press: Oxford 2013
19. Loidean N.; The End of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law; Journal of Internet Law, Vol 19, nr 8; veebruar 2016, lk 8-14
20. Marcinkowski B. M.; Privacy Paradox(es): In Search of a Transatlantic Data Protection Standard; Ohio State Law Journal, Vol 74 nr 6, lk 1167-1193
21. Meltzer J.; The importance of the internetand transatlantic dataflows for U.S. and EU trade and investment; Global Economy & Development; Brookings Institution working paper 79, oktoober 2014
22. Moss R. D.; Legal effectiveness of presidentaal directive, as compared to an executive order; 29.01.2000; kättesaadav: https://fas.org/irp/offdocs/predirective.html (01.05.2017)
23. Männiko M.; Õigus privaatsusele ja Andmekaitsele; Tallinn: Juura 2011
24. Narits R.; Õiguse Entsüklopeedia; Tallinn: Juura 2007
25. Nõmper A., Tikk E.; Informatsioon ja õigus; Tallinn: Juura 2007
26. Prosser W.; Privacy - R. Wacks; Privacy: The International Library of Essays in Law and Legal Theory. Volume II: Privacy and the Law; London: Dartmouth Publishing Company Limited 1993; lk 41-63;
27. Shaffer G.; Globalization and social protection: the impact of EU and International rules in the ratcheting up of U.S. data privacy standards; Talv 2000; vol 25, Yale Journal of International law, lk 1-88

28. Thomson J.; The Right to Privacy; - R. Wacks; Privacy: The International Library of Essays in Law and Legal Theory. Volume I: The Concept of Privacy; Dartmouth Publishing Company Limited; 1993, lk 3-5;
29. Tzanou M.; Data Protection as a fundamentaal right next to privacy? Reconstructing a not so new right; International Data Privacy Law, Vol. 3, No. 2; 2013; lk 88-99
30. Tzanou M.; Is Data Protection the Same as Privacy? An Analysis of Telecommunications' Metadata Retention Measures; Journal of Internet Law, Vol 17, nr 3; September 2013; lk 21-34
31. Schwartz P., Solove D.; Information Privacy Law; Wolters Kluwer Law & Business; New York, 2011, lk 10-11
32. Wacks R.; Privacy: The International Library of Essays in Law and Legal Theory. Volume I: The Concept of Privacy; Dartmouth Publishing Company Limited; 1993

Kasutatud õigusaktid

Euroopa Liidu õigusaktid

33. Euroopa Komisjoni otsus, 26. juuli 2000, 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; 2000/520/EÜ. – ELT L 215/7, 25.08.2000, lk 119-138
34. Euroopa Komisjoni otsus, 15. juuni 2001, kolmandatesse riikidesse isikuandmete edastamise lepingu tüüptingimuste kohta direktiivi 95/46/EÜ alusel (2001/497/EÜ) – ELT L181/19, 04.07.2001, lk 347-360
35. Euroopa Komisjoni otsus, 27. detsember 2004, millega muudetakse otsust 2001/497/EÜ kolmandatesse riikidesse isikuandmete edastamise lepingu alternatiivsete tüüptingimuste kogumi kasutuselevõtu kohta (2004/915/EÜ) – ELT L 385/74, 29.12.2004, lk 74-84
36. Euroopa Komisjoni otsus, 5. veebruar 2010, kolmandatesse riikidesse asuvatele volitatud töötajatele isikuandmete edastamise lepingu tüüptingimuste kohta nõukogu ja Euroopa Parlamendi direktiivi 95/46/EÜ alusel (2010/87/EL) – ELT L 39/5, 12.02.2010, lk 5-18

37. Euroopa Komisjoni rakendusotsus (EL) 2016/1250, 12. juuli 2016, isikuandmete kaitse piisavuse kohta ELi-USA andmekaitseraamistikus Privacy Shield vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ – ELT L 207, 01.08.2016, lk 1-112
38. Euroopa Liidu Põhiõiguste Harta – ELT C 326. 26. oktoober 2012, lk 391-407
39. Euroopa Parlamendi ja nõukogu 24.10.1995. a direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta; ELT L 281, 23.11.1995, lk 31-50.
40. Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiiv 95/46/EÜ kehtetuks tunnistamise kohta – ELT L 119/1, 04.05.2016, lk 1-88

