ARTIKLI 29 ALUSEL ASUTATUD ANDMEKAITSE TÖÖRÜHM

16/ET
WP 238

Arvamus 01/2016 ELi-USA andmekaitseraamistiku Privacy Shield piisavusotsuse eelnõu kohta

Vastu võetud 13. aprillil 2016

KOMMENTEERITUD KOKKUVÕTE

Euroopa Komisjon avaldas 29. veebruaril 2016 teatise, piisavusotsuse eelnõu ja lisad, mis moodustavad uue raamistiku isikuandmete Atlandi-üleseks vahetamiseks kaubanduslikel eesmärkidel. Sellele anti nimeks ELi-USA andmekaitseraamistik Privacy Shield (edaspidi „Privacy Shield“ või „raamistik“) ja sellega asendatakse varasem USA programm Safe Harbor, mille Euroopa Liidu Kohus tunnistas 6. oktoobril 2015 Schremsi kohtuasjas tehtud otsusega kehtetuks.

Vastavalt direktiivi 95/46/EÜ artikli 30 lõike 1 punktile c hindas artikli 29 alusel asutatud andmekaitse töörühm (edaspidi „artikli 29 töörühm“ või „töörühm“) nimetatud dokumente, et esitada oma arvamus piisavusotsuse eelnõu kohta. Artikli 29 töörühm hindas nii kaubandusaspekte kui ka Privacy Shieldi põhimõtete võimalikke erandeid, mis tehakse riikliku julgeoleku, õiguskaitse ja avaliku huvi eesmärgil.

Artikli 29 töörühm võttis arvesse direktiivis 95/46/EÜ sätestatud kohaldatavat ELi andmekaitse õigusraamistikku, samuti Euroopa inimõiguste konventsiooni artiklis 8 ning Euroopa Liidu põhiõiguste harta artiklites 7 ja 8 sõnastatud põhiõigust eraelule ja isikuandmete kaitsele. Samuti vaagis töörühm harta artiklis 47 sätestatud õigust tõhusale õiguskaitsevahendile ja õiglasele kohtulikule arutamisele ning eri põhiõigustega seotud kohtupraktikat.

Lisaks on analüüsis kajastatud Schremsi kohtuotsuses esitatud Euroopa Liidu Kohtu arutluskäiku, kus käsitletakse komisjoni kaalutlusõigust piisavuse hindamisel. Piisavusnõuete täitmist tuleb rangelt kontrollida, võttes arvesse eraelu ja andmekaitsega seotud põhiõigusi ning nende isikute arvu, keda andmete edastamine võib mõjutada.

Privacy Shieldi tuleb vaadelda praeguses rahvusvahelises kontekstis, näiteks suurandmete tekke ja kasvava julgeolekuvajaduse taustal. Isikuandmete kogumise ja kasutamise ulatus on märgatavalt suurenenud pärast programmi Safe Harbor käsitleva algse otsuse väljaandmist 2000. aastal Euroopa andmekaitseasutused kinnitavad jõuliselt enda kaitstavate põhimõtete tähtsust.

Kõigepealt väljendab artikli 29 töörühm heameelt oluliste täiustuste üle, mida Privacy Shield pakub võrreldes Safe Harbori otsusega. Töörühm märgib, et läbirääkimiste pidajad on kõrvaldanud palju programmi Safe Harbor puudusi, millele töörühm oli juhtinud tähelepanu oma 2014. aasta 10. aprilli kirjas asepresident Redingile.

Asjaolu, et Privacy Shieldi põhimõtted ja pakutavad tagatised on sätestatud nii piisavusotsuses kui ka selle lisades, muudab teabe raskesti leitavaks ja teinekord ebajärjekindlaks. See suurendab uue raamistiku üldist ebaselgust ning muudab andmesubjektide, organisatsioonide ja andmekaitseasutuste juurdepääsu raamistikule palju keerulisemaks. Samuti jääb selgusest puudu keelekasutuses. Seepärast kutsub artikli 29 töörühm komisjoni üles muutma andmekaitseraamistik selgeks ja arusaadavaks mõlemal pool Atlandi ookeani.

Seoses kohaldatava õigusega rõhutab artikli 29 töörühm, et kui Privacy Shieldi piisavusotsus võetakse direktiivi 95/46/EÜ alusel vastu, peavad nii selle kohaldamisala kui ka terminid olema kooskõlas ELi andmekaitse õigusraamistikuga. Artikli 29 töörühm leiab, et andmekaitseraamistik tuleks üsna pea pärast isikuandmete kaitse üldmääruse jõustumist läbi vaadata tagamaks, et piisavusotsuses ja selle lisades peetakse kinni määrusega pakutavast kõrgematasemelisest andmekaitsest.

Privacy Shieldi kaubandusaspektid

Artikli 29 töörühma põhieesmärk on tagada, et kui isikuandmeid töödeldakse Privacy Shieldi sätete alusel, säilib üksikisikutele sisuliselt samaväärne kaitse. Ehkki töörühm ei oota, et Privacy Shield oleks ELi õigusraamistiku pelk ja täielik koopia, leiab ta, et see peaks kajastama aluspõhimõtete olemust ja selle tulemusel tagama sisuliselt samaväärse kaitsetaseme.

Olenemata Privacy Shieldis sisalduvatest täiustustest, leiab artikli 29 töörühm, et mõni Euroopa õiguses visandatud oluline andmekaitsepõhimõte ei kajastu piisavusotsuse eelnõus ja lisades või on puudulikult asendatud alternatiivsete mõistetega.

Näiteks on andmete säilitamise põhimõte sõnaselgelt nimetamata jäänud ning seda ei ole võimalik kindlapiiriliselt tuletada ka andmete terviklikkuse ja eesmärgi piiramise põhimõtte praegusest sõnastusest. Peale selle ei ole kirjeldatud kaitset, mida tuleks pakkuda ainult automatiseeritud töötlemisel põhinevate automatiseeritud üksikotsuste eest. Samuti on ebaselge eesmärgi piiramise põhimõtte kohaldamine andmetöötluse suhtes. Et tuua mitme tähtsa mõiste kasutamisse rohkem selgust, soovitab artikli 29 töörühm ELil ja USA-l kokku leppida selgetes määratlustes ning kanda need terminite loetellu, mis lisatakse Privacy Shieldi kohta käivatele korduma kippuvatele küsimustele.

Kuna Privacy Shieldi kasutatakse ka andmete edastamiseks väljapoole USAd, toonitab artikli 29 töörühm, et andmete edasisaatmisel raamistikuga hõlmatud üksuselt kolmanda riigi vastuvõtjatele tuleks tagada kõikide raamistiku aspektide (sh riiklik julgeolek) samatasemeline kaitse ning selline andmete edasisaatmine ei tohiks kaasa tuua ELi andmekaitsepõhimõtete nõrgenemist ega nendest kõrvalehoidmist. Kui Privacy Shieldi raames on kavandatud andmete edasisaatmine kolmandale riigile, peaks igal raamistiku alusel tegutseval organisatsioonil olema kohustus hinnata enne andmete edasisaatmist andmeimportija suhtes kohaldatavaid kolmanda riigi õigusaktide kohustuslikke nõudeid. Artikli 29 töörühm on jõudnud järeldusele, et ELi isikuandmete edasisaatmist, eriti nende andmete ulatust, eesmärgi piiramist ja tagatisi, mida kohaldatakse andmete edastamisel esindajatele, reguleeritakse üldjuhul ebapiisavalt.

Lõpetuseks – ehkki artikli 29 töörühm võtab teadmiseks lisamehhanismid, mida üksikisikud saavad oma õiguste teostamiseks kasutada – tunneb ta muret selle pärast, et uus õiguskaitsemehhanism võib osutuda praktikas ELi üksikisikutele kasutamiseks liiga keeruliseks ja seega ebatõhusaks. Seepärast tuleb erinevaid kaebuste käsitlemise menetlusi lähemalt selgitada. Eelkõige võiksid ELi andmekaitseasutused – kui nad selleks valmis on –

olla eri menetlustes ELi üksikisikute endastmõistetavad kontaktpunktid, kellel on võimalus nende nimel tegutseda.

Riikliku julgeoleku huvides tehtavad erandid

Seoses avaliku sektori asutuste juurdepääsuga andmetele nii ELis kui ka kolmandates riikides tuletab artikli 29 töörühm meelde oma analüüsi, mis hõlmab asjakohaseid põhiõigusi ja asub töödokumendis, milles on käsitletud eraelu ja andmekaitsega seotud põhiõigustesse sekkumise põhjendatust juhul, kui isikuandmete edastamisel rakendatakse jälgimismeetmeid (Euroopa olulised tagatised) (WP 237).

Safe Harbori otsusest suur samm edasi on see, et piisavusotsuse eelnõus on käsitletud ulatuslikult võimalikku juurdepääsu Privacy Shieldi alusel töödeldavatele andmetele riikliku julgeoleku ja õiguskaitse eesmärgil. Artikli 29 töörühm tunnistab seda märkimisväärset sammu ja USA valitsuse pakutud suuremat läbipaistvust luureandmete kogumisel kohaldatavate õigusaktide suhtes (VI lisa).

Siiski märgib töörühm, et USA riikliku luurejuhi ameti kinnitustes ei välistata EList pärit isikuandmete massilist ja valimatut kogumist. Artikli 29 töörühm tuletab meelde oma kauaaegset seisukohta, et üksikisikute massilist ja valimatut jälgimist ei saa kunagi pidada proportsionaalseks ja demokraatlikus ühiskonnas hädavajalikuks, nagu seda nõutakse kohaldatavate põhiõigustega tagatud kaitse puhul. Peale selle on üliolulisel kohal kõikide jälgimisprogrammide põhjalik järelevalve. Töörühm võtab teadmiseks asjaolu, et terrorismivastase võitluse taustal levib suundumus koguda massiliselt ja valimatult veelgi rohkem teavet. Võttes arvesse probleeme, mida see tekitab eraelu puutumatuse ja andmekaitsega seotud põhiõiguste kaitsmisel, ootab töörühm huviga Euroopa Liidu Kohtu peatseid otsuseid andmete massilise ja valimatu kogumisega seotud kohtuasjades.

Õiguskaitse vallas valmistab artikli 29 töörühmale rõõmu ombudsmani kui uue õiguskaitsemehhanismi kasutuselevõtt. See võib tähendada ELi üksikisikute õiguste märkimisväärset suurenemist USA luuretegevuse puhul. Ometi tunneb töörühm muret, et see uus institutsioon ei ole piisavalt sõltumatu, et sellele ei ole antud oma ülesannete tõhusaks täitmiseks piisavaid volitusi ja et see ei taga lahkarvamuse korral rahuldavat õiguskaitsevahendit.

Ühine läbivaatamine

Piisavusotsuse eelnõus nimetatud iga-aastase ühise läbivaatamise mehhanism on Privacy Shieldi üldise usaldusväärsuse seisukohast väga oluline ja artikli 29 töörühmal on väga hea meel võimaluse üle piisavusotsus läbi vaadata. Artikli 29 töörühm mõistab, et töörühma liikmesriikidest pärit esindajad saavad kõnealuses läbivaatamises igati osaleda, kuid palub selgitada läbivaatamise täpset korraldust. Üksikasjades (sh koostatav aruanne, selle avalikustamine ja võimalikud tagajärjed, samuti rahastamine) tuleb kokku leppida aegsasti enne esimest läbivaatamist.

Järeldus

Artikli 29 töörühm on tähele pannud suuri täiustusi, mida Privacy Shield pakub võrreldes programmi Safe Harbor käsitleva kehtetuks tunnistatud otsusega. Seoses väljendatud murede ja palutud selgitustega kutsub töörühm komisjoni üles neid muresid leevendama, tegema kindlaks sobivad lahendused ja esitama soovitud selgitused, et piisavusotsuse eelnõu täiustada ja kanda hoolt selle eest, et Privacy Shieldiga tagatav kaitse oleks tõepoolest sisuliselt samaväärne ELi pakutava kaitsega.

SISUKORD

KOMMENTEERITUD KOKKUVÕTE 2

PRIVACY SHIELDI KAUBANDUSASPEKTID 3
RIIKLIKU JULGEOLEKU HUVIDES TEHTAVAD ERANDID 4
ÜHINE LÄBIVAATAMINE 4
JÄRELDUS 5

SISUKORD 6

1. SISSEJUHATUS 8

1.1. ÜLDISED MÄRKUSED 9
1.1.1. ARTIKLI 39 TÖÖRÜHMA HINNANGU ULATUS 9
1.1.2. PIISAVUSOTSUSE EELNÕU KAUBANDUSLIKU OSA HINDAMINE 9
1.1.3. AVALIKU SEKTORI ASUTUSTE JUURDEPÄÄSUL KOHALDATAVATE ERANDITE JA NENDEGA SEOTUD KAITSEMEETMETE HINDAMINE 10
1.2. PIISAVUSOTSUSE EELNÕU 11
1.2.1. ELI ANDMEKAITSERAAMISTIKU JA EELKÕIGE DIREKTIIVI 95/46/EÜ PÕHIMÕTETE KOHALDAMISALA 11
1.2.2. PRIVACY SHIELDI DOKUMENTIDE EBASELGUS 11
1.2.3. ÜHINE LÄBIVAATAMINE JA PEATAMINE 13
1.2.4. ELI ÕIGUSRAAMISTIKU LÄBIVAATAMINE 14

2. PIISAVUSOTSUSE EELNÕU KAUBANDUSLIKU OSA HINDAMINE 14

2.1. ÜLDISED MÄRKUSED 14
2.1.1. TÄIUSTUSED 14
2.1.2. PRIVACY SHIELDI KOHALDAMINE VOLITATUD TÖÖTLEJANA TEGUTSEVATE ORGANISATSIOONIDE (ESINDAJATE) SUHTES 15
2.1.3. PÕHIMÕTETE JÄRGIMISE KOHUSTUSE PIIRANGUD 16
2.1.4. ISIKUANDMETE SÄILITAMISE PIIRAMISE PÕHIMÕTTE PUUDUMINE 16
2.1.5. TAGATISTE PUUDUMINE AUTOMATISEERITUD OTSUSTE PUHUL, MILLEL ON ÕIGUSLIKUD TAGAJÄRJED VÕI MÄRKIMISVÄÄRNE MÕJU ÜKSIKISIKULE 16
2.1.6. OLEMASOLEVATE KAUBANDUSSIDEMETE PUHUL KOHALDATAV ÜLEMINEKUAEG 17
2.2. KONKREETSED MÄRKUSED 17
2.2.1. LÄBIPAISTVUS 17
2.2.2. VALIKUVÕIMALUS 18
2.2.3. EDASISAATMINE 19
2.2.4. ANDMETE TERVIKLIKKUS JA EESMÄRGI PIIRAMINE 23
2.2.5. ANDMESUBJEKTIDE JUURDEPÄÄSUÕIGUS NING ÕIGUS ANDMETE PARANDAMISELE JA KUSTUTAMISELE 25
2.2.6. KAEBUSTE MENETLEMINE, TÄITMISE TAGAMINE JA VASTUTUS (ÕIGUSKAITSEMEHHANISM) 26
2.2.7. PERSONALIANDMETE TÖÖTLEMINE 30
2.2.8. FARMAATSIA- JA MEDITSIINITOOTED 32
2.2.9. AVALIKULT KÄTTESAADAV TEAVE 34
2.3. JÄRELDUSED 34

3. PIISAVUSOTSUSE EELNÕU RIIKLIKU JULGEOLEKUGA SEOTUD TAGATISTE HINDAMINE 34

3.1. USA RIIKLIKE JULGEOLEKUASUTUSTE SUHTES KOHALDATAVAD KAITSEMEETMED JA PIIRANGUD 34
3.2. TAGATIS A. TÖÖTLEMINE PEAB TOIMUMA KOOSKÕLAS ÕIGUSAKTIDEGA NING PÕHINEMA SELGETEL, TÄPSETEL JA LIGIPÄÄSETAVATEL EESKIRJADEL 35
3.2.1. KORRALDUS 12333 JA PRESIDENDI POLIITIKASUUNIS NR 28 36
3.2.2. VÄLISLUURE JÄLITUSTEGEVUSE SEADUS 37

3.2.3. JÄRELDUSED 38
3.3. TAGATIS B. TÕESTADA TULEB VAJALIKKUST JA PROPORTSIONAALSUST TAOTLETAVATE ÕIGUSPÄRASTE EESMÄRKIDE VAATENURGAST 39
3.3.1. PRESIDENDI POLIITIKASUUNIS NR 28 39
3.3.2. VÄLISLUURE JÄLITUSTEGEVUSE SEADUS 39
3.3.3. JÄRELDUSED 41
3.4. TAGATIS C. OLEMAS PEAKS OLEMA SÕLTUMATU JÄRELEVALVEMEHHANISM 41
3.4.1. SISEJÄRELEVALVE 41
3.4.2. VÄLISJÄRELEVALVE 42
3.4.3. JÄRELDUSED 44
3.5. TAGATIS D. ÜKSIKISIKULE PEAVAD OLEMA KÄTTESAADAVAD TÕHUSAD ÕIGUSKAITSEVAHENDID 44
3.5.1. KOHTULIKUD ÕIGUSKAITSEVAHENDID 44
3.5.1.1. KAEBEÕIGUSE NÕUE 44
3.5.1.2. PRESIDENDI POLIITIKASUUNIS NR 28 45
3.5.1.3. VÄLISLUURE JÄLITUSTEGEVUSE SEADUS 45
3.5.2. HALDUSLIKUD ÕIGUSKAITSEVAHENDID 45
3.5.2.1. PEAINSPEKTORID 45
3.5.2.2. TEABEVABADUSE SEADUS 46
3.5.3. PRIVACY SHIELDI OMBUDSMAN 46
3.5.3.1. OMBUDSMANI MEHHANISMI KASUTUSELEVÕTT 46
3.5.3.2. UUE OMBUDSMANI MEHHANISMI HINDAMINE 47
3.5.3.3. KAS PELGALT OMBUDSMANI MEHHANISMI KASUTUSELEVÕTUST PIISAB? 47
3.5.3.4. OMBUDSMANI MEHHANISMI KOHALDAMISALA 49
3.5.3.5. KAEBEÕIGUS JA TAOTLUSE MENETLEMINE 49
3.5.3.6. SÕLTUMATUS 50
3.5.3.7. UURIMISVOLITUSED 51
3.5.3.8. HEASTAMISVOLITUSED 52
3.5.4. JÄRELDUSED 52
3.6. KOKKUVÕTVAD MÄRKUSED USA RIIKLIKE JULGEOLEKUASUTUSTE SUHTES KOHALDATAVATE KAITSEMEETMETE JA PIIRANGUTE KOHTA 53