USA õigusaktid

41. Bill of Rights of the United States of America (1791) kättesaadav: http://billofrightsinstitute.org/wp-content/uploads/2011/12/BillofRights.pdf (01.05.2017)
42. California Civil Code Section 1798.83 (The Shine the Light Law), kättesaadav: http://codes.findlaw.com/ca/civil-code/civ-sect-1798-83.html (01.05.2017)
43. Children's Online Privacy Protection Act of 1998, kättesaadav: https://www.law.cornell.edu/uscode/text/15/6501 (01.05.2017)
44. Constitution of the United States, kättesaadav: https://www.senate.gov/civics/constitution_item/constitution.htm (01.05.2017)
45. Executive Order: Enhancing Public Saftey in the Interior of the United States, 25.01.2017; kättesaadav: https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united (01.05.2017)
46. Executive Order: Protecting the nation from foreign terrorist entry into the United States; 27.01.2017; kättesaadav: https://www.whitehouse.gov/the-press-office/2017/01/27/executive-order-protecting-nation-foreign-terrorist-entry-united-states (01.05.2017)
47. Fair Credit Reporting Act, kättesaadav: https://www.law.cornell.edu/uscode/text/15/chapter-41/subchapter-III (01.05.2017)
48. Federal Trade Commission Act of 1914, kättesaadav: https://www.law.cornell.edu/uscode/text/15/chapter-2/subchapter-I (01.05.2017)

49. Foreign Intelligence Surveillance Act of 1978, kättesaadav: https://www.law.cornell.edu/uscode/text/50/1802 (03.04.2017)
50. Health Insurance Portability and Accountability Act of 1996, kättesaadav: https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm (01.05.2017)
51. Judicial Redress Act of 2015; kättesaadav: https://www.congress.gov/bill/114th-congress/house-bill/1428/text (24.04.2017)
52. Presidential Executive Order on the Revocation of Federal Contracting Executive Orders, 27.03.2017, kättesaadav: https://www.whitehouse.gov/the-press-office/2017/03/27/presidential-executive-order-revocation-federal-contracting-executive (01.05.2017)
53. Presidential Policy Directive/PPD-28, 17.01.2014, kättesaadav: https://fas.org/irp/offdocs/ppd/ppd-28.pdf (01.05.2017)
54. The Privacy Act of 1974; kättesaadav: https://www.law.cornell.edu/uscode/text/5/552a (24.04.2017)

Muud õigusaktid

55. Hessischen Datenschutzgesetz, 7. Oktober 1970, kättesaadav: http://lagis.online.uni-marburg.de/de/subjects/idrec/sn/edb/id/204 (01.05.2017)
56. Isikuandmete kaitse seadus – RT I, 1996, 48, 944.
57. OECD Guidlines on the Protection of Privacy and Transborder Flows of Personal Data, kättesaadav: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (01.05.2017)

Kasutatud kohtupraktika

Euroopa Kohtu praktika

58. EKo, 06.11.2003, C-101/01 *Lindqvist*
59. EKo, 07.05.2009, C-553/07, *Rijkeboer*
60. EKo, 09.10.2010, C-92/09, C-93/09, *Volker und Markus Schecke, Eifert*
61. EKo, 08.04.2014, C-293/12, C-594/12, *Digital Rights Ireland Ltd jt.*

62. EKo, 06.10.2015, C-362/14, *Schrems*

63. EKo, 06.10.2015, C-362/14, *Schrems*, kohtujuristi Yves Bot ettepanek

USA kohtupraktika

64. FTC complaint in the Matter of Twitter Inc. Docket NO. C-4316; kättesaadav: https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twittercmpt.pdf (01.05.2017)

65. Roberson v. Rochester Folding Box Co., N.Y. App. Div. 1901, kättesaadav: https://casetext.com/case/roberson-v-rochester-folding-box-co (01.05.2017)

66. Pavesich v. New England Life Insurance Co, 122 Ga. 190 (Ga. 1905), kättesaadav: https://casetext.com/case/pavesich-v-new-england-life-ins-co (01.05.2017)

Muu kohtupraktika

67. Saksamaa Bundesverfassungsgericht, 15.12.1983, otsus Volkszählungsurteil, kättesaadav: http://openjur.de/u/268440.html (01.05.2017)

Muud kasutatud materjalid

Euroopa Liidu organite infoallikad, juhendid, arvamused ja teadaanded

68. Artikkel 29 Töörühm; Statement of the Article 29 Working Party; 16.10.2015, Brüssel; kättesaadav: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf (01.05.2017)

69. Artikkel 29 Töörühm; WP 12: Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, 24.07.1998

70. Artikkel 29 Töörühm; WP 15: Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government, 26.01.1999

71. Artikkel 29 Töörühm; WP 114: Working Document on a common interpretation of Article 26(1) of the Directive 95/46/EC of 24 October 1995, 25.11.2005

72. Artikkel 29 Töörühm; WP 238: Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision; 13.04.2016

73. Euroopa Liidu delegatsioon USA-s; EU-US facts & figures; kättesaadav: http://www.euintheus.org/what-we-do/eu-us-facts-figures/ (01.05.2017);

74. Euroopa Kohus; 16. septembril 2016 esitatud hagi – Digital Rights ireland versus komisjon (Kohtuasi T-670/16) – ELT C 410, 07.11.2016, lk 26-27

75. Euroopa Komisjon; Binding Corporate rules; kättesaadav: http://ec.europa.eu/justice/data-protection/article-29/bcr/index_en.htm (01.05.2017)

76. Euroopa Komisjon; Commission decisions on the adequacy of the protection of personal data in third countries; kättesaadav: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (01.05.2017)

77. Euroopa Komisjon; Daily news 19/12/16; 19.12.2016, Brüssel; kättesaadav: http://europa.eu/rapid/press-release_MEX-16-4463_en.htm (01.05.2017)

78. Euroopa Komisjon; EU-U.S. Privacy Shield fully operational from today; pressiteade 01.08.2016; kättesaadav: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=33704 (01.05.2017)

79. Euroopa Komisjon; Euroopa Liidu Komisjon ja Ameerika Ühendriigid leppisid kokku Atlandi-üleste andmevoogude uues andmekaitseraamistikus Privacy Shield; pressiteade 02.02.2016, Strasbourg; kättesaadav: http://europa.eu/rapid/press-release_IP-16-216_et.htm (01.05.2017)

80. Euroopa Komisjon; Komisjon tegi ettepaneku andmekaitse-eeskirju põhjalikult reformida, et võimaldada kasutajatele suuremat kontrolli oma andmete üle ja vähendada kulusid; pressiteade 25.01.2012, Brüssel; kättesaadav: http://europa.eu/rapid/press-release_IP-12-46_et.htm (01.05.2017)

81. Euroopa Komisjon; Statement by Vice-President Ansip and Commissioner Jourova on the occasion of the adoption by MemberStates of the EU-U.S. Privacy Shield; teadaanne 08.07.2016, Brüssel; kättesaadav: http://europa.eu/rapid/press-release_STATEMENT-16-2443_en.htm (01.05.2017)

82. Euroopa Komisjoni teatis Euroopa Parlamendile ja nõukogule, mis käsitleb programmi Safe Harbor toimimist ELi kodanike ja ELis asuvate äriühingute seisukohast, COM(2013) 847 final; 27.11.2013, Brüssel

83. Euroopa Komisjoni teatis Euroopa Parlamendile ja nõukogule usalduse taastamine ELi ja Ameerika Ühendriikide vaheliste andmevoogude vastu, COM(2013) 846 final; 27.11.2013, Brüssel

84. Euroopa Komisjon; Questions and Anwser on the EU-U.S. Data Protection „Umbrella Agreement“; pressiteade 01.12.2016, Brüssel; kättesaadav: http://europa.eu/rapid/press-release_MEMO-16-4183_en.htm (01.05.2017)
85. Euroopa Komisjon; What is TTIP about?; kättesaadav: http://ec.europa.eu/trade/policy/in-focus/ttip/about-ttip/ (01.05.2017)
86. Euroopa Parlament; Parlamendiliikmed – Jan Philipp Albert; kättesaadav: http://www.europarl.europa.eu/meps/et/96736/JAN+PHILIPP_ALBRECHT_home.html (01.05.2017)