4. PRIVACY SHIELDI ÕIGUSKAITSETAGATISTE HINDAMINE 53

4.1. SISSEJUHATUS 53
4.2. EUROOPA OLULISTE TAGATISTE KOHALDAMINE ÕIGUSKAITSEASUTUSTE JUURDEPÄÄSUL ETTEVÕTETE KÄSUTUSES OLEVATELE ANDMETELE 54
4.2.1. ÕIGUSKAITSEAUSTUSTE JUURDEPÄÄS ISIKUANDMETELE PEAB OLEMA KOOSKÕLAS ÕIGUSAKTIDEGA NING PÕHINEMA SELGETEL, TÄPSETEL JA LIGIPÄÄSETAVATEL EESKIRJADEL 54
4.2.2. TÕESTADA TULEB VAJALIKKUST JA PROPORTSIONAALSUST TAOTLETAVATE ÕIGUSPÄRASTE EESMÄRKIDE VAATENURGAST 54
4.2.3. OLEMAS PEAKS OLEMA SÕLTUMATU JÄRELEVALVEMEHHANISM 56
4.2.4. ÜKSIKISIKULE PEAVAD OLEMA KÄTTESAADAVAD TÕHUSAD ÕIGUSKAITSEVAHENDID 56
4.3. KOKKUVÕTVAD MÄRKUSED 57

5. JÄRELDUSED JA SOOVITUSED 58

5.1. KOLM MUREKÜSIMUST 58
5.2. SOOVITUSLIKUD SELGITUSED 59

1. SISSEJUHATUS

Pärast Euroopa Liidu Kohtu 6. oktoobri 2015. aasta otsust Schremsi kohtuasjas[1] kutsus artikli 29 alusel asutatud andmekaitse töörühm (edaspidi „artikli 29 töörühm“ või „töörühm“) Euroopa Liidu (edaspidi „EL“) liikmesriike ja teisi Euroopa institutsioone üles alustama arutelusid Ameerika Ühendriikide (edaspidi „USA“) ametiasutustega, et leida poliitilised, õiguslikud ja tehnilised lahendused, mis võimaldavad edastada andmeid USA territooriumile viisil, mille puhul austatakse põhiõigusi.

2. veebruaril 2016, pärast enam kui kaks aastat kestnud läbirääkimisi, saavutasid Euroopa Komisjon ja Ameerika Ühendriikide kaubandusministeerium (edaspidi „kaubandusministeerium“) poliitilise kokkuleppe seoses uue raamistikuga Atlandi-üleseks isikuandmete vahetamiseks kaubanduslikel eesmärkidel, mis sai nimeks ELi-USA andmekaitseraamistik Privacy Shield (edaspidi „Privacy Shield“ või „raamistik“) ja millega asendati varasem USA programm Safe Harbor.

29. veebruaril 2016 avaldas komisjon teatise,[2] piisavusotsuse eelnõu ja lisad, mis moodustavad Privacy Shieldi. Vastavalt direktiivi 95/46/EÜ (edaspidi „direktiiv“) artikli 30 lõike 1 punktile c hindas artikli 29 töörühm nimetatud dokumente, et esitada oma arvamus komisjoni koostatud piisavusotsuse eelnõu, sealhulgas selle aluseks olevate Privacy Shieldi dokumentide kohta. Selle käigus hindas artikli 29 töörühm Privacy Shieldi kaubanduslikku osa ning analüüsis kaitsemeetmeid, mis on kehtestatud seoses raamistiku põhimõtete eranditega riikliku julgeoleku, õiguskaitse ja avaliku huvi eesmärgil.

Artikli 29 töörühm on pidanud pärast Schremsi kohtuotsust mitu kohtumist USA valitsuse delegatsioonidega, nii ELi kui ka USA kodanikuühiskonna organisatsioonide esindajatega ja teadlastega, et koostada hinnang Schremsi kohtuotsuse tagajärgede kohta. Privacy Shieldi hindamise ajal on toimunud lisakohtumised Euroopa Komisjoni ja USA valitsuse esindajatega. Nendel kohtumistel on saadud mõningaid selgitusi, mida on samuti käesolevas arvamuses arvesse võetud. Töörühm rõhutab, et praeguses etapis on need selgitused olnud üksnes mitteametlikud ja neid ei saa käsitada piisavusotsuse eelnõu lahutamatu osana, sest neid ei ole veel kirja pandud.

Sellegipoolest on artikli 29 töörühmal iseäranis hea meel selle üle, et kaubandusministeerium võttis neil kohtumistel kohustuse teha Privacy Shieldi kohaldamise küsimustes koostööd ELi liikmesriikide andmekaitseasutustega ning avaldada oma veebisaitidel raamistiku kohaldamise juhiseid ja õiguslikke tõlgendusi.

[1] Kohtuotsus, Euroopa Kohus, 6.10.2015, Maximilian Schrems *vs.* Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650 (edaspidi „Schremsi kohtuotsus“).
[2] COM(2016) 117 final, 29. veebruar 2016.

1.1. Üldised märkused

1.1.1. Artikli 29 töörühma hinnangu ulatus

Artikli 29 töörühm võttis eelkõige arvesse ELi liikmesriikides kohaldatavat andmekaitseraamistikku, sealhulgas Euroopa inimõiguste konventsiooni (edaspidi „inimõiguste konventsioon“) artiklit 8, millega kaitstakse õigust era- ja perekonnaelu austamisele, ning Euroopa Liidu põhiõiguste harta (edaspidi „harta“) artikleid 7, 8 ja 47, millega kaitstakse vastavalt õigust era- ja perekonnaelu austamisele, õigust isikuandmete kaitsele ning õigust tõhusale õiguskaitsevahendile ja õiglasele kohtulikule arutamisele. Samuti võttis töörühm arvesse asjakohast kohtupraktikat ja direktiivi nõudeid.

Kolmandale riigile kehtestatud nõuet tagada andmekaitse piisav tase on Euroopa Liidu Kohus üksikasjalikumalt määratlenud Schremsi kohtuasjas tehtud otsuses. Kohus selgitab, et direktiivi sätete tõlgendamisel tuleb „lähtuda hartaga tagatud põhiõigustest“,[3] eelkõige artiklitest 7 ja 8. Ent peale selle märgib kohus veel, et väljendit „kaitse piisav tase“ tuleb mõista nii, et see „nõuab, et kolmas riik tõepoolest tagab oma siseriikliku õigusega või endale võetud rahvusvaheliste kohustustega põhiõiguste ja -vabaduste kaitse taseme, mis on sisuliselt samaväärne sellega, mis on liidus tagatud vastavalt direktiivile 95/46 koostoimes hartaga“[4]. Endise programmi Safe Harbor käsitleva otsuse puhul ei ole sellist hindamist kunagi piisavalt üksikasjalikult tehtud. Seepärast hindas artikli 29 töörühm piisavusotsuse eelnõu, pidades silmas nõuet analüüsida, kas põhiõiguste ja -vabaduste kaitse tase on *sisuliselt samaväärne* sellega, mis on tagatud ELis. Töörühm rõhutab, et käesolevas arvamuses on kajastatud töörühma peamisi muresid, ent kuna piisavusotsuse eelnõu avaldamisest on möödunud vähe aega, võidakse hiljem avastada lisaprobleeme.

Artikli 29 töörühm tunnistab, et andes direktiivi artikli 25 lõikes 6 kasutatud sõnale „piisav“ tähenduse „sisuliselt samaväärne“, määratles Euroopa Liidu Kohus Schremsi kohtuotsuses piisavuse mõistet veelgi üksikasjalikumalt. Kohus toonitab, et väljendit „kaitse piisav tase“ – ehkki sellega ei nõuta, et kolmas riik tagaks kaitsetaseme, mis on ELi õiguskorras tagatuga identne – tuleb mõista nii, et see nõuab, et kolmas riik tõepoolest tagab oma siseriikliku õigusega või endale võetud rahvusvaheliste kohustustega põhiõiguste ja -vabaduste kaitse taseme, mis on *sisuliselt samaväärne* sellega, mis on liidus tagatud vastavalt direktiivile 95/46 koostoimes hartaga.

1.1.2. Piisavusotsuse eelnõu kaubandusliku osa hindamine

Seda, kuidas artikli 29 töörühm kohaldab peamisi ELi andmekaitsepõhimõtteid isikuandmete edastamisel kolmandatele riikidele, on ta selgitanud juba oma töödokumendis nr 12 „Isikuandmete edastamine kolmandatele riikidele – ELi andmekaitsedirektiivi artiklite 25 ja 26 kohaldamine“[5]. Töörühm püüdis leida samaväärsed kaitsemeetmed, mis tagavad direktiivi põhimõtetega samaväärse kaitsetaseme, eriti kui need hõlmavad eesmärgi piiramist, andmete

[3] Schremsi kohtuotsus, punkt 38.
[4] Schremsi kohtuotsus, punkt 73.
[5] Vastu võetud 24. juulil 1998, vt eeskätt lk 6.

kvaliteeti ja proportsionaalsust, läbipaistvust, turvalisust, juurdepääsuõigust, andmete parandamist ja töötlemisele vastu seismist, andmete säilitamist ja nende edasisaatmise piiranguid. Sarnast meetodit on kasutatud arvamustes, mille töörühm andis välja programmi Safe Harbor piisavust käsitleva algse otsuse hindamise ajal,[6] ning soovitustes, mille töörühm esitas 10. aprillil 2014 avaldatud kirjas Euroopa Komisjoni endisele asepresidendile ja õigusküsimuste volinikule Vivian Redingile[7].

1.1.3. Avaliku sektori asutuste juurdepääsul kohaldatavate erandite ja nendega seotud kaitsemeetmete hindamine

Erandeid, mida kohaldatakse avaliku sektori asutuste juurdepääsul Privacy Shieldiga hõlmatud isikuandmetele, on keeruline hinnata, eriti kui võtta arvesse andmekaitseasutuste ja üldsuse suurenenud teadlikkust USA jälgimisprogrammidest pärast Snowdeni paljastusi. Artikli 29 töörühm avaldab USA valitsusele tunnustust püüdluste eest suurendada jälgimisprogrammide läbipaistvust ja valmisoleku eest lisada Privacy Shieldi uued kaitsemeetmed. Samal ajal rõhutab töörühm, et igasugune sekkumine eraelu ja andmekaitsega seotud põhiõigustesse peab olema demokraatlikus ühiskonnas põhjendatav. Euroopa Liidu Kohus on kritiseerinud asjaolu, et Safe Harbori otsus ei sisaldanud mingeid järeldusi selle kohta, kas Ameerika Ühendriikides kehtib riigi tasandil õigusnorme, mille eesmärk oleks piirata võimalikke sekkumisi. Pealegi ei ilmne otsusest, et sedalaadi sekkumiste vastu oleks olemas tõhus õiguslik kaitse[8].

Seepärast on artikli 29 töörühm analüüsinud praegust USA õigusraamistikku, otsuse eelnõu lisades kirjeldatud USA luureasutuste tavasid ja tingimusi, mille alusel need võimaldavad sekkumist Euroopa õigusraamistiku alusel kaitstud põhiõigustesse eraelu austamisele ja andmekaitsele.

Et teha kindlaks, kas mingit laadi sekkumine oleks demokraatlikus ühiskonnas põhjendatav, võeti hindamisel arvesse põhiõiguste alast Euroopa kohtupraktikat, milles on sätestatud luuretegevuse kohta neli olulist tagatist[9].

A. Töötlemine peab toimuma kooskõlas õigusaktidega ning põhinema selgetel, täpsetel ja ligipääsetavatel eeskirjadel – iga mõistlikult teavitatud isik peaks suutma ette näha, mis juhtub tema andmetega, kui neid edastatakse.
B. Tõestada tuleb vajalikkust ja proportsionaalsust taotletavate õiguspäraste eesmärkide vaatenurgast – andmete kogumise ja andmetele juurdepääsu eesmärgi ning üksikisiku õiguste vahel tuleb leida tasakaal.
C. Olemas peaks olema sõltumatu järelevalvemehhanism, mis on nii tõhus kui ka erapooletu – selleks võib olla kas kohtunik või mõni muu sõltumatu organ, kellel on piisav võime teha vajalikku kontrolli.

[6] Vt WP62, WP32, WP27, WP23, WP21, WP19, WP15 ja WP7.
[7] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf.
[8] Schremsi kohtuotsus, punktid 87 ja 88.
[9] Euroopa olulised tagatised põhinevad Euroopa Liidu Kohtu ja Euroopa Inimõiguste Kohtu praktikal ning neid on kirjeldatud üksikasjalikumalt artikli 29 töörühma töödokumendis WP 237, mis avaldati 13. aprillil 2016.

D. Üksikisikule peavad olema kättesaadavad tõhusad õiguskaitsevahendid – igaühel peaks olema õigus kaitsta oma õigusi sõltumatu organi ees.

1.2. Piisavusotsuse eelnõu

Artikli 29 töörühm tunneb eelkõige heameelt selle üle, et uue piisavusmenetluse saab algatada vähem kui kuus kuud pärast seda, kui Euroopa Liidu Kohtus tunnistas Safe Harbori otsuse kehtetuks. Võttes arvesse seda, kui mahukas on ELi ja USA vaheline igapäevane andmeedastus, mis on töörühma kinnitusel majanduse oluline osa mõlemal pool Atlandi ookeani, on õiguslikku selgust vaja pigem varem kui hiljem.

Siiski avaldab artikli 29 töörühm kahetsust, et komisjoni avaldatud piisavusotsuse eelnõu ei sisalda piisavusaruande vormis USA riigisisese õiguse ja rahvusvaheliste kohustuste põhjalikku hinnangut, mille koostamine on olnud sarnaste menetluste puhul ja kooskõlas direktiivi artikliga 25 varem tavaks. See ei ole lasknud töörühmal analüüsida täiel määral õiguslikku konteksti, milles Privacy Shield hakkab toimima. Näiteks märgib töörühm, et praegune piisavusotsuse eelnõu ei sisalda järeldusi nii föderaalsel kui ka osariigi tasandil olemasolevate eraelu puutumatuse ja andmekaitse alaste USA õigusaktide, sealhulgas valdkondlikke õigusaktide kohta, samuti õigusaktide kohta, mis võimaldavad avalikku juurdepääsu muus kui jälgimise vormis. Samuti ei ole kindlaks määratud, milline on seos Privacy Shieldi kaudu toimuva andmeedastuse ning selle andmeedastuse vahel, mis leiab aset muude olemasolevate, näiteks ELi ja USA vahelist broneeringuinfo vahetamise lepingut ning terrorismi rahastamise jälgimise programmi käsitlevate piisavusotsuse raames.

1.2.1. ELi andmekaitseraamistiku ja eelkõige direktiivi 95/46/EÜ põhimõtete kohaldamisala

Artikli 29 töörühm tuletab meelde, et ELi andmekaitse õigusraamistiku ja eeskätt direktiivi (artikli 4 lõige 1) alusel ei kohaldata liikmesriikide õigusakte üksnes liikmesriikide territooriumil registreeritud vastutavate töötlejate teostatavate töötlemistoimingute suhtes, vaid ka juhul, kui vastutavad töötlejad (kuigi nad ei ole registreeritud ELi territooriumil) kasutavad ELi territooriumil paiknevaid vahendeid, eelkõige isikuandmete kogumiseks. Seetõttu kohaldatakse ELi liikmesriikide õigusakte igasuguse töötlemise suhtes, mis toimub enne andmete edastamist USAsse kas ELis registreeritud organisatsiooni tegevuse raames või ELis paiknevate vahendite kasutamisel organisatsiooni poolt, kes ei ole ELis registreeritud. Artikli 29 töörühm soovib, et see oleks piisavusotsuse eelnõus sõnaselgelt sätestatud.

Peaks olema selge, et Privacy Shieldi põhimõtteid kohaldatakse alates hetkest, mil toimub andmete edastamine. Lisaks tuletab artikli 29 töörühm meelde, et ELis registreeritud volitatud töötlejate suhtes, kes edastavad andmeid volitatud töötlejale USAs, kohaldatakse ELi andmekaitseõigust.