USA ametlike organite infoallikad, juhendid, arvamused ja teadaanded

87. Department of Commerce; Privacy Shield List; https://www.privacyshield.gov/list (01.05.2017)
88. Federal Trade Commission; Children’s Online Privacy Protection Rule: A Six-Step Compliance Plan for You Business; kättesaadav: https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance (15.03.2017)
89. Privacy and Civil Liberties Oversight Board; About the Board; kättesaadav: https://www.pclob.gov/about-us.html (08.04.2017)
90. Privacy and Civil Liberties Oversight Board; Board Members; kättesaadav: https://www.pclob.gov/about-us/board.html (09.04.2017)
91. The United States Department of Justice; Overview of the The privacy Act of 1974, kättesaadav: https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition (15.03.2017)
92. U. S. Department of Health and Human Services; The HIPAA Privacy Rule; kättesaadav: http://www.hhs.gov/hipaa/for-professionals/privacy/ (01.05.2017)
93. U.S. State Department; About Transatlantic Economic Council; kättesaadav: https://www.state.gov/p/eur/rt/eu/tec/c33255.htm (01.05.2017);
94. U.S. State Department; Alphabetical List of Bureaus and Offices – Other Senior Officials: Coordinators; kättesaadav: https://www.state.gov/r/pa/ei/rls/dos/1718.htm?MobileOptOut=1 (01.05.2017)
95. White House; Presidential actions; kättesaadav https://www.whitehouse.gov/briefing-room/presidential-actions (01.05.2017)

96. White House; The Inaugural Address; kättesaadav: https://www.whitehouse.gov/inaugural-address (01.05.2017)

Muud ametlikud allikad

97. Andmekaitse Inspektsioon; Isikuandmete liigutamine Euroopa ja Ameerika vahel lihtsustub; pressiteade 14.07.2016; kättesaadav: http://www.aki.ee/et/uudised/pressiteated/isikuandmete-liigutamine-euroopa-ja-ameerika-vahel-lihtsustub (01.05.2017)
98. Business Coalition for Transatlantic Trade; Economic Benefits of a Transatlantic Trade and Investment Partnership; kättesaadav: http://www.transatlantictrade.org/faqs/economic-benefits-of-a-transatlantic-trade-and-investment-partnership/ (01.05.2017)
99. Corrnell University Law School, Legal Information Institution; Commerce Clause; kättesaadav: https://www.law.cornell.edu/wex/commerce_clause (01.05.2017)
100. Cornell University Law School, Legal Information Institution; U.S. Constitution: Tenth Amendment; kättesaadav: https://www.law.cornell.edu/anncon/html/amdt10_user.html#amdt10_hd4 (01.05.2017)
101. Cornell University Law School, Legal Information Institution; U.S. Constitution: Fourth Amendment; Kättesaadav: https://www.law.cornell.edu/constitution/fourth_amendment (01.05.2017)
102. Encyclopedia.com; Economic liberalism; kättesaadav: http://www.encyclopedia.com/topic/liberalism.aspx (01.05.2017)
103. EPIC; Privacy Laws by State; kättesaadav: https://www.epic.org/privacy/consumer/states.html (01.05.2017)
104. Live Internet Stats; Internet Users; kättesaadav: http://www.internetlivestats.com/internet-users/ (01.05.2017)

Meedia, sotsiaalmeedia allikad ja eriala blogid

105. Albert J. P.; 26.01.2017 säuts; Twitter; kättesaadav: https://twitter.com/JanAlbrecht/status/824553962678390784?ref_src=twsrc%5Etfw&ref_url=http%3A%2F%2Fwww.wired.co.uk%2Farticle%2Ftrump-privacy-shield-data (01.05.2017)