1.2.2. Privacy Shieldi dokumentide ebaselgus

Asjaolu, et Privacy Shieldi põhimõtted ja pakutavad tagatised on sätestatud nii piisavusotsuses kui ka selle lisades, muudab teabe raskesti leitavaks ja teinekord ebajärjekindlaks. See suurendab uue raamistiku üldist ebaselgust ning muudab

andmesubjektide, organisatsioonide ja andmekaitseasutuste juurdepääsu raamistikule palju keerulisemaks. Samuti jääb selgusest puudu keelekasutuses. Seepärast kutsub artikli 29 töörühm komisjoni üles muutma andmekaitseraamistik selgeks ja arusaadavaks mõlemal pool Atlandi ookeani.

Artikli 29 töörühm teeb ettepaneku koostada eraldi lisa, kus oleksid määratletud Privacy Shieldi dokumentides kasutatavad põhimõisted. Ühine ja ühene arusaam Privacy Shieldi piisavusotsusega kehtestatud kohustustest on oluline selleks, et raamistik toimiks tõhusalt mõlemal pool Atlandi ookeani. Töörühm muretseb sellepärast, et arvukate ristviidete, kooskõlastamata sõnastuse ja raamdokumentide keerukuse tõttu tekivad raskused raamistiku järjepideva, arusaadava ja selge rakendamisega.

Veelgi olulisem on see, et Privacy Shieldi dokumentides kasutatakse termineid, mis ei ole kooskõlas ELis andmekaitsega tegelemisel üldjuhul kasutatava sõnavaraga. See ei pruugi olla ilmtingimata probleem, kui on selge, millised on vastavad terminid ELi (ja USA) õiguses. Töörühmal tuleb kahetsusega märkida, et nii see paraku ei ole, sealhulgas piisavusotsuse eelnõus. Näiteks sõna „juurdepääs“ on kasutatud piisavusotsuse eelnõu 3. peatükis tähenduses, mis viitab isikuandmete kogumisele, mitte sellele, et kellelgi võimaldatakse näha juba kogutud andmeid. Äriühingute juurdepääs andmetele ja üksikisiku juurdepääsuõigus on kaks eri mõistet, mida ei tohiks omavahel segamini ajada.

Artikli 29 töörühm rõhutab, et termineid tuleks kasutada järjekindlalt ka dokumentides endis, sealhulgas piisavusotsuse eelnõus. Praegu seda ei tehta, näiteks mõistete „töötlemine“ ja „isikuandmed“ puhul. Mõlemad mõisted on põhimõtteliselt II lisas põhjalikult määratletud, kuid dokumentides ei kasutata neid järjepidevalt, mistõttu tekivad kaitses lüngad[10,11].

Artikli 29 töörühmal on hea meel, et mõne kasutatud mõiste määratlus on Privacy Shieldi moodustavatesse dokumentidesse lisatud. Paraku ei ole seda tehtud mitme teise olulise mõiste, sealhulgas „esindaja“ või „volitatud töötleja“, „kodeeritud andmete“, „anonüümseks muudetud andmete“ ja „ELi üksikisiku“ puhul, mille määratlemine tagaks töörühma meelest selge arusaama sellest, milles USA ja EL on kokku leppinud, vältimaks hilisemas etapis segadust Privacy Shieldi kasutavate vastutavate ja volitatud töötlejate ning järelevalveasutuste

[10] Mõnes sättes on loetletud üksnes mõni andmetöötlustoimingute liik, selle asemel et kasutada terminit „töötlemine“. Selle tagajärg on puudulik kaitse. Nt II lisa jao III.6.f sõnastuse kohaselt kohaldatakse Privacy Shieldi põhimõtteid üksnes juhul, kui organisatsioon „säilitab, kasutab või avalikustab“ saadud andmeid (st mitte muude mõistega „töötlemine“ hõlmatud toimingute puhul, nagu kogumine, salvestamine, muutmine, väljavõtete tegemine, järelepärimise teostamine ja kustutamine). Andmete turvalisuse tagamise meetmeid tuleb rakendada üksnes organisatsioonidel, kes „säilitavad, kasutavad või levitavad“ isikuandmeid (II lisa jagu II.4). Samuti hõlmab isikuandmete mõiste määratlus vaid andmeid, mille organisatsioon „saab“ ja „salvestab“. Veel on teate põhimõtte (II lisa jagu II.1.a.iv) kirjeldamisel näiteks öeldud, et põhimõtete järgimist kinnitanud organisatsioonid peavad andma üksikisikutele teada, millised on „nende isikuandmete kogumise ja kasutamise eesmärgid“. II lisa jaos III.9.a.ii on öeldud, et raamistiku põhimõtted on asjakohased pelgalt andmete „edastamisel“ või neile „juurdepääsul“. Isegi kui selgub, et enamikul sellistel juhtudel ei ole olnud kavas piirata põhimõtete kohaldamisala ega tekitada kaitses lünkasid, kaasneb ebajärjekindlate terminitega selliste lünkade tekkimise oht. Kuna töötlemise mõiste on põhimõtete all määratletud, on oluline kasutada seda järjekindlalt, et vältida praegu esinevaid lünki. Vastasel juhul jääb liiga palju ruumi otsuse sõnastuse eeldatavasti tahtmatu väärtõlgendamise jaoks.

[11] II lisa jaos I.8.a esitatud isikuandmete määratluses on kasutatud väljendit „identifitseeritud või identifitseeritava üksikisiku kohta käivad [---] andmed“. Täienduspõhimõtetes on aga öeldud, et seoses personaliandmetega kohaldatakse neid põhimõtteid üksnes „tuvastatavate registriandmete edastamisel või neile juurdepääsul“. Artikli 29 töörühm leiab, et sellega avaneb võimalus töödelda isikuandmeid viisil, mis ei ole kooskõlas ELi õiguse kohaste andmekaitsepõhimõtetega ega Privacy Shieldi üldise isikuandmete määratlusega.

ja üldsuse seas. Lihtne lahendus oleks lisada Privacy Shieldi korduma kippuvate küsimuste juurde mõistete loetelu.

Artikli 29 töörühm juhib tähelepanu ka 1. täienduspõhimõtte all (II lisa jagu III.1) nimetatud tundlike andmete töötlemise õiguslikele alustele olukorras, kus organisatsioon ei ole kohustatud hankima sõnaselget nõusolekut (*opt in*). 1. täienduspõhimõtet võib käsitada ELis andmete kogumise õiguslike aluste üksikasjaliku kirjeldusena, sest see loetelu sarnaneb direktiivi artikliga 8. Töörühm soovib meelde tuletada, et igasugune tundlike andmete töötlemine (sh kogumine ja edastamine) peab ELi õiguse kohaselt toimuma vastavalt direktiivi artiklile 8 õiguslikel alustel. Privacy Shieldi ei saa tõlgendada vahendina, mis pakub selliseks töötlemiseks muid aluseid. Töörühma meelest ei ole näiteks mõnel USA organisatsioonil võimalik koguda ELi õigusega reguleeritud andmeid USA tööõiguse alusel (II lisa jagu III.1.a.v). Seepärast rõhutab töörühm, et igasugune 1. täienduspõhimõtte tõlgendamine võib kaasa tuua üksnes selle põhimõtte kohaldamise tundlike andmete suhtes, mis on pärast direktiivi artiklis 8 loetletud õiguslikel alustel toimunud kogumist ELis juba edastatud.

Lõpetuseks juhib artikli 29 töörühm tähelepanu selguse puudumisele küsimuses, keda saab pidada ELi üksikisikuks ja kellele saab seega osaks Privacy Shieldi kohane kaitse – kas kõikidele ELi kodanikele või kõikidele ELis elavatele isikutele. See on eriti tähtis seoses õigusega õiguskaitsele, sh juurdepääsuga ombudsmani mehhanismile. Peale selle tuleks piisavusotsuses käsitleda küsimust, mil määral kohaldatakse Privacy Shieldi EMP riikide ja Šveitsi kodanikele/elanikele, kes ei olnud varem programmiga Safe Harbor hõlmatud.

1.2.3. Ühine läbivaatamine ja peatamine

Artikli 29 töörühmal on hea meel, et Euroopa Komisjon ja USA valitsus on leppinud kokku Privacy Shieldi praktilise kohaldamise korrapärases läbivaatamises. Ühine läbivaatamine on olnud ELi andmekaitsevaldkonnas aastaid tuntud tava, eriti lepingute puhul, milles käsitletakse broneeringuinfo vahetamist kolmandate riikidega, ja terrorismi rahastamise jälgimise programmi käsitleva lepingu puhul. Lisaks rõõmustab töörühm selle üle, et selles ühises läbivaatamises saab osaleda kindlaksmääramata arv andmekaitseasutuste esindajaid.

Võttes arvesse viimaste aastate ühise läbivaatamise käigus saadud kogemusi, soovib artikli 29 töörühm väljendada selgelt oma lootust, et ühine läbivaatamine on Privacy Shieldi puhul ulatuslikum, kui see oli broneeringuinfo vahetamise ja terrorismi rahastamise jälgimise programmi puhul. Eelkõige on soovitav, et ühine läbivaatamine ei hõlmaks üksnes kohtumisi USA asutuste, organisatsioonide ja ettevõtete esindajatega, vaid ka Privacy Shieldi teatud elementide kohapealset kontrolli. Ühises läbivaatamises osalevatel andmekaitseasutuste esindajatel peaks olema võimalik esitada sellise kohapealse kontrolli tegemiseks ettepanekuid.

Artikli 29 töörühm leiab, et ühisel läbivaatamisel on vaja järeldusi ühiselt hinnata. Seni on ühise läbivaatamise tulemusi tutvustatud komisjoni talituste töödokumendis, mille jaoks ei ole vaja olnud komisjonivälise ühise läbivaatamise meeskonna liikmete heakskiitu. Privacy Shieldi ühise läbivaatamise puhul meeldiks töörühmale, kui aruanne järelduste kohta

koostataks tõepoolest ühiselt. Kaaluda võiks andmekaitseasutuse ühise läbivaatamisaruande väljaandmist.

Lõpetuseks tuletab artikli 29 töörühm seoses ühise läbivaatamisega meelde komisjoni lubadust hüvitada töörühma esindajatele ühise läbivaatamise käigus tekkivad kulud. Töörühm eeldab, et see lubadus kehtib ka Privacy Shieldi ühisel läbivaatamisel, vähemalt mõistliku arvu andmekaitseasutuste esindajate puhul.

Artikli 29 töörühm teeb ettepaneku, et komisjon, USA valitsus ja töörühm lepiksid hiljemalt kolm kuud enne Privacy Shieldi esimest ühist läbivaatamist kokku ja paneksid kirja ühise läbivaatamise korra.

1.2.4. ELi õigusraamistiku läbivaatamine

Privacy Shieldi piisavust käsitlev otsus on esimene piisavusotsus, mis on koostatud pärast põhimõttelist kokkuleppimist isikuandmete kaitse üldmääruse tekstis. Artikli 29 töörühm on siiski kindlaks teinud, et Privacy Shield ei kajasta veel tulevast olukorda. Näiteks ei hõlma see niisuguseid uusi olulisi põhimõtteid nagu õigus andmete ülekantavusele ja vastutavate töötlejate lisakohustused, sealhulgas vajadus teha andmekaitsealaseid mõjuhinnanguid ning järgida lõimitud eraelukaitse ja eraelu kaitsvate vaikesätete põhimõtteid. Seepärast soovitab töörühm Privacy Shieldi – nagu ka kõik olemasolevad piisavusotsused – üsna pea pärast isikuandmete kaitse üldmääruse jõustumist läbi vaadata. Töörühm oleks rahul, kui piisavusotsuse lõppversioonis oleks sellele läbivaatamisele selge viide.

2. PIISAVUSOTSUSE EELNÕU KAUBANDUSLIKU OSA HINDAMINE

2.1. Üldised märkused

2.1.1. Täiustused

Artikli 29 töörühma rõõmustavad Privacy Shieldiga kaasnenud täiustused ja läbirääkimiste pidajate valmidus püüda kõrvaldada programmi Safe Harbor puudused, mida töörühm on esile toonud. Võrreldes programmiga Safe Harbor võib täheldada paranemist eelkõige järgmiste elementide puhul: mõne põhimõiste, nagu „isikuandmed“, „töötlemine“ ja „vastutav töötleja“ määratluse lisamine, Privacy Shieldiga ühinenute nimekirja järelevalve tagamise mehhanism ja praeguseks kohustuslik vastavuse sise- või väliskontroll. Täiustatud on ka juurdepääsu põhimõtet ning töörühm märgib, et nüüdseks on tagatud parandamise ja kustutamise õigus, kui andmeid kasutatakse viisil, mis on vastuolus Privacy Shieldi põhimõtetega. Lisaks on nüüd selgeks tehtud, et üksikisik peab saama nii kinnituse temaga seotud andmete töötlemise kohta kui ka teabe töödeldud andmete kohta.

Samuti teeb artikli 29 töörühmale heameelt õiguslike tagatiste tugevdamine andmete edasisaatmise korral ning kaubandusministeeriumi ja föderaalse kaubanduskomisjoni võetud kohustus jõustada Privacy Shieldiga kehtestatud kohustused.

2.1.2. Privacy Shieldi kohaldamine volitatud töötlejana tegutsevate organisatsioonide (esindajate) suhtes

Kahjuks jääb ebaselgeks, kui suures ulatuses kohaldatakse Privacy Shieldi põhimõtteid selliste põhimõtete järgimist kinnitanud organisatsioonide suhtes, kes saavad ELilt teavet üksnes töötlemise eesmärgil („esindajad“ või „volitatud töötlejad“). Ehkki II lisa jaos III.10.a on nimetatud andmete edastamist põhimõtete järgimist kinnitanud organisatsioonidele sellisel eesmärgil – viidates nõudele sõlmida leping –, ei ole seal märgitud, kuidas tuleks kohaldada raamistiku põhimõtteid volitatud töötlejate (esindajate) suhtes. See põhjustab ebakindlust nii põhimõtete järgimist kinnitanud USA organisatsioonides, kes saavad töötlemise eesmärgil andmeid, kui ka ELi äriühingutes, kes edastavad andmeid volitatud töötlejatena tegutsevatele organisatsioonidele, samuti üksikisikute jaoks, kelle andmeid töödeldakse. Selle tagajärjel on keeruline kindlaks määrata, millised kohustused on EList saadud isikuandmeid töötlevatel ja raamistiku alusel tegutsevatel organisatsioonidel volitatud töötleja rollis tegelikult. Seepärast on kindlasti vaja selgitusi.

Tuleb arvesse võtta, et paljud põhimõtete hulka lisatud kohustused volitatud töötlejatele ei sobi, sest andmete töötlemise eesmärgid ja vahendid määrab alati kindlaks vastutav töötleja (vt mõiste „vastutav töötleja“ määratlus II lisa jaos I.8.c). Sel põhjusel võib mõni põhimõtete all nimetatud kohustus, mida kohaldatakse esindajana tegutseva organisatsiooni suhtes, minna vastuollu ELi õiguse alusel nõutava andmete töötlemise lepinguga (II lisa jaos III.10.a nimetatud leping). Näiteks ei anta andmete töötlemise lepinguga volitatud töötlejale (esindajale) üldjuhul luba saata andmeid edasi kolmandast isikust vastutavale töötlejale, isegi mitte II lisa jaos II.3.a nimetatud asjaoludel. Andmete edasisaatmine kolmandast isikust esindajale peaks olema lubatud alles pärast vastutavalt töötlejalt eelneva heakskiidu saamist. Samuti ei saa volitatud töötleja (esindaja) ELi õiguse nõuete kohaselt esitada üksikisikutele teate põhimõttega ette nähtud täielikku teadet (II lisa jagu II.1), näiteks sellepärast, et asjaomane organisatsioon ei määra kindlaks töötlemise eesmärki.

Seepärast on hädavajalik selgitada põhimõtetes, et niisuguse vastuolu korral on ülimuslikud andmete töötlemise lepingu sätted ja eeskätt EList andmeid edastava organisatsiooni juhised. Ilma sellise selgituseta võidakse põhimõtteid tõlgendada ja kohaldada viisil, mis jätab Privacy Shieldiga hõlmatud esindajale liiga suure kontrolli, mistõttu ELi andmeeksportijal on oht rikkuda vastutava töötlejana oma ELi andmekaitseõigusest tulenevaid kohustusi, mida tal tuleb esindajana toimivale ja raamistiku alusel tegutsevale organisatsioonile andmete edastamisel täita. Lisaks jääb selguse puudumise tõttu mulje, et volitatud töötleja võib soovi korral kasutada andmeid uuesti.

Seoses organisatsiooni tegutsemisega volitatud töötlejana (esindajana) tuleks sätestada konkreetsed eeskirjad ka selle tagamiseks, et kõnealune organisatsioon peaks kinni vastutava töötleja juhistest. Tuleks selgeks teha, et USA organisatsioonid, kes saavad andmeid pelgalt töötlemise eesmärgil, ei saa teha otsust töödelda andmeid enda nimel. Olukorras, kus puuduvad volitatud töötlejatena tegutsevate organisatsioonide suhtes kohaldatavad konkreetsed eeskirjad, on keeruline kindlaks teha, milliste eeskirjade täitmist saaks volitatud töötleja (esindaja) kinnitada.

2.1.3. Põhimõtete järgimise kohustuse piirangud

II lisa jaos I.5 on sätestatud muu hulgas põhimõtetest tehtavad erandid Privacy Shieldiga hõlmatud andmete kasutamisel riikliku julgeoleku,[12] avaliku huvi või õiguskaitse eesmärgil või statuudi, valitsuse määruse või pretsedendiõigusega, mis loob vasturääkivaid kohustusi või annab otseseid volitusi. Omamata täielikku ülevaadet USA õigusest nii föderaalsel kui ka osariigi tasandil, on artikli 29 töörühmal keeruline hinnata selle erandi ulatust ja kaaluda, kas kõnealused piirangud on demokraatlikus ühiskonnas põhjendatavad. On oluline, et Euroopa Komisjon lisaks oma piisavusotsuse eelnõusse ka analüüsi, milles käsitletakse kaitsetaset kõnealuste erandite kohaldamise korral. Töörühm kutsub komisjoni üles tagama, et ELi teavitataks igast põhimõtete järgimist mõjutavast statuudist või valitsuse määrusest, mida juba kohaldatakse, või et sellisest statuudist või määrusest teavitataks ELi ajal, mil see USAs jõustub.

2.1.4. Isikuandmete säilitamise piiramise põhimõtte puudumine

Isikuandmete säilitamise piiramise põhimõte (direktiivi artikli 6 lõike 1 punkt e) on ELi andmekaitseõiguse aluspõhimõte, mille kohaselt tuleb isikuandmeid säilitada ainult seni, kuni see on vajalik andmete kogumise või hilisema töötlemise eesmärgi saavutamiseks.

Artikli 29 töörühm ei leia Privacy Shieldi moodustavatest dokumentidest ühtki viidet selle kohta, et vastutavad töötlejad peavad tagama andmete kustutamise, kui nende kogumise või hilisema töötlemise eesmärk on aegunud. Seega tundub, et raamistiku põhimõtetega ei ole põhimõtete järgimist kinnitanud organisatsioonidele kehtestatud andmete säilitamise ajalist piirangut, mis oleks võrreldav ELi õiguse kohase andmete säilitamise piiramise põhimõttega.

Andmete terviklikkuse ja eesmärgi piiramise põhimõtte (II lisa jagu II.5) sõnastust ei ole kuidagi võimalik tõlgendada nii, justkui seataks vastutava töötlejana tegutsevale organisatsioonile kohustus kustutada andmed pärast seda, kui need ei ole andmete kogumise või hilisema töötlemise eesmärkidel enam vajalikud, või volitatud töötlejana tegutsevale organisatsioonile kohustus kustutada andmed pärast teenuselepingu lõppemist.

Artikli 29 töörühm rõhutab, et kui puuduvad sätted, millega kehtestatakse Privacy Shieldi kohaste andmete säilitamisele ajaline piirang, annab see organisatsioonidele võimaluse säilitada andmeid nii kaua, kuni nad soovivad, isegi pärast Privacy Shieldist lahkumist, mis ei ole kooskõlas olulise andmete säilitamise piiramise põhimõttega.

2.1.5. Tagatiste puudumine automatiseeritud otsuste puhul, millel on õiguslikud tagajärjed või märkimisväärne mõju üksikisikule

Privacy Shield ei anna ühtki õiguslikku tagatist juhuks, kui üksikisiku kohta tehakse õiguslike tagajärgedega või märkimisväärse mõjuga otsus, mis toetub ainult selliste andmete automatiseeritud töötlemisele, mille eesmärk on anda hinnang andmesubjekti teatavatele

[12] Rohkem teavet Privacy Shieldiga hõlmatud isikuandmete kasutamise kohta riikliku julgeoleku ja õiguskaitse eesmärgil leiab vastavalt 3. ja 4. peatükist.

isikuomadustele, näiteks tööviljakusele, krediidivõimelisusele, usaldusväärsusele, käitumisele jne.

Vajadust näha (üksikisiku kohta õiguslike tagajärgedega või märkimisväärse mõjuga) automatiseeritud otsuste jaoks ette õiguslikud tagatised, et kindlustada piisaval tasemel kaitse, on artikli 29 töörühm rõhutanud juba oma töödokumendis nr 12.

See vajadus muutub aina pakilisemaks, sest üha arenev tehnoloogia võimaldab arvukamatel äriühingutel kaaluda automatiseeritud otsuseid tegevate süsteemide kasutuselevõttu. Sellega võib halveneda üksikisikute olukord, sest nad jäetakse ilma kõigist vahenditest, mis kaitseksid selliste arvuti tehtavate otsuste eest. Kui otsused, mida teevad üksnes automatiseeritud süsteemid, mõjutavad üksikisikute õiguslikku olukorda või avaldavad neile märkimisväärset mõju (nt nad kantakse musta nimekirja ja jäetakse sellega ilma nende õigustest), on väga oluline näha ette piisavad tagatised, sealhulgas õigus teada rakendatavat loogikat ja taotleda otsuse automatiseerimata läbivaatamist.

2.1.6. Olemasolevate kaubandussidemete puhul kohaldatav üleminekuaeg

Privacy Shieldiga on ette nähtud, et põhimõtteid hakatakse kohaldama kohe, kui on kinnitatud nende järgimist. Organisatsioonid, kes kinnitavad põhimõtete järgimist esimese kahe kuu jooksul pärast raamistiku jõustumist, peavad viima kõik oma kolmandate isikutega sõlmitud olemasolevad kaubandussidemed võimalikult kiiresti vastavusse andmete edasisaatmisel kohaldatava vastutuse põhimõttega. Igal juhul peavad nad tegema seda hiljemalt üheksa kuud pärast Privacy Shieldi põhimõtete järgimise kinnitamist.

See tähendab, et olemasolevad lepingud tuleb viia põhimõtetega vajalikus ulatuses kooskõlla kaks kuni üheksa kuud pärast põhimõtete järgimise kinnitamist. Sel üleminekuajal piisab teate ja valikuvõimaluse põhimõtte järgimisest. Artikli 29 töörühm toonitab, et andmeid saab Privacy Shieldi alusel edastada alles alates hetkest, mil organisatsioon suudab täielikult täita kõiki raamistiku nõudeid. Andmete saatmist üleminekuajal, ilma et andmete vastuvõtja oleks suuteline täielikult täitma raamistiku põhimõtteid, ei saa lugeda seadusliku edastamise tingimustele vastavaks ja seetõttu ei ole see vastuvõetav.

2.2. Konkreetsed märkused

2.2.1. Läbipaistvus

a) Üldised märkused teate kohta.

Artikli 29 töörühmale valmistavad heameelt teate põhimõtte all sätestatud põhjalikumad ja üksikasjalikumad nõuded, eriti see, et teade peab sisaldama linki veebisaidile või veebiaadressi, kus asub Privacy Shieldiga ühinenute nimekiri, ning et teates tuleb viidata üksikisikute juurdepääsuõigusele ja alternatiivsetele vaidluste lahendamise mehhanismidele[13]. Siiski soovitab töörühm olla sõnaselgem muude reguleeritud õiguste puhul (õigus selliste

[13] II lisa, jagu II.1. Artikli 29 töörühm viitab ka komisjoni teatises COM(2013) 847 final esitatud komisjoni teisele soovitusele ja töörühma 2014. aasta 10. aprilli kirjale asepresident Redingile, eelkõige jao „Läbipaistvus“ punktile 4.

andmete parandamisele või kustutamisele, mis on ebatäpsed või mida on töödeldud raamistiku põhimõtteid rikkudes).

Privacy Shieldi moodustavad dokumendid annavad põhjust tunda muret aja pärast, mil raamistiku alusel tegutsev organisatsioon peab esitama üksikisikule teate. II lisa jaos II.1.b on öeldud, et „teade tuleb esitada [---], kui üksikisikutel palutakse esmakordselt esitada organisatsioonile isikuandmeid või pärast seda niipea, kui see on teostatav, kuid igal juhul enne, kui organisatsioon seda teavet kasutab muul eesmärgil kui see, milleks see algselt koguti või milleks andmeid edastav organisatsioon neid töötles või avaldab need esmakordselt kolmandale isikule“. Artikli 29 töörühm leiab, et paljudes olukordades ei kogu Privacy Shieldi alusel tegutsev USA organisatsioon andmeid otse andmesubjektilt ja seega peaks teate esitama hetkel, kui raamistiku alusel tegutsev organisatsioon andmed registreerib.

Artikli 29 töörühm märgib, et teate põhimõttega seotud nõuete ja eraelu puutumatuse normide tegelikku rakendamist tuleks hinnata Privacy Shieldi esimese iga-aastase läbivaatamise käigus.

b) Eraelu puutumatuse normide kättesaadavus avalikkusele

Artikli 29 töörühmal on hea meel nüüdseks saabunud selguse üle selles, et kaubandusministeerium kontrollib, kas äriühingud, kellel on avalik veebisait, on avaldanud sellel oma eraelu puutumatuse normid või kui äriühingutel sellist avalikku veebisaiti ei ole, kas nad on teinud oma eraelu puutumatuse normid avalikkusele kättesaadavaks[14].

c) Volitatud töötlejatega sõlmitud lepingute eraelu puutumatust käsitlevate tingimuste avaldamine

Tingimuste seas, mille alusel Privacy Shieldi alusel tegutsevad organisatsioonid saavad edastada volitatud töötlejale (esindajale) andmeid, on raamistikus nõue, et põhimõtete järgimist kinnitanud organisatsioon peab esitama „nõudmisel ministeeriumile kokkuvõtte või koopia kõnealustest eraelu puutumatust käsitlevatest, asjaomase esindajaga sõlmitud lepingu sätetest“ (II lisa jagu II.3.b.v). Artikli 29 töörühma rõõmustab see läbipaistvusnõue kaubandusministeeriumi suhtes.

2.2.2. Valikuvõimalus

Privacy Shieldiga on ette nähtud õigus keelduda isikuandmete edastamisest kolmandale isikule või isikuandmete kasutamisest algsest eesmärgist oluliselt erineval eesmärgil[15] (II lisa jagu III.2). Peale selle on üksikisikutel alati keeldumisõigus seoses isikuandmete kasutamisega otseturunduseesmärkidel (II lisa jagu III.12.a)[16].

[14] Vt komisjoni esimene soovitus teatises COM(2013) 847 final ja töörühma 2014. aasta 10. aprilli kiri asepresident Redingile, eelkõige jao „Läbipaistvus“ punkt 3.
[15] Täienduspõhimõtete all jaos 14.c.I on sätestatud õigus loobuda kliinilisest katsest, mida võidakse käsitada õigusena esitada vastuväide või õigusena keelduda nõusoleku andmisest.
[16] See on identne programmi Safe Harbor raames ette nähtuga (korduma kippuv küsimus nr 12) ja selle kohta ei ole tehtud ühtki muudatust.

Peale otseturunduseesmärkidega seotud konteksti ei ole esitatud ühtki üksikasja selle keeldumisõiguse kasutamise viisi ja aja kohta. Artikli 29 töörühm leiab, et eraelu puutumatuse normides esitatud lihtsast viitest selle õiguse olemasolule ei piisa, vaid pakkuda tuleks *individuaalset* võimalust kasutada seda õigust *enne* isikuandmete avalikustamist või uuesti kasutamist.

Veel rõhutab artikli 29 töörühm, et Privacy Shieldiga tuleks tagada üldine õigus esitada vastuväide, mida tuleks mõista kui õigust paluda lõpetada andmete töötlemine alati, kui isikul on selleks oma konkreetse olukorraga seotud õigustatud ja veenvad põhjused[17]. Töörühm soovitab tungivalt teha piisavusotsuse eelnõus selgeks, et vastuväidete esitamise õigus peaks olema olemas igal hetkel, mitte üksnes andmete kasutamisel otseturunduse eesmärgil[18].

Artikli 29 töörühm kardab, et mõiste „oluliselt erinev eesmärk" määratluse puudumine toob kaasa segaduse ja õigusliku ebakindluse. Tuleks selgitada, et valikuvõimaluse põhimõtet ei või mingil juhul kasutada eesmärgi piiramise põhimõttest kõrvalehiilimiseks[19]. Valikuvõimalust peaks saama kasutada üksnes juhul, kui eesmärk on oluliselt erinev, kuid siiski kooskõlas algse eesmärgiga, sest eesmärgiga vastuolus olev töötlemine on keelatud (II lisa jagu II.5.a). Tuleb selgitada, et keeldumisõigus ei saa võimaldada organisatsioonil kasutada andmeid algse eesmärgiga vastuolus olevatel eesmärkidel. Seega soovitab töörühm sellekohast sõnastust ühtlustada, kasutades üht ja kindlat väljendit (nt „oluliselt erinev eesmärk, mis on siiski kooskõlas algse eesmärgiga").

Abi oleks selgitusest selle kohta, kas otsus töödelda andmeid muul eesmärgil või avalikustada teavet kuulub ELi õiguse alla. Sellises olukorras otsekohaldatakse – muu hulgas ELi õiguse kohaldamisalasse jäävate USA organisatsioonide suhtes – sedalaadi töötlemise suhtes kohaldatavaid tavalisi ELi õiguslikke tingimusi (nagu keeld töödelda andmeid algse eesmärgiga vastuolus olevatel eesmärkidel, nõue nimetada töötlemise õiguslik alus ja vajadus üksikisikut teavitada). Praktikas tähendab see seda, et ELi õiguse kohaselt on töötlemise läbipaistvuse ja seaduslikkuse tagamine sellist otsust tegeva ELi eksportija ülesanne. Seepärast kohaldatakse valikuvõimaluse põhimõtet üksnes juhul, kui otsuse teeb ainuisikuliselt Privacy Shieldi alusel tegutsev USA organisatsioon, kelle suhtes ELi õigust ei kohaldata.

2.2.3. Edasisaatmine

a) Kohaldamisala

Artikli 29 töörühm tunneb muret olukordade pärast, kus Privacy Shieldi põhimõtete järgimist kinnitanud USA organisatsioon saadab andmed edasi kolmandas riigis asuvale vastuvõtjale.

[18] Vt asepresident Redingile saadetud artikli 29 töörühma kirja jagu „Valikuvõimalus".
[19] Konkreetne näide algse eesmärgiga vastuolus oleva hilisema töötlemise kohta, mis on valikuvõimaluse põhimõtte alusel lubatud, on esitatud täienduspõhimõtete all jaos 9.b.1 (vt artikli 29 töörühma sellekohane märkus punktis, milles on käsitletud personaliandmeid).

Raamistikku ei tuleks näha üksnes vahendina ELi andmete edastamiseks EList USAsse, vaid ka vahendit, mida kasutada andmete edastamiseks USAst kolmandatesse riikidesse. Seepärast moodustavad raamistiku olulise osa andmete edasisaatmist käsitlevad sätted, mis peaksid andma piisavad tagatised ja sobiva kaitsetaseme andmete edasisaatmisel väljapoole USAd. Üks konkreetne küsimus on seotud riikliku julgeoleku ja õiguskaitsega.

Privacy Shieldi raames andmete edasisaatmisel rakendatavat vastutuse põhimõtet ei kohaldata üksnes USAs registreeritud, andmeid vastuvõtvate vastutavate töötlejate, volitatud töötlejate või esindajate suhtes. Seetõttu võib andmeid Privacy Shieldi alusel kolmandale riigile edasi saata isegi juhul, kui sellel kolmandal riigil on olemas õigusaktid, milles on sätestatud avalikkuse juurdepääs isikuandmetele näiteks jälgimise eesmärgil. Sellega tekib ELi andmete puhul oht, et põhiõiguste kaitsesse sekkutakse põhjendamatult.

Andmete edasisaatmisel kolmandale riigile peaks iga Privacy Shieldi alusel tegutsev organisatsioon olema alati kohustatud hindama enne andmete edasisaatmist andmeimportija suhtes kohaldatavaid kolmanda riigi õigusaktide kohustuslikke nõudeid. Kui avastatakse oht, et Privacy Shieldiga ette nähtud tagatistele, kohustustele ja kaitsetasemele võib avalduda märkimisväärne kahjulik mõju, peab raamistiku alusel tegutsev volitatud töötlejast USA organisatsioon (esindaja) ELi vastutavat töötlejat enne igasugust andmete edasisaatmist viivitamata teavitama. Sellisel juhul on andmeeksportijal õigus andmete edasisaatmine peatada ja/või leping lõpetada. Niisuguse märkimisväärse kahjuliku mõju ohu korral ei tohiks raamistiku alusel tegutseval vastutavast töötlejast organisatsioonil olla lubatud andmeid edasi saata, sest see seaks ohtu tema kohustuse tagada andmete edasisaatmisel sama kaitsetase kui see, mis on ette nähtud raamistiku põhimõtete alusel (II lisa jagu II.3.a).

Ka juhul, kui kolmanda riigi õigusaktides tehakse muudatus, millel on tõenäoliselt märkimisväärne kahjulik mõju Privacy Shieldiga ette nähtud tagatistele, kohustustele ja kaitsetasemele, peaks raamistiku alusel tegutsev volitatud töötlejast USA organisatsioon (esindaja) olema raamistiku kohaselt kohustatud teavitama sellest kohe pärast kõnealusest muudatusest teadasaamist andmeeksportijat, kellel on õigus andmete edasisaatmine peatada ja/või leping lõpetada. Sellisel juhul ei tohiks Privacy Shieldi alusel tegutseval vastutavast töötlejast organisatsioonil olla lubatud andmeid edasi saata, sest tal on kohustus tagada sama kaitsetase kui see, mis on ette nähtud raamistiku põhimõtete alusel (II lisa jagu II.3.a).

Artikli 29 töörühm tuletab meelde oma seisukohta, et kui ELi vastutav töötleja on teadlik andmete edasisaatmisest väljaspool USAd asuvale kolmandale isikule juba enne andmete edastamist USA-le või kui ELi vastutav töötleja on ühiselt vastutav otsuse eest lubada andmete edasisaatmist, tuleks seda edasisaatmist käsitada andmete edastamisena otse EList väljaspool USAd asuvasse kolmandasse riiki. See tähendab, et Privacy Shieldi andmete edasisaatmise põhimõtte asemel kohaldatakse edastamise suhtes direktiivi artikleid 25 ja 26.

b) Andmete edastamine Privacy Shieldi alusel tegutsevalt organisatsioonilt kolmandast isikust vastutavale töötlejale

Artikli 29 töörühm kiidab heaks kohustuse sõlmida lepingud (II lisa jagu II.3.a) kandmaks hoolt selle eest, et kolmandast isikust vastutav töötleja tagab vähemalt samal tasemel eraelu puutumatuse kaitse, kui on nõutud Privacy Shieldi põhimõtetega. Eesmärk on kindlustada, et isikuandmed oleksid kogu aeg piisavalt kaitstud, isegi pärast nende edasisaatmist. Töörühmal on kavandatud tingimuste kohta siiski mõni märkus.

Puudub viide eesmärgi piiramise põhimõttele

Artikli 29 töörühm soovitusel võiks lisada tingimustesse, mis käsitlevad andmete edasisaatmist kolmandast isikust vastutavale töötlejale (II lisa jagu II.3.a), ka selge viite eesmärgi piiramise põhimõttele (II lisa jagu II.5). Sellega tehtaks selgeks, et andmeid ei tohi edasi saata, kui kolmandast isikust vastutav töötleja töötleb neid algse eesmärgiga vastuolus oleval eesmärgil.

Vastutavate töötlejate vahelise grupisisese andmeedastuse puhul kehtiv erand lepingu sõlmimise vajadusest

Vastutavate töötlejate vahelise grupisisese andmeedastuse puhul on lepingu sõlmimise vajaduse kohta sätestatud erand. Sellise olukorra jaoks on põhimõtetes kirjas, et jätkuva kaitse tagamiseks on võimalik tugineda siduvatele kontsernisisestele eeskirjadele või „muudele grupisisestele vahenditele (nt vastavuse ja kontrolli programmid)“ (II lisa jagu III.10.b). Artikli 29 töörühm leiab, et viide muudele grupisisestele vahenditele ei kindlusta seda, et grupi teised liikmed võtavad endale õiguslikult siduvaid kohustusi. Kuna töörühmas ja ELi õigusaktides[20] üldjuhul pooldatakse grupisisese andmeedastuse reguleerimiseks siduvaid kohustusi, tuleb vältida Privacy Shieldi kasutamist sellest nõudest möödahiilimiseks. Töörühm tuletab meelde, et andmete edasisaatmist USAst kolmandatele riikidele, mida kavandati juba enne andmete edastamist USA-le või mida kontrollitakse ühiselt ELi vastutava töötlejaga,[21] tuleb käsitada andmete edastamisena otse EList väljaspool USAd asuvale kolmandale riigile ning seega kohaldatakse selle suhtes direktiivi artikleid 25 ja 26.

c) Andmete edastamine Privacy Shieldi alusel tegutsevalt organisatsioonilt kolmandast isikust volitatud töötlejale (esindajale)

Artikli 29 töörühmal on hea meel, et andmeid vastuvõtvad üksused, kes tegutsevad volitatud töötlejana (esindajad), on nüüd kohustatud sõlmima andmete edasisaatmiseks lepingu, ükskõik kas nad osalevad Privacy Shieldis või kas nende puhul kasutatakse andmekaitse piisavuse tagamiseks mõnda muud lahendust. Samuti kiidab töörühm heaks sellise edasisaatmisega seotud täiendavad kaitsemeetmed (II lisa jagu II.3.a.i, jagu II.3.a.iii, jagu II.3.a.iv, jagu II.3.a.v, jagu II.7.d). Viimati nimetatud jaos (II 7.d) on käsitletud kohustust kanda vastutust, kui andmed avalikustatakse esindajale. Siiski tundub, et see tagatis ei kehti, kui organisatsioon on otsustanud teha koostööd andmekaitseasutusega (vt II lisa jao III.5.a

[20] Vajadust siduvate ja täitmisele pööratavate kohustuste järele on rõhutatud ka isikuandmete kaitse üldmääruses, sõltumata kasutatavast vahendist (siduvad kontsernisisesed eeskirjad, lepingutingimused, toimimisjuhend või sertifitseerimismehhanism).
[21] Nt personaliandmed.

viimane lause). Artikli 29 töörühm ei mõista, mis on sellise erandi põhjus, ja leiab, et vastutus peaks kehtima isegi sellisel juhul.

Puudub viide eesmärgi piiramise põhimõttele

Artikli 29 töörühm märgib, et andmete edasisaatmise eest kohaldatava vastutuse põhimõttega (II lisa jagu II.3) seoses on selgitatud, et isikuandmeid võib edastada esindajana tegutsevale kolmandale isikule üksnes piiratud ja konkreetsel eesmärgil, kuid ei ole sõnaselgelt öeldud, et see piiratud ja konkreetne eesmärk peab olema vastavuses andmete kogumise algse eesmärgiga ja vastutava töötleja juhistega. Selles küsimuses on vaja rohkem selgust. Seepärast soovitab töörühm tagada piisavusotsuse suurem üksikasjalikkus, lisades näiteks selge viite eesmärgi piiramise põhimõttele (II lisa jagu II.5), mille kohaselt ei tohi andmeid töödelda (sh avalikustada) andmete edasisaatmise põhimõttega (mida kohaldatakse lisaks keeldumispõhimõttele) vastuolus oleval eesmärgil.

Vajadus Privacy Shieldi alusel tegutseva volitatud töötlejast organisatsiooni (esindaja) arvukamate lisakohustuste järele andmete edasisaatmisel teisele volitatud töötlejale (esindajale)

Selgete eeskirjade puudumine olukorras, kus Privacy Shieldi alusel tegutsev organisatsioon, kes toimib esindajana (st ELi vastutava töötleja nimel), toob kaasa lünga ja võib takistada ELi vastutavat töötlejat kontrolli säilitamast. Raamistiku alusel tegutsev organisatsioon, kes võtab andmeid vastu ELi vastutava töötleja esindajana, peab järgima ELi vastutava töötleja juhiseid. See peaks olema põhimõtetes selgelt sätestatud kindlustamaks, et kõnealuste juhiste eiramine tähendaks lepingu (II lisa jagu III.10.a.ii) rikkumise kõrval ka Privacy Shieldi põhimõtete rikkumist.

Esindajana toimiva, raamistiku alusel tegutseva organisatsiooni võimalus saata andmed edasi kolmandast isikust esindajale peab olema vastutava töötleja jaoks läbipaistev ja selleks on nõutav viimase eelnev heakskiit. Seepärast peaks olema selgelt öeldud, et esindaja ja ELi vastutava töötleja vahel sõlmitavas lepingus (millele on viidatud korduma kippuvas küsimuses nr 10 kui artikli 17 lepingule) määratakse kindlaks, kas andmete edasisaatmine on lubatud[22].

Praegused tingimused, mida kohaldatakse andmete edasisaatmisel esindajale, põhinevad eeldusel, et Privacy Shieldi alusel tegutsev organisatsioon toimib vastutava töötlejana ja saab seega ise otsustada kolmandast isikust esindaja võimaliku sekkumise üle. Raamistiku alusel tegutseva organisatsiooni toimimisel esindajana ei tohiks see siiski võimalik olla. Vastasel juhul jääks ELi vastutav töötleja ilma oma kontrollisuutlikkusest.

Kolmandast isikust esindajaga sõlmitud lepingu asjakohased eraelu puutumatust käsitlevad sätted tuleb teha vastutavale töötlejale kättesaadavaks. Samuti peab nendega olema tagatud vähemalt sama kaitsetase, kui on tagatud vastutava töötlejaga sõlmitud lepinguga.

[22] Vt 10. aprillil 2014 asepresident Redingile saadetud artikli 29 töörühma kirja jao „Andmete edasisaatmine“ punkt 4.

2.2.4. Andmete terviklikkus ja eesmärgi piiramine

a) Proportsionaalsus

Seoses ühe väiksema probleemiga viitab artikli 29 töörühm asepresident Redingile saadetud kirjale, milles on öeldud, et „isikuandmete töötlemine võib isegi teate ja valikuvõimaluse põhimõtte rangel järgimisel olla andmesubjekti või ühiskonna huve, õigusi ja vabadusi silmas pidades ebaproportsionaalne. Proportsionaalsuse ja mõistlikkuse põhimõtet, mis peaks olema kohaldatav lisaks teate ja valikuvõimaluse põhimõttele, tuleb austada kõikides töötlemise etappides“[23].

Privacy Shieldiga (II lisa jagu II.5.a) sätestatakse, et koguda tohib üksnes töötlemise eesmärgile vastavat teavet. Artikli 29 töörühmale meeldiks, kui seda sõnastust piisavusotsuse lõppversioonis muudetaks, sest ainuüksi sellest, et andmed vastavad töötlemise eesmärgile, ei piisa, et muuta töötlemine proportsionaalseks. Proportsionaalsuse põhimõtte järgimiseks tuleks töödelda üksnes andmeid, mis on asjaomaseks töötlemiseks vajalikud.

b) Täpsus

Andmete terviklikkuse ja eesmärgi piiramise põhimõtte all (II lisa jagu II.5) on öeldud järgmist: „Nendel eesmärkidel vajalikus ulatuses peab organisatsioon võtma mõistlikke meetmeid, tagamaks et andmed on kavatsetud kasutuseks usaldusväärsed, täpsed, täielikud ja ajakohased.“ Artikli 29 töörühm märgib, et täpselt sama sõnastust on kasutatud programmis Safe Harbor. Töörühm kahtleb, kas fraas „nendel eesmärkidel vajalikus ulatuses“ tuleks alles jätta, sest tema vaatenurgast ei tohiks andmete täpsus sõltuda töötlemise eesmärgist. Töörühm eelistaks, et piisavusotsuse lõppversioonis seda seost ei loodaks.

c) Eesmärgi piiramine

Kui ELis registreeritud vastutav töötleja edastab USA organisatsioonile isikuandmeid, peaks andmeeksportija sõnaselgelt teavitama USA organisatsiooni eesmärgist, mille jaoks andmeid algselt koguti. See on vajalik selleks, et määrata kindlaks, kas pärast edastamist eesmärk muutub, tuues kaasa teate ja valikuvõimaluse põhimõtte kohaldamise. Samuti aitab see jagada riske ja vastutust.

Andmete terviklikkuse ja eesmärgi piiramise põhimõtte all (II lisa jagu II.5) on öeldud, et organisatsioon ei tohi töödelda isikuandmeid viisil, mis ei vasta eesmärkidele, milleks need koguti või milleks üksikisik seejärel loa andis. Teisalt on valikuvõimaluse põhimõtte (II lisa jagu II.2) raames sätestatud võimalus valida, kas anda nõusolek kasutada tundlikke andmeid (st isikuandmed, mis täpsustavad meditsiinilist või tervislikku seisundit, rassilist või etnilist päritolu, poliitilisi vaateid, religioosseid või filosoofilisi vaateid, ametiühingu liikmelisust, või teave üksikisiku seksuaalelu kohta ja karistusregistri andmed) eesmärgil, mis on oluliselt erinev sellest, milleks need algselt koguti või milleks üksikisik seejärel loa andis. Seda

[23] Vt 10. aprillil 2014 asepresident Redingile saadetud artikli 29 töörühma kiri, lk 8.

nõusolekut ei nõuta täienduspõhimõtte 1.a all nimetatud olukordades (II lisa jagu III.1.a). Mittetundlike isikuandmete kohta on ette nähtud keeldumise kord.

Artikli 29 töörühm märgib, et eesmärgi piiramise põhimõtte kohaldamisala on teate, valikuvõimaluse, andmete terviklikkuse ja eesmärgi piiramise põhimõtete puhul erinev. Mõisteid „vastuolus olev eesmärk“ ja „oluliselt erinev eesmärk“ kasutatakse samas tekstis, ilma et neid kumbagi oleks selgelt määratletud[24].

Artikli 29 töörühm tunneb tõsist muret sellepärast, et niisugune ebajärjekindlus võib tekitada suuri raskusi andmete terviklikkuse ja eesmärgi piiramise põhimõtte (II lisa jagu II.5) ühitamisel valikuvõimaluse põhimõttega (II lisa jagu II.2), sest kui ühe põhimõtte kohaselt ei tohi andmeid ei tohi töödelda viisil, mis ei vasta eesmärkidele, milleks need koguti, siis teise puhul on ette nähtud võimalus valida, kui andmeid töödeldakse eesmärgil, mis on oluliselt erinev algsest eesmärgist.

Seega võib valikuvõimaluse põhimõtet tõlgendada kui loa andmist algse eesmärgiga vastuolus olevaks hilisemaks töötlemiseks[25]. Artikli 29 töörühma arvates tuleb selgeks teha, et organisatsioonil ei ole lubatud töödelda andmeid algsest eesmärgist oluliselt erineval eesmärgil, kui see on eesmärgi piiramise põhimõtte alusel algse eesmärgiga vastuolus. Teisisõnu peaks olema selge, et valikuvõimaluse põhimõttega ei tehta erandit eesmärgi piiramise põhimõttest.

Ka siis, kui hilisemat töötlemist saab lugeda algse eesmärgiga kooskõlas olevaks, tuleks igal juhul kohaldada ka teate ja valikuvõimaluse põhimõtet.

2.2.5. Erandid ajakirjandusele

Erandeid, mida tehakse isikuandmete töötlemisel ajakirjandusele, on käsitletud 2. täienduspõhimõtte all (II lisa jagu III.2). Need sätted kajastavad sõnavabaduse põhiseaduslikku kaitset USAs. Seepärast on Privacy Shieldi dokumentides öeldud: „Andmekaitseraamistiku Privacy Shield põhimõtete nõudeid ei kohaldata [---] massiteabevahendite arhiivide levitatavast varem avaldatud materjalist leitud teabe suhtes.“ (II lisa jagu III.2.b). See erand tundub hõlmavat iga vastutava või volitatud töötleja poolset mis tahes hilisemat töötlemist, st see ei ole piiratud hilisema töötlemisega ajakirjanduslikel eesmärkidel. Nagu asepresident Redingile 10. aprillil 2014 saadetud kirjas on juba öeldud, oleks artikli 29 töörühm soovinud näha ajakirjandusele tehtavate erandite puhul piiratumat lähenemist, mis oleks rohkem kooskõlas ELis kohaldatavate põhimõtetega ja Google Spaini kohtuasjas kehtestatud õigusega eemaldada andmeid otsingutulemuste loetelust[26].

[24] Artikli 29 töörühm täheldab, et kasutatud on ka mõnda teist väljendit: „ei kasutata kooskõlas“ (II lisa jagu III.14.b.ii), „erinevatel eesmärkidel“ (II lisa jagu III.9.b.i), „muul eesmärgil kui see, milleks see algselt koguti“ (II lisa jagu II.1.b). Selline ebaselgus võib viia selleni, et eesmärgi piiramise põhimõttega seotud piisavad tagatised puuduvad.

[25] Vt ka valikuvõimaluse põhimõtte käsitlemisel esitatud märkus. Sellise tõlgendamise ohtu suurendab artikli 29 töörühma meelest asjaolu, et andmete edasisaatmise eeskirjades (II lisa jagu II.3) on viidatud üksnes valikuvõimaluse põhimõttele, kuid jäetud nimetamata eesmärgi piiramise põhimõte.

[26] Kohtuotsus, Euroopa Kohus, 13. mai 2014, Google Spain *vs.* Agencia Española de Protección de Datos ja Mario Costeja González, C-131/12, ECLI:EU:C:2014:317.

2.2.5. Andmesubjektide juurdepääsuõigus ning õigus andmete parandamisele ja kustutamisele

Privacy Shieldi alusel on üksikisikutel õigus saada *kinnitus* selle kohta, kas organisatsioon töötleb või ei töötle nende andmeid, ning *saada* selliseid andmeid (II lisa jagu III.8.a.i). Ent organisatsioonide kohustus vastata üksikisikute päringutele töötlemise eesmärgi, töödeldavate isikuandmete kategooriate ja selle kohta, kellele või millise kategooria vastuvõtjatele isikuandmed avalikustatakse, on paraku võrdlemisi väikese jõuga. Artikli 29 töörühm leiab, et andmesubjektile esitatavad üksikasjad peaksid olema loetletud põhitekstis, mitte pelgalt joonealuses märkuses, ja et nende esitamine tuleks sõnastada selge kohustusena (seotud lisa II jaoga III.8.a.i.1).

Vastavalt 8. täienduspõhimõttele tuleb „[j]uurdepääs [---] võimaldada ainult organisatsiooni poolt isikuandmete säilitamise ulatuses“ (II lisa jagu III.8.d.ii). Seda eeskirja ei tuleks tõlgendada kitsalt, st juurdepääs tuleks põhimõtteliselt tagada mis tahes viisil organisatsiooni poolt töödeldavatele, mitte üksnes säilitatavatele andmetele. Seepärast on juurdepääsuõiguse tõhususe huvides tähtis selgeks teha, et II lisa jaos I.8.b esitatud määratluse tähenduses mõeldakse säilitamise all töötlemist. Selle eeskirja kohaldamist tuleks raamistiku ühisel läbivaatamisel tähelepanelikult kontrollida.

Endiselt on põhjust muret tunda seoses II lisa jaos III.8.e.i esitatud erandite loeteluga, mis sarnaneb programmi Safe Harbor korduma kippuva küsimuse nr 8 all esitatud loeteluga ja mis kaldub nihutama tasakaalukeset organisatsioonide huvide poolele. Nimelt ei anta üksikisikutele juurdepääsu oma isikuandmetele järgmistel põhjustel: „see toob kaasa õigusliku või muu ametialase privileegi või kohustuse rikkumise“ (II lisa jagu III.8.e.3), „see kahjustab töötajate julgeolekukontrolli või töövaidluste käsitlemist või on seotud töötajate töökohtade planeerimise ja äriühingute ümberkorraldamisega“ (II lisa jagu III.8.e.4) ja „see kahjustab heakvaliteedilise juhtimisega seotud järelevalve, kontrolli või regulatiivtoimingute teostamiseks või organisatsiooni tulevasteks või käimasolevateks läbirääkimisteks vajalikku konfidentsiaalsust“ (II lisa jagu III.8.e.5). Need põhjused lisanduvad II lisa jaos III.8.c nimetatud üldisele konfidentsiaalse äriinfoga seotud erandile. Seega ei pääse üksikisikud eespool loetletud olukordades kunagi oma andmetele ligi, sest juurdepääsutaotluse rahuldamiseks lahenduse leidmiseks ei looda üksikisiku ja organisatsiooni õiguste ja huvide vahel mingit tasakaalu.

Artikli 29 töörühm tuletab meelde, et õigus tutvuda oma andmetega on tagatud üksikisikutele harta artikli 8 lõikega 2. Ehkki tegemist ei ole absoluutse õigusega, on see seoses isikuandmete kaitsmise õigusega väga oluline, sest see muudab andmesubjekti jaoks lihtsamaks teiste õiguste, näiteks andmete parandamise ja kustutamise õiguse kasutamise.

Mis puudutab õigust andmete parandamisele ja kustutamisele, siis artikli 29 töörühmale valmistab heameelt tähtis täiustus, mille Privacy Shieldi põhimõtted on võrreldes programmiga Safe Harbor kaasa toonud, nimelt et kõnealused õigused ei ole tagatud mitte üksnes olukorras, kus andmed on ebatäpsed, vaid ka juhul, kui neid on töödeldud raamistiku põhimõtteid rikkudes (II lisa jagu II.6).

2.2.6. Kaebuste menetlemine, täitmise tagamine ja vastutus (õiguskaitsemehhanism)

a) ELi üksikisikute õiguskaitsega seotud õiguste tõhus kasutamine

Artikli 29 töörühm kiidab heaks kohustused, mille USA ametiasutused on võtnud seoses õiguskaitsemehhanismi eri tasanditega. Mehhanismi üldise ülesehituse keerukust ja ebaselgust silmas pidades tunneb töörühm aga kartust, et praktikas võib andmesubjekti õiguse tõhus kasutamine siiski ohtu sattuda. Töörühm märgib, et õiguskaitsemehhanismi kvaliteet tuleks seada tähtsamale kohale kui ELi üksikisikutele kättesaadavate mehhanismide hulk. Muret tuntakse ka selle pärast, et enamiku – kui mitte kõigi – kaebuste menetlemise mehhanismide puhul on ette nähtud menetluse toimumine USAs, mistõttu ELi andmekaitseasutustel on keeruline seda jälgida.

Privacy Shieldiga sätestatud kaebuste menetlemise mehhanismis keskendutakse eeskätt andmesubjekti võimalusele „kaitsta oma õigusi ja esitada kaebused raamistiku põhimõtete järgimata jätmise kohta otse põhimõtete järgimist kinnitanud USA ettevõttele“[27]. Lisaks peavad organisatsioonid määrama sõltumatu vaidluste lahendamise organi, kes uurib ja lahendab üksikkaebusi. Artikli 29 töörühmal on hea meel, et sellega ei kaasne üksikisikule mingeid kulusid.

Samuti võib kaebuse esitada otse föderaalsele kaubanduskomisjonile, ehkki see komisjon ei ole kohustatud kaebust menetlema. Kaebuse võib esitada ka andmekaitseasutus. Kaubandusministeerium on võtnud kohustuse vaadata kaebused läbi ja teha kõik selleks, et hõlbustada kaebuste menetlemist (I lisa), mille föderaalne kaubanduskomisjon „vaatab esmajärjekorras läbi“ (II isa jagu III.7.e). Kaebuste esmajärjekorras läbivaatamine föderaalses kaubanduskomisjonis ei anna andmesubjektile siiski mingit kindlust, et tema kaebust hakatakse menetlema.

Viimase abinõuna on üksikisikutel võimalus algatada siduv vahekohtumenetlus. See toimub USAs ja selle vaatavad läbi USA kohtud.

Lisaks pakutakse Privacy Shieldiga organisatsioonile võimalust valida koostöö ELi andmekaitseasutustega (II lisa jagu III.5.a). Töösuhte raames kogutavate personaliandmete puhul on see lausa kohustuslik (II lisa jagu III.9.d.ii). Sellisel juhul ei ole alternatiivne vaidluste lahendamine võimalik (II lisa jagu III.5.a). Privacy Shieldiga ei ole üheselt kindlaks määratud, kuidas koostöö ELi andmekaitseasutustega praktikas korraldatakse. Eelkõige on ebaselge, kas kõikide juhtumitega tegeleb üks vahekohus või iga erinevat juhtumit lahendab erinev vahekohus.

Artikli 29 töörühm leiab, et piisavusotsuses tuleks üksikasjalikumalt sätestada andmekaitseasutuste pädevus kaebuste menetlemisel. See sõltub ilmselt organisatsiooni liigist, kuid on selgusetu, mil viisil.

[27] Euroopa Komisjoni piisavusotsuse eelnõu, punkt 30.

Kui organisatsioon tegutseb ELi vastutava töötleja nimel esindajana, on üksikisikul igal juhul võimalus esitada kaebus pädevale ELi andmekaitseasutusele. Seda saab teha sarnasel viisil nii personaliandmete kui ka muude äriandmete töötlemisel.

Kui Privacy Shieldi alusel tegutsev organisatsioon toimib vastutava töötlejana, piirdub andmekaitseasutuse pädevus kaebuse menetlemisel ELi õiguse kohase töötlemisega (ELi vastutava töötleja vastutuse alla kuuluv töötlemine, sh ühine kontroll USA organisatsiooniga, või kui raamistiku alusel tegutseva organisatsiooni suhtes otsekohaldatakse ELi õigust, näiteks ELis asuvate vahendite kasutamisel). Kui andmeid töödeldakse üksnes USA õiguse alusel, kohaldatakse siiski vaid Privacy Shieldi mehhanisme. Et ületada keelebarjäärid ja korvata teadmiste puudumine USA õigussüsteemi kohta, oleks abi sellest, kui ELi andmekaitseasutustel oleks õigus tegutseda üksikisiku kaebuse vahendajana või aidata üksikisikut USA organisatsioonidega seotud alternatiivsetes vaidluste lahendamise menetlustes või ühenduse võtmisel USA ametiasutustega, kui andmekaitseasutus peab seda asjakohaseks.

Artikli 29 töörühm rõhutab, et Privacy Shieldi raames kirjeldatud mehhanismi puhul ei ole järgitud varasemat soovitust, mille kohaselt peaks ELi üksikisikutel olema „võimalik esitada kahjunõuded Euroopa Liidus“ ja neile peaks olema „antud õigus esitada hagi pädevas ELi liikmesriigi kohtus“[28]. Oleks tervitatav, kui raamistiku alusel tegutsevad organisatsioonid lisaksid selle võimaluse oma eraelu puutumatuse normidesse.

Tõhususe tagamiseks soovitab artikli 29 töörühm, et süsteem võimaldaks ELi andmekaitseasutustel esindada andmesubjekti ja tegutseda tema nimel või vahendajana. Teise võimalusena peaks süsteem sisaldama jurisdiktsiooni käsitlevaid erisätteid, mis lasevad andmesubjektidel teostada oma õigusi Euroopas.

b) Vahekohtumenetlus

Vahekohtumenetlus ei ole veel lõplikult välja töötatud ja see muudab hindamise artikli 29 töörühma jaoks keeruliseks. Kuna tundub, et menetlus hakkab toimuma USA õiguse alusel ja ainsaks menetluskeeleks saab inglise keel, võivad ELi andmekaitseasutused soovida endale õigust üksikisikuid selles aidata.

Vahekohtumenetlus võeti kasutusele põhjusel, et puudus kindlus, et kaebusega hakatakse tegelema, kuivõrd föderaalsel kaubanduskomisjonil ei ole kohustust iga kaebust menetleda. Artikli 29 töörühm märgib, et kui ELi üksikisik peaks tundma vajadust kasutada advokaadi abi, peab ta maksma oma advokaaditasud ise, mis võib takistada isikuid esitamast vahekohtule kaebust.

c) Õiguskaitsemehhanismide järelevalve, jõustamine ja tõhusus

<u>Privacy Shieldiga ühinemise tingimused</u>

[28] Vt artikli 29 töörühma 2014. aasta 10. aprilli kiri asepresident Redingile.

Euroopa Liidu Kohtu sõnul põhineb põhimõtete järgimise kinnitamise süsteemi usaldusväärsus „selliste tõhusate avastamis- ja kontrollimehhanismide sisseseadmisel, mis võimaldavad põhiõiguste [---] kaitset tagavate õigusnormide võimalikke rikkumisi praktikas tuvastada ja nende eest karistada“[29].

Artikli 29 töörühm märgib, et kaubandusministeeriumi roll Privacy Shieldi kohases kinnitamisprotsessis on kahanenud pelgalt dokumentide täielikkuse kontrollimisele. Kuigi artikli 29 töörühm tunnistab, et põhimõtete järgimise kinnitamine ei tähenda eraelu puutumatuse normide rakendamise eelnevat süstemaatilist kontrolli, peaks kaubandusministeerium kohustuma korrakindlalt kontrollima vähemalt seda, et eraelu puutumatuse normid hõlmaksid kõiki Privacy Shieldi põhimõtteid. Piisavusotsuse eelnõus on sellist kohustust nimetatud, kuid kaubandusministeeriumi esitiskirjas ei ole võimalik seda selgelt kindlaks teha[30].

Privacy Shieldi põhimõtete rikkumine võib jääda pikaks ajaks märkamata – see võidakse avastada alles pärast seda, kui andmesubjekti põhiõigusi on tõsiselt, võimalik et pöördumatult kahjustatud. Seetõttu võib selline olukord minna vastuollu Euroopa ettevaatuspõhimõttega.

<u>Läbipaistvuse tagamine Privacy Shieldiga ühinenute nimekirja abil ja nimekirjast eemaldatud organisatsioonide üle arvestuse pidamise kaudu</u>

Märkimisväärseid täiustusi on tehtud läbipaistvuse tagamisel andmesubjekti jaoks. Lisaks kõigile USA organisatsioonidele, kes on kinnitanud kaubandusministeeriumile Privacy Shieldi põhimõtete järgimist, sisaldab uus Privacy Shieldiga ühinenute nimekiri teavet kõikide nimekirjast eemaldatud organisatsioonide, sealhulgas nende eemaldamise põhjuste kohta[31]. Kaubandusministeeriumi hallataval Privacy Shieldi veebisaidil keskendutakse edaspidi rohkem sihtrühmadele, et oleks lihtsam kontrollida organisatsioonipoolse põhimõtete järgimise kinnitusega hõlmatud teabe liiki, hõlmatud teabe suhtes kohaldatavaid eraelu puutumatuse norme, samuti meetodeid, mida organisatsioon kasutab põhimõtete järgimise tõendamiseks[32]. Artikli 29 töörühmal on hea meel nüüdseks saabunud selguse üle selles, et kaubandusministeerium kontrollib, kas äriühingud, kellel on avalik veebisait, on avaldanud sellel oma eraelu puutumatuse normid või kui äriühingutel sellist avalikku veebisaiti ei ole, kas nad on teinud oma eraelu puutumatuse normid avalikkusele kättesaadavaks[33]. Samuti sisaldavad dokumendid rohkem teavet eraelu puutumatuse normide sisu kohta[34].

Artikli 29 töörühm leiab, et probleem võib tekkida juhul, kui organisatsioon, mis on Privacy Shieldiga ühinenute nimekirja juba kantud, kinnitab hiljem põhimõtete järgimist ka muude andmekategooriate puhul. Sellisel juhul ei kajastu nimekirjas, millistel erinevatel perioodidel

[29] Schremsi kohtuotsus, punkt 81.
[30] Euroopa Komisjoni piisavusotsuse eelnõu, punkt 34.
[31] I lisa, lk 5, ja II lisa, jagu II.1. Artikli 29 töörühm viitab ka komisjoni teatises COM(2013) 847 final esitatud komisjoni neljandale soovitusele ja töörühma 2014. aasta 10. aprilli kirjale asepresident Redingile, eelkõige jao „Läbipaistvus“ punktile 5.
[32] I lisa, lk 8. Artikli 29 töörühm viitab ka oma 2014. aasta 10. aprilli kirjale asepresident Redingile, eelkõige jao „Läbipaistvus“ punktile 2.
[33] I lisa, lk 3 ja 4. Artikli 29 töörühm viitab ka komisjoni teatises COM(2013) 847 final esitatud komisjoni esimesele soovitusele ja töörühma 2014. aasta 10. aprilli kirjale asepresident Redingile, eelkõige jao „Läbipaistvus“ punktile 3.
[34] I lisa, lk 5 ja 6, ning II lisa, jagu III.6.

neid põhimõtteid eri andmekategooriate suhtes kohaldatakse. Sellega tekib oht, et ELi üksikisikud ja ettevõtjad ei saa täiel määral hinnata, kas mingite kindlate andmete suhtes kohaldatakse Privacy Shieldi põhimõtteid, ja kui seda tehakse, siis mis ajast saadik. Selle puuduse vältimiseks soovitab artikli 29 töörühm märkida Privacy Shieldiga ühinenute nimekirjas sisalduvatesse organisatsioonide andmetesse eraldi iga isikuandmete kategooria puhul kuupäev, mil raamistiku põhimõtete järgimise kinnitust hakati kohaldama.

Artikli 29 töörühmal on hea meel, et kaubandusministeerium hakkab pidama arvestust Privacy Shieldiga ühinenute nimekirjast eemaldatud organisatsioonide üle ja et see arvestus sisaldab selgitust, et ehkki kõnealustele organisatsioonidele ei ole enam tagatud Privacy Shieldi soodustused, peavad nad jätkama põhimõtete järgimist raamistikus osalemise ajal saadud isikuandmete puhul niikaua, kuni nad neid andmeid säilitavad (I lisa lk 3). Ent kuna üks nimekirjast eemaldatud organisatsioon võib otsustada raamistikus osalemise ajal saadud andmed tagastada või kustutada, teine aga sellised andmed säilitada, on oluline tagada üksikisikutele selles küsimuses suurem läbipaistvus. Arvestuses, mida kaubandusministeerium selliste organisatsioonide üle peab, tuleks seetõttu täpsustada, kas nende käsutuses on veel Privacy Shieldi kaudu saadud isikuandmeid või on ta sellised andmed tagastanud või kustutanud. Kui mõni organisatsioon säilitab veel selliseid andmeid, tuleks sõnaselgelt öelda, et ta peab jätkama selliste andmete suhtes raamistiku põhimõtete kohaldamist.

Peale selle tuleks kaubandusministeeriumi peetavas arvestuses märkida, et kõnealustele organisatsioonidele ei ole uute andmeedastuste puhul Privacy Shieldi eelised enam tagatud, mis tähendab, et neil ei ole enam lubatud ELilt raamistiku põhimõtete alusel andmeid vastu võtta.

Kontrollimenetlus

Kontrollimaks, kas Privacy Shieldi põhimõtete järgimise kinnitamine on praktikas tõhus, võivad organisatsioonid korraldada enesehindamisi või väliseid vastavuskontrolle. Artikli 29 töörühmal on kahju, et töötajate koolitamist nõutakse vaid siis, kui organisatsioon on valinud kontrollimiseks enesehindamismeetodi (II lisa jagu III.7.c). Samuti tundub, et eraelu puutumatuse normide täpsuse, terviklikkuse, selgelt esitamise, rakendamise ja kättesaadavuse kontrollimist nõutakse vaid juhul, kui organisatsioon on valinud sisekontrolli (enesehindamise), ning et väliskontrolli ajal vaadeldakse üksnes seda, kas organisatsioonisisestest eraelu puutumatuse normidest on kinni peetud.

Järelkontroll

Artikli 29 töörühm peab õigeks, et föderaalsele kaubanduskomisjonile ja kaubandusministeeriumile on antud seoses kaebustega uurimisvolitused. Lisaks märgib töörühm, et kaubandusministeeriumil on võimalus teha *ex officio* kontrolli, eelkõige küsimustike väljasaatmise teel. Siiski tahaks töörühm veenduda, et sellisest toimimisviisist piisab täitmaks Euroopa Liidu Kohtu nõuet tagada rikkumiste tõhusad avastamis- ja kontrollimehhanismid. Õigupoolest on töörühmal endiselt küsimusi selle kohta, millised on USA täitevasutuste täpsed volitused selliste kohapealsete kontrollide korraldamisel, mis tehakse Privacy Shieldi põhimõtete järgimist kinnitanud organisatsioonide ruumides raamistiku rikkumise uurimiseks, kuidas on võimalik saavutada USA territooriumil ELi ametiasutuse otsuse täidetavaks tunnistamine ja kas Privacy Shieldi kohastel karistustel on praktikas heidutav toime.

2.2.7. Personaliandmete töötlemine

Kohaldamisala

9. täienduspõhimõtet (II lisa jagu III.9) kohaldatakse töösuhte kontekstis kogutud (endiste või praeguste) töötajate isikuandmete suhtes. Kõnealuse täienduspõhimõtte punkti a alapunkti ii alusel kohaldatakse Privacy Shieldi põhimõtteid üksnes „eraldi tuvastatud registriandmete edastamisel või neile juurdepääsul“. Mõiste „tuvastatud registriandmed“ ei ole kooskõlas II lisa jaos I.8.a esitatud isikuandmete määratlusega, mille alla kuuluvad „identifitseeritud või identifitseeritava üksikisiku kohta käivad andmed“, ega sobi seetõttu kokku direktiivis kasutatud määratlusega[35].

9. täienduspõhimõtte punkti a alapunktis ii on kirjas: „Statistiline aruandlus, mis tugineb personali koondandmetele ja ei sisalda isikuandmeid, või anonüümsete andmete kasutamine ei põhjusta eraelu puutumatuse kaitse alaseid probleeme.“ See väide on vastuolus artikli 29 töörühma mitme avaldatud arvamusega. Töörühm soovib toonitada, et koondandmete puhul saab andmesubjekti taastuvastada ja seepärast tuleks neid käsitada isikuandmetena[36].

[35] Nagu juba rõhutatud, ei ole ka piirang „edastamisel või neile juurdepääsul“ kooskõlas mõistega „töötlemine“ (II lisa jagu I.8.b).
[36] Vt arvamus 4/2007 isikuandmete mõiste kohta ja arvamus 05/2014 anonüümimisvõtete kohta.

Teade, valikuvõimalus ja eesmärgi piiramine

9. täienduspõhimõtte punkti b alapunktis i on esitatud näide teate ja valikuvõimaluse põhimõtte kohaldamise kohta, kui personaliandmeid kasutatakse algsest eesmärgist erineval eesmärgil. Näide puudutab USA organisatsiooni, kes „kavatseb kasutada töösuhte kaudu kogutud isikuandmeid töösuhtega mitteseotud eesmärkidel, näiteks turunduskommunikatsioonis“. Sellisel juhul antakse eesmärgi muutmiseks luba tingimusel, et teate ja valikuvõimaluse põhimõtetest peetakse kinni. Artikli 29 töörühma arvates tuleks personaliandmete hilisemat töötlemist turundusotstarbel enamikul juhtudel lugeda algse eesmärgiga vastuolus olevaks ja seega eesmärgi piiramise põhimõttega kokkusobimatuks eesmärgiks (II lisa jagu II.5.a). Lisaks leiab töörühm, et valikuvõimaluse põhimõte ei saa olla asjakohane alus, mille toel saada töötaja nõusolek (keeldumine) töötlemise eesmärgi muutmiseks, kuivõrd töösuhte kontekstis ei pruugi selline nõusolek olla täiesti vabatahtlik.

Artikli 29 töörühm kahtleb sügavalt, kas see, et Privacy Shieldi raames keskendutakse eeskätt valikuvõimaluse põhimõttele, mis kujutab endast tingimust andmete hilisemaks kasutamiseks muul eesmärgil, on kooskõlas OECD eraelu puutumatust käsitlevate suunistega, sest puuduvad piisavad tagatised vältimaks võimalust, et keeldumismehhanismi kasutatakse ka hilisemal töötlemisel, mis on algse eesmärgiga vastuolus. 9. täienduspõhimõtte punkti b alapunktis iv on esitatud ulatuslik ja selge teate ja valikuvõimaluse põhimõtete erand „[s]elles ulatuses ja ajavahemikuks, mis on vajalik organisatsiooni teovõime kahjustamise vältimiseks edutamiste, ametisse nimetamiste või muude sarnaste töösuhteid puudutavate otsuste langetamiseks“. Esiteks, kui personaliandmeid kasutatakse sellistel eesmärkidel, tuleks sellele sõnaselgelt viidata juba andmete kogumisel. Teiseks on väljend „muude sarnaste töösuhteid puudutavate otsuste langetamiseks“ liiga ebamäärane ja lai. Selle tagajärjeks on see, et personaliandmed jäetakse teate ja valikuvõimaluse põhimõtete kohaldamisalast täielikult välja, kui neid töödeldakse töösuhte kontekstis. Kõnealune mõiste on nii lai, et see ei võimalda hinnata, kas hilisem kasutamine on vastavuses algse eesmärgiga. Artikli 29 töörühm soovitab selle erandi välja jätta.

Juurdepääsuõigus

9. täienduspõhimõtte punkti e alapunktis i on sätestatud ka erand, mille kohaselt ei pea rakendama juurdepääsu põhimõtet või sõlmima personaliandmete edastamiseks lepingut vastutava töötlejaga, kes on kolmas isik, juhuslike töösuhtega seotud operatiivvajaduste rahuldamiseks, nagu väikese arvu töötajate isikuandmete edastamine lennupiletite või hotellitoa broneerimiseks või kindlustuse tellimiseks, tingimusel et järgitakse teate ja valikuvõimaluse põhimõtteid. Artikli 29 töörühma meelest ei ole sellise erandi tegemiseks ühtki mõistlikku põhjust, mistõttu soovitab ta selle punkti välja jätta.

2.2.8. Farmaatsia- ja meditsiinitooted

Kohaldamisala

Privacy Shieldi kohaselt ei kujuta farmaatsia- ja meditsiinitooteid käsitlevate kodeeritud andmete edastamine EList USAsse endast Privacy Shieldiga reguleeritud edastamist (II lisa jagu III.14.g.i). Kodeeritud andmete edastamine on kaitstud Euroopa andmekaitseõiguse alusel. See tähendab, et praktikas ei saa Privacy Shield selliste andmete edastamist hõlmata. Artikli 29 töörühm kutsub komisjoni üles sõnaselgelt sätestama, et piisavusotsuse eelnõu ei hõlma farmaatsia- ja meditsiinitooteid käsitlevate kodeeritud andmete edastamist ning et seetõttu peab selliste andmete edastamine olema kaetud muude kaitsemeetmetega, näiteks lepingu tüüptingimuste või siduvate kontsernisiseste eeskirjadega. Töörühm leiab, et seda võiks piisavusotsuse lõppversioonis selgitada.

Edastamine reguleerimis- ja järelevalve eesmärkidel (II lisa jagu III.14.d)

Artikli 29 töörühm tunneb muret sellepärast, et nende sätete alusel võidakse USA seadusandjatele edastada isikuandmeid, mis on oma meditsiinilise sisu tõttu enamasti tundlikku laadi. Kuna Privacy Shield on mõeldud andmete vahetamiseks eraõiguslike üksuste vahel, tundub, et selline avaliku sektori asutus nagu USA seadusandja ei saa kinnitada Privacy Shieldi põhimõtete järgimist, millega tekib küsimus piisava andmekaitse kohta sellise andmeedastuse korral. Kui selline andmeedastus on vajalik reguleerimiseesmärkidel, tuleb võtta asjakohaseid meetmeid, et tagada ELi andmesubjekti põhiõiguste pidev kaitse. Artikli 29 töörühm juhib tähelepanu asjaolule, et piisavusotsuse eelnõus ei ole esitatud selle kohta ühtki järeldust. Seepärast ei ole töörühmal mingit tagatist, et ELi andmesubjektide tundlike andmete jaoks on tagatud sellises olukorras piisav kaitse.

Peale selle märgib artikli 29 töörühm, et ta ei mõista, miks on tulevaste teadusuuringute huvides toimuva töötlemise näitena esitatud eesmärk „turundus“. Samuti on ebaselge põhjus, miks on punktis „Edastamine reguleerimis- ja järelevalve eesmärkidel“ käsitletud andmete edasisaatmist äriühingu teistesse asukohtadesse ja teistele uurijatele. Need küsimused vajavad piisavusotsuse lõppversioonis selgitamist.

Toote ohutuse ja tõhususe jälgimine (sh aruandmine valitsusasutustele) ning patsientide poolt teatavate ravimite või meditsiiniseadmete kasutamise jälgimine

Privacy Shieldiga on ette nähtud erand, mille puhul ei pea teate, valikuvõimaluse, edasisaatmise ja juurdepääsu põhimõtet kohaldama ulatuses, milles nendest põhimõtetest kinnipidamine segaks regulatiivsete nõuete järgimist. Piisavusotsuse eelnõus ei ole esitatud ühtki näidet olukorra kohta, kus eraelu puutumatusega seotud põhimõtetest kinnipidamine segaks regulatiivsete nõuete järgimist. Ehkki artikli 29 töörühm võib mõista, et valitsuste korraldatud uurimised võivad õigustada teate ja juurdepääsuõiguse põhimõtte piiramist uurimise kaitseks, jääb arusaamatuks, millega saab õigustada selliste ulatuslike erandite tegemist olukorras, kus töötleja on erasektori organisatsioon või kolmas isik. Näiteks kuna patsientide ravimeetodeid individualiseeritakse üha enam, on selline ulatuslik eraelu puutumatuse põhimõttega seotud erand teatavaid ravimeid või meditsiiniseadmeid kasutavate patsientide jälgimisel lubamatu, kuivõrd selline raviviis on muutumas tavaliseks. Sama kehtib juhul, kui ravimiettevõtted kasutavad andmeid toote ohutuse ja tõhususe jälgimiseks (uute ravimite katsetamine või müük).

2.2.9. Avalikult kättesaadav teave

Juurdepääsuõiguse erand, mis kehtib avalikult kättesaadava teabe ja avalike registrite puhul (II lisa jagu III.15.d ja III.15.e), paneb muretsema siis, kui üksikisik soovib oma juurdepääsuõiguse kasutamisel teada, kas konkreetne vastutav töötleja töötleb tema andmeid ja milliseid andmeid töödeldakse, et ta saaks kontrollida oma andmete töötlemist. Artikli 29 töörühm on korduvalt väitnud, et ELi õiguse kohaselt on andmesubjektidel alati õigus tutvuda oma andmetega ja vajaduse korral nõuda nende parandamist või kustutamist, kui neid ei ole töödeldud seaduslikult või kui nad on puudulikud või ebatäpsed, olenemata sellest, kas need isikuandmed on avaldatud[37]. Kui üksikisiku taotlus oma andmetega tutvuda lükatakse tagasi põhjusel, et andmed on saadud avalikult kättesaadavatest allikatest või avalikest registritest, kaotab isik võimaluse kontrollida andmete täpsust ja veenduda selles, kas andmete avalikustamine on üldse olnud seaduslik.

Privacy Shieldiga jäetakse avalikud registrid ja avalikult kättesaadav teave teate, valikuvõimaluse, juurdepääsu ja andmete edasisaatmise eest kohaldatava vastutuse põhimõtte kohaldamisalast välja (II lisa jagu II.15.b). Võrreldes direktiiviga tunduvad need erandid olevat liiga ulatuslikud ja annavad põhjust muret tunda, kuivõrd nad kahjustavad muu hulgas üksikisikute võimalust kontrollida oma andmete täpsust ja piirata oma andmete levitamist.

2.3. Järeldused

Artikli 29 töörühm tunnistab, et USA ametiasutused ja Euroopa Komisjon on märkimisväärselt täiustanud kahe maailmajao vahelise andmeedastuse kaubanduslikke aspekte. Eespool esitatud analüüsi arvesse võttes leiab töörühm siiski, et Privacy Shieldi kaubanduslik osa vajab mitmes punktis veel selgitamist. Muretsema paneb näiteks sõnaselge andmete säilitamise põhimõtte puudumine. Seepärast kahtleb töörühm tõsiselt, kas Privacy Shield suudab tagada kaitsetaset, mis on sisuliselt samaväärne ELis tagatud kaitsetasemega.

Piisavusotsuses tuleks eesmärgi piiramise ja valikuvõimaluse põhimõtteid lähemalt selgitada. Mitme põhimõtte puhul säilib lünkade tekkimise oht, eriti seoses andmete edasisaatmise, kaebuste menetlemise mehhanismi ja personali- või farmaatsiaandmete töötlemisega. Samuti on vaja kirjeldada üksikasjalikumalt, kuidas tuleb kohaldada Privacy Shieldi põhimõtteid volitatud töötlejate (esindajate) suhtes, ning pöörata erilist tähelepanu terminite selgele ja ühetähenduslikule kasutamisele.

3. PIISAVUSOTSUSE EELNÕU RIIKLIKU JULGEOLEKUGA SEOTUD TAGATISTE HINDAMINE

3.1. USA riiklike julgeolekuasutuste suhtes kohaldatavad kaitsemeetmed ja piirangud

Sekkumine eraelu puutumatuse ja andmekaitsega seotud põhiõigustesse võib olla lubatav, kui see on demokraatlikus ühiskonnas põhjendatav. See tähendab, et eraelu puutumatusega seotud põhimõtted ei ole absoluutsed ja võimalikud on erandid, ent üksnes juhul, kui on kinni peetud

[37] Vt WP 20, lk 4.

kohaldatavatest (olulistest) tagatistest. Kooskõlas eesmärgiga edendada eraelu puutumatuse kaitset peaksid organisatsioonid lisaks püüdma rakendada kõnealuseid põhimõtteid täielikult ja läbipaistvalt, sealhulgas pannes oma eraelu puutumatuse normidesse kirja, kui nende põhimõtete erandeid, mis on USA õigusraamistikus lubatud, hakatakse korrapäraselt kohaldama. Samal põhjusel eeldatakse, et kui põhimõtete ja/või USA õigusaktide alusel on võimalik teha valik, valivad organisatsioonid võimaluse korral kõrgema kaitsetaseme.

II lisa jaos I.5 on öeldud: „Nende põhimõtete järgimist võib piirata: a) riikliku julgeoleku, avaliku huvi või õiguskaitseliste vajaduste täitmiseks vajalikus ulatuses; b) statuudi, valitsuse määruse või pretsedendiõigusega, mis loob vasturääkivaid kohustusi või annab otseseid volitusi, tingimusel et selliste volituste kasutamisel suudab organisatsioon tõendada, et põhimõtete mittejärgimine tema poolt piirdub ulatusega, mis on vajalik selliste volitustega seotud ülekaaluka õigustatud huvi järgimiseks; või c) kui direktiiv või liikmesriigi seadus lubab erandeid ja kõrvalekaldeid, tingimusel et selliseid erandeid või kõrvalekaldeid rakendatakse sarnastes olukordades.“

Küsimus on selles, kas II lisas nimetatud erandid on demokraatlikus ühiskonnas põhjendatavad. Komisjon leiab Privacy Shieldi piisavusotsuse eelnõus, et „Ameerika Ühendriikides on olemas eeskirjad, mille ülesandeks on piirata selliste isikute põhiõiguste riivamist riikliku julgeoleku huvides, kelle isikuandmeid edastatakse liidust Ameerika Ühendriikidesse ELi-USA andmekaitseraamistiku Privacy Shield alusel, rangelt sellega, mis on vajalik asjaomase seadusliku eesmärgi saavutamiseks“[38].

Võttes aluseks raamistiku, nagu seda on kirjeldatud käesoleva arvamuse punktis 1.2, ning arvestades USA ametiasutuste kinnitusi ja komisjoni järeldusi, hindas artikli 29 töörühm USA praegust õigusraamistikku, USA luureasutuste tavasid ja tingimusi, mille alusel need võimaldavad sekkumist ELi õigusraamistikuga kaitstud põhiõigustesse eraelu austamisele ja andmekaitsele. Selle hindamise raames on analüüsitud presidendi poliitikasuunist (*Presidential Policy Directive*) nr 28 (edaspidi „PPD-28“), korraldust (*Executive Order*) 12333 ja välisluure seadusega (*Foreign Intelligence Act,* edaspidi „FISA“, paragrahvid 104, 402, 215, 501 ja 702) kehtestatud eri õiguslikke aluseid. Artikli 29 töörühm on tuginenud Privacy Shieldi VI lisale, mis sisaldab riikliku luurejuhi ameti (*Office of the Director of National Intelligence*, edaspidi „ODNI“) kirja, kus on käsitletud USA riiklike julgeolekuasutuste suhtes kohaldatavaid kaitsemeetmeid ja piiranguid ning kus on kokku võetud teave, mis on esitatud Euroopa Komisjonile USA signaaliluure andmete kogumise kohta.

3.2. Tagatis A. Töötlemine peab toimuma kooskõlas õigusaktidega ning põhinema selgetel, täpsetel ja ligipääsetavatel eeskirjadel

Euroopa õiguse kohaselt peab sekkumine olema kooskõlas õigusaktide, kehtestatud tegevuspõhimõtete ja menetlustega ning piisavalt selge ja ligipääsetav (konkreetsetele riikidele antud kaalutlusõiguse raames), et anda kodanikele asjakohane ülevaade asjaoludest

[38] Komisjoni otsuse (isikuandmete kaitse piisavuse kohta ELi-USA andmekaitseraamistikus Privacy Shield vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ) eelnõu, punkt 75.

ja tingimustest, mille korral ja alusel on avaliku sektori asutustel õigus kasutada jälgimismeetmeid[39].

Artikli 29 töörühm märgib, et signaaliluuretegevus toimub ligipääsetava õigusraamistiku alusel. Kõik VI lisas nimetatud seadused (PPD-28, FISA, USA vabadusseadus (*USA Freedom Act*), teabevabaduse seadus (*Freedom of Information Act*, FOIA) on internetis üldsusele kättesaadavad (nii USAs kui ka sellest väljaspool). VI lisas on esitatud kokkuvõte reguleeriva õigusraamistiku, kogumise piirangute, säilitamise ja levitamise piirangute, vastavuse ja järelevalve ning läbipaistvuse ja hüvitamise kohta. Luuretegevuse valdkonnas kohaldatav USA õigussüsteem koosneb mitmest dokumendist, mille hulka kuuluvad konkreetsete asutuste aruanded, tegevuspõhimõtted ja menetlused, mida tuleb analüüsida, et mõista seda tegevust nii teoorias kui ka praktikas paremini. Artikli 29 töörühm on keskendunud sellega seoses teatud küsimustele, mida ta peab oluliseks.

3.2.1. Korraldus 12333 ja presidendi poliitikasuunis nr 28

Korralduse 12333 kohaldamisala on lai. Korralduse alusel võib USA presidendi otsusel koguda põhimõtteliselt igasuguseid välisluure andmeid. Siiski on väidetud, et pärast FISA jõustumist saab korraldust 12333 kasutada ainult andmete kogumiseks väljaspool USA territooriumi. Artikli 29 töörühm märgib, et korralduses 12333 ei ole eriti üksikasjalikult sätestatud, milline on korralduse geograafiline kohaldamisala või kui suures ulatuses võib andmeid koguda, säilitada või levitada, ega ka seda, millist laadi rikkumine võib kaasa tuua jälgimise või mis liiki teavet võib koguda või kasutada.

Presidendi poliitikasuunise nr 28 (PPD-28) põhieesmärk on töörühma arusaama kohaselt kehtestada piirid isikuandmete kogumisele ja töötlemisele, olenemata sellest, millist jälgimisprogrammi kasutatakse või kust andmed on saadud.

PPD-28 on Ameerika Ühendriikide presidendi suunis, kus on sätestatud järjepidevuspõhimõtted, mille alusel signaaliluure andmete kogumist lubatakse ja ellu viiakse, kuid see ei ole nende andmete kogumise õiguslik alus. PPD-228 on tõhus, kehtestades luureasutustele kõnealused põhimõtted rakendamiseks oma strateegiates ja menetlustes. Suunist kohaldatakse signaaliluuretegevuse suhtes olenemata andmete asukohast nende kogumise ajal nii USAs kui ka sellest väljaspool. Seepärast kohaldatakse seda ka andmete suhtes, mida kogutakse signaaliluure eesmärgil andmete edastamisel EList USAsse.

Eeskätt on suunises öeldud, et signaaliluuret tuleb teostada nii kohandatud kujul kui võimalik[40]. Andmete kasutamise kohta on selles sätestatud menetlused, mis hõlmavad

[39] Euroopa Inimõiguste Kohus sedastab Zakharovi kohtuotsuse punktis 247 järgmist: „Kohus on varem leidnud, et õiguse „etteaimatavuse“ nõudega ei minda nii kaugele, et sellega kohustataks riike jõustama õigusnorme, kus oleks loetletud üksikasjalikult kõik käitumisviisid, mis võivad kaasa tuua otsuse hakata isikut riikliku julgeoleku huvides salaja jälgima. Riiklikule julgeolekule avalduv oht võib olla sõltuvalt asja olemusest laadilt erinev ning ettenägematu või seda võib olla keeruline eelnevalt määratleda (vt eespool tsiteeritud Kennedy kohtuotsuse punkt 159). Samal ajal on kohus rõhutanud ka seda, et põhiõigusi mõjutavates küsimustes oleks see, kui riikliku julgeoleku valdkonnas tegutsevale täidesaatvale organile antud kaalutlusõigus väljenduks piiramatus võimus, vastuolus õigusriigi põhimõttega ehk ühe konventsioonis sätestatud demokraatliku ühiskonna aluspõhimõttega. Seepärast tuleks õigusaktides piisavalt selgelt kindlaks määrata iga selline pädevale asutusele antav kaalutlusõigus ja selle kasutamise viis, võttes arvesse asjaomase meetme õiguspärast eesmärki, et tagada üksikisikule piisav kaitse meelevaldse sekkumise eest.“

andmete vähendamist (sh andmete säilitamise ja levitamise tingimused), andmete turvalisust ja asjakohaste töötajate ligipääsu andmetele (st eeskirjad, mis sisaldavad kuritarvitamise ja kohatu kasutamise ohtu piiravaid kaitsemeetmeid), andmete kvaliteeti ja järelevalvet. Neid kaitsemeetmeid kohaldatakse sõltumata andmesubjekti kodakondsusest, st nii USA kodanike kui ka mittekodanike suhtes.

Andmete edastamisel USA-le kohaldatakse ka suunises kehtestatud kaitsemeetmeid. VI lisa sisaldab ODNI võetud kohustust, mille kohaselt juhul, kui USA luureteenistus kogub andmeid Atlandi-üleste kaablite kaudu andmete edastamisel Ameerika Ühendriikidesse, „tuleb seda teha siin kehtestatud piirangute ja kaitsemeetmete raames, sealhulgas PPD-28 nõuete alusel“[41]. Artikli 29 töörühm märgib, et endiselt puudub väljakujunenud kohtupraktika, milles oleks kindlaks määratud kaabli kaudu toimuva andmeedastuse jälgimise seaduslikkus, kui seda teostab riik. Igatahes USA ei kinnita ega lükka ka ümber, et ta jälgib kaabli kaudu toimuvat andmeedastust luureandmete kogumiseks.

Mõistet „signaaliluure“ ei ole määratletud ei kõnealuses suunises ega üheski teises kohaldatavas dokumendis.

3.2.2. Välisluure jälitustegevuse seadus

Üldiselt tundub välisluure jälitustegevuse seadus (FISA) olevat selgem ja täpsem. Ometi sõltub seaduse mitme sätte tõlgendamine PPD-28 valguses ja seega nende praktiline kohaldamine suuresti sellest, kuidas eri asutused seadust rakendavad. Ehkki täielik aruanne uute kaitsemeetmete rakendamise kohta ei ole veel kättesaadav, on USA esindajad teavitanud artikli 29 töörühma esindajaid sellest, et PPD-28 kaitsemeetmete kasutuselevõtt on tõepoolest lõpule viidud ja et kõnealuseid meetmeid rakendatakse ühetaoliselt kõikides USA luureasutustes.

Täpsemalt on paragrahvis 501 võrdlemisi selgelt sätestatud luuretegevus, mille jaoks võib anda loa: „mis tahes materiaalsete esemete (sealhulgas raamatud, andmekandjad, paberid, dokumendid ja muud esemed) kogumine“. Tuleks siiski märkida, et asjaolu, et materiaalsete esemete määratlus hõlmab „muid esemeid“, muudab selle loa kohaldamisala küllaltki ulatuslikuks.

Paragrahvis 702, millega lubatakse koguda välisluureinfo hankimiseks andmeid isikutelt, kes ei ole USA kodanikud ja kelle puhul on piisavalt alust arvata, et nad asuvad väljaspool Ameerika Ühendriike,[42] ei olda nii üksikasjalik kui paragrahvis 501. Paragrahvi 702 kohaldamisel on võetud sihikule USAs asutatud elektroonilise side teenuste osutajad, et koguda väljaspool USAd asuvatelt isikutelt välisluureinfot. Mõiste „välisluureinfo“ määratlus on lai. Selle alla kuulub muu hulgas „teave võõrvõimu või välisriigi territooriumi kohta, mis

[40] „Signaaliluuret tuleb teostada nii kohandatud kujul kui võimalik. Otsustades selle üle, kas signaaliluure andmeid koguda, kaaluvad Ameerika Ühendriigid muu, sealhulgas diplomaatilistest ja avalikest allikatest pärit teabe kättesaadavust. Sellised sobivad ja võimalikud signaaliluure alternatiivid tuleks seada esikohale“ (paragrahv 1 punkt d).

[41] Privacy Shieldi VI lisas esitatud riikliku luurejuhi ameti (ODNI) kiri USA riiklike julgeolekuasutuste suhtes kohaldatavate kaitsemeetmete ja piirangute kohta, lk 2.

[42] USA seadustiku 50. jagu, paragrahv 1881a, punkt D, lõige 1.

on seotud Ameerika Ühendriikide välisasjadega“,[43] mis tekitab teatavat ebakindlust ses suhtes, mis liiki teavet võib tegelikult koguda.

Hoolimata dokumentide, kongressile esitatud aruannete ning eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjoni (*Privacy and Civil Liberties Oversight Board*, edaspidi „PCLOB“) järelevalvearuannete avalikustamisest on FISA kohaldamine, sealhulgas selle kohaldamisala ja kindlaksmääratud valikutingimused, endiselt ebaselged ja segadusseajavad. Kindlaksmääratud valikutingimuste kasutamisele on PCLOBi aruandes viidatud,[44] kuid artikli 29 töörühma meelest ei vasta see paragrahvi 702 kohastele sihtmärgi võtmise eeskirjadele[45]. Samuti ei ole töörühmale teadaolevalt nimetatud neid üldiselt ligipääsetavates eeskirjades.

3.2.3. Järeldused

Artikli 29 töörühm märgib kokkuvõtteks, et luuretegevusega seotud kohaldatavad dokumendid on internetis kättesaadavad ja USA ametiasutused on astunud mitu olulist sammu läbipaistvuse poole.

Töörühm tunnistab, et alates 2013. aastast on avaldatud suur hulk dokumente, mis sisaldavad tegevuspõhimõtteid, menetlusi, FISA kohtu otsuseid, samuti muid dokumente, mille salastatus on kustutatud. Peale selle on PCLOB avaldanud tähtsad aruanded FISA paragrahvi 702 ja USA vabadusseaduse alusel ellu viidud tegevuse kohta. Sarnast aruannet on oodata korralduse 12333 kohase tegevuse kohta.

Mitu seadusandlikku lisa, mis võiksid heita valgust sellele, milline on korralduse 12333 mõju üksikisikutele väljaspool Ameerika Ühendriike, ja kõik kohaldatavad kaitsemeetmed on salastatud ega ole seega ligipääsetavad ei avalikkusele ega isikutele, keda meetmete kohaldamine võib mõjutada. Avalikuks tehtud dokumendid on väikese väärtusega ega anna kuigi head ülevaadet luuretegevusest.

Hoolimata püüdlustest selgitada korralduse 12333 toimimist pärast Snowdeni paljastusi, eelkõige PPD-28 vastuvõtmise abil, on selle praktiline kohaldamine praegu endiselt ebaselge. Artikli 29 töörühm märgib, et Privacy Shieldi VI lisas ei ole esitatud üksikasjalikku teavet korralduse 12333 toimimise kohta.

Ehkki artikli 29 töörühm rõõmustab PPD-28 vastuvõtmisega lisandunud piirangute üle, on keeruline hinnata, kas jälgimistegevust reguleeriv USA õigusraamistik on piisavalt etteaimatav, st kas see annab „piisava ülevaate asjaoludest ja tingimustest, mille korral ja alusel avaliku sektori asutustel on õigus selliseid meetmeid kasutada“, kuivõrd lisaselgitused, sealhulgas PCLOBi aruanne korralduse 12333 rakendamise kohta, on alles valmimas.

[43] USA seadustiku 50. jagu, paragrahv 1801, punkt e, lõige 2.
[44] PCLOBi aruanne FISA paragrahvi 702 kohaselt rakendatava jälgimisprogrammi kohta, lk 32.
[45] USA seadustiku 50. jagu, paragrahv 1881a, punkt D.

3.3. Tagatis B. Tõestada tuleb vajalikkust ja proportsionaalsust taotletavate õiguspäraste eesmärkide vaatenurgast

3.3.1. Presidendi poliitikasuunis nr 28

PPD-28s on kirjas piirangud, mis on seotud eesmärkidega, milleks isikuandmeid võib kasutada, tingimustega, mille alusel neid andmeid võib levitada, ja signaaliluure andmete kogumise mõjuga, olenemata kasutatavast õiguslikust alusest.

Eeskätt on PPD-28 paragrahvis 1 öeldud, et signaaliluuret tuleb alati teostada „nii kohandatud kujul kui võimalik“. Ehkki see piirang on igati tervitatav, on keeruline kindlaks teha, kas „nii kohandatud kujul kui võimalik“ tähendab seda, et kõikide andmete kogumine on vajalik ja proportsionaalne.

Suunises on sätestatud, et andmete laiaulatuslik kasutamine on endiselt lubatud, „avastamaks uusi või tekkivaid ohte ja muid olulisi riikliku julgeoleku andmeid, mis on sageli peidetud kaasaegse ülemaailmse side suurde ja keerulisse süsteemi“[46]. Artikli 29 töörühma sõnul on suunises öeldud, et „signaaliluure andmete laiaulatuslik kogumine tähendab suure koguse signaaliluure andmete heakskiidetud kogumist, mis tehnilistel või operatiivsetel kaalutlustel toimub ilma kategooriate kasutamiseta (nt eritunnuste, valiku jms alusel)“.

Suunises on piiratud laiaulatuslikult kogutavate signaaliluure andmete kasutamise eesmärke. Need kuus eesmärki, mille jaoks võib andmeid laiaulatuslikult koguda, hõlmavad terrorismivastast võitlust ja muid raske (rahvusvahelise) kuritegevuse vorme. Artikli 29 töörühma analüüs näitab, et eesmärgi piiramine on võrdlemisi ulatuslik (ja võimalik et liiga ulatuslik), et pidada seda sihipäraseks.

Suunisega ei ole kaotatud võimalust koguda isikuandmeid laiaulatuslikult ja valimatult, lisaks on sellise kogumisvõimaluse ulatus ebaselge ja tõenäoliselt suur. Seepärast juhib artikli 29 töörühm tähelepanu VI lisas esitatud ODNI kinnitusele, mille kohaselt „kõik laiaulatusliku kogumisega seotud tegevused seoses internetisidega, mida USA luureteenistus teostab signaaliluure kaudu, hõlmavad väikest osa internetist“[47]. Töörühm sooviks saada selle kohta läbipaistvusmeetmete kaudu lisatõendeid.

3.3.2. Välisluure jälitustegevuse seadus

FISA paragrahvis 215 ja 702 sätestatud vähendamismenetlused on sisse seatud selleks, et kaitsta USA isikuid valitsuse kaugeleulatuva juurdepääsu eest nende andmetele. Need piiranguid välismaalaste suhtes ametlikult ei kohaldata, ehkki USA valitsuse ametnikud on väitnud korduvalt nii avalikel kui ka eraviisilistel kohtumistel artikli 29 töörühma

[46] PPD-28 paragrahv 2 ning Privacy Shield VI lisas esitatud riikliku luurejuhi ameti (ODNI) kiri USA riiklike julgeolekuasutuste suhtes kohaldatavate kaitsemeetmete ja piirangute kohta, lk 3.

[47] Privacy Shieldi VI lisas esitatud riikliku luurejuhi ameti (ODNI) kiri USA riiklike julgeolekuasutuste suhtes kohaldatavate kaitsemeetmete ja piirangute kohta, lk 4. Artikli 29 töörühm tuletab sellega seoses meelde aruannet ELi-USA ajutise andmekaitsetöörühma ELi kaasesimeeste järelduste kohta, kus on öeldud, et „sideandmed moodustavad üleilmsest internetiliiklusest väga väikese osa“, sest „lõviosa üleilmsest internetiliiklusest moodustub suuremahulistest voogedastustest ja allalaadimistest, nagu televisioonisarjad, filmid ja spordiülekanded“ (aruande punkt 3.1.2).

esindajatega, et vähendamismenetluste kohaldamisala on praktikas laiendatud, et hõlmata kõik isikud olenemata nende kodakondsusest ja alalisest elukohast.

Paragrahvis 702 on sätestatud, et andmete heakskiidetud kogumine „toimub viisil, mis on kooskõlas Ameerika Ühendriikide põhiseaduse neljanda muudatusega, millega piiratakse andmete kogumist sellega, mida peetakse mõistliku otsingu põhimõttega kooskõlas olevaks. Selles küsimuses ei tehta mingit vahet USA äriühingute ja väljaspool USAd asutatud äriühingute vahel“. Teisisõnu – kui neljandat muudatust kohaldatakse kõikide USAs kogutavate andmete suhtes, on USAs toimuv andmete laiaulatuslik kogumine „ebamõistlik“ ja seega põhiseadusega vastuolus.

Artikli 29 töörühm toetab PCLOBi aruandes esitatud järeldust, et „praktikas saavad eri asutuste vähendamise ja/või eesmärgistatud kasutamisega seotud menetlustes ette nähtud juurdepääsu- ja säilitamispiirangutest kasu ka isikud väljastpoolt USAd, kuivõrd USA isikute teabe kindlakstegemise ja suurest andmekogumist eraldamise kulukuse ja keerukuse tõttu käsitletakse tavaliselt kogu andmekogumit kooskõlas kõige rangemate USA andmekaitsestandarditega“.

Edasi märgib artikli 29 töörühm, et PCLOBi järelduste kohaselt „ei toimi programm teabevahetuse laiaulatusliku kogumise kaudu“. Seda järeldust on kinnitatud ODNI avaldatud 2014. aasta statistilises läbipaistvusaruandes. Peale selle kasutatakse PCLOBi aruande andmeil jälgimise sihtmärgiks võtmiseks valikutingimusi, näiteks e-posti aadresse või telefoninumbreid[48].

Asjaomased kättesaadavad avalikud