106. Burgess M.; New presidential order could wreck US-EU Privacy Shield; Wired 27.02.2017; kättesaadav: http://www.wired.co.uk/article/trump-privacy-shield-data (01.05.2017)
107. Cobb S.; Data Privacy and data protection: US law and legislation; We Live Security 26.04.2016, https://www.welivesecurity.com/2016/04/26/data-privacy-data-protection-us-law-legislation-white-paper/ (01.05.2017)
108. Free Snowden; Surveillance programs; kättesaadav: https://edwardsnowden.com/surveillance-programs/ (01.05.2017)
109. Google Inc., Google'i teenusetingimused; kättesaadav: https://www.google.ee/intl/et/policies/terms/regional.html ((01.05.2017)
110. Google Inc., Privaatsuseeskirjad; kättesaadav: https://www.google.ee/intl/et/policies/privacy/ (01.05.2017)
111. Facebook Inc.; Data Policy; kättesaadav: https://www.facebook.com/policy.php (01.05.2017)
112. Facebook Inc.; Facebook Inc. and the EU-U.S. Privacy Shield, kättesaadav: https://www.facebook.com/about/privacyshield (01.05.2017)
113. Facebook Inc.; Statement of Rights and Resposibilities; kättesaadav: https://www.facebook.com/legal/terms (01.05.2017)
114. Hynes L.; Privacy Shield – lipstick on a pig?; Leman Solicitors 11.03.2016; kättesaadav: http://thoughtleadership.leman.ie/post/102d8f1/privacy-shield-lipstick-on-a-pig (01.05.2017)
115. Jablonski C.; Data is the oil of 21st century: Gartnersupply chain exe; Trade Shift blog 15.05.2015; kättesaadav: http://blog.tradeshift.com/data-oil-21st-century-gartner-supply-chain-exec/ (01.05.2017)
116. Kayali L.; 26.01.2017 säuts; Twitter; kättesaadav: https://twitter.com/LauKaya/status/824674537803550721 (01.05.2017)
117. Liem C., G. Petropoulos; The economic value of personal data for online platforms, firms and consumers; Bruegel blog 14.01.2016; kättesaadav: http://bruegel.org/2016/01/the-economic-value-of-personal-data-for-online-platforms-firms-and-consumers/ (01.05.2017)
118. Lomas N.; Trump order strips privacy rights from non-U.S. citizens, could nix EU-US data flows; TechCrunch 26.01.2017; kättesaadav:

https://techcrunch.com/2017/01/26/trump-order-strips-privacy-rights-from-non-u-s-citizens-could-nix-eu-us-data-flows/ (01.05.2017)

119. McGinnis K.; President Obama Signs New Privacy Law – Judicial Redress Act; JDSupra 04.03.2016; kättesaadav: http://www.jdsupra.com/legalnews/president-obama-signs-new-privacy-law-59057/ (01.05.2017)
120. Palmer M.; Data is the new oil; ANA Marketing Maestros blog, 03.11.2006; kättesaadav: http://ana.blogs.com/maestros/2006/11/data_is_the_new.html (01.05.2017)
121. Rotella P.; Is data the new oil?; Forbes 02.04.2012; kättesaadav: http://www.forbes.com/sites/perryrotella/2012/04/02/is-data-the-new-oil/#2caf418677a9 (01.05.2017)
122. Sidahmed M., Yuhas A.; Is this a Muslim ban? Trump's executive order explained; The Guardian 31.01.2017; kättesaadav: https://www.theguardian.com/us-news/2017/jan/28/trump-immigration-ban-syria-muslims-reaction-lawsuits (01.05.2017)
123. Timberg C.; NSA slide shows surveillance of undersea cables; The Washington Post 10.07.2013; kättesaadav: https://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html (01.05.2017)
124. Toonders J.; Data is the new oil of digitaal economy; Wired; kättesaadav: http://www.wired.com/insights/2014/07/data-new-oil-digital-economy/ (01.05.2017)

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Carel Kivimaa

(sünnikuupäev 02.12.1990)

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „EUROOPA KOMISJONI RAKENDUSOTSUSE (EL) 2016/1250 KEHTIVUST MÕJUTAVAD OLULISED ARENGUD USA JA EUROOPA LIIDU ÕIGUSES“, mille juhendajateks on LL.M. Mati Kaalep ja J.S.D. Helen Eenmaa-Dimitrieva,

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tallinnas, **02.05.2017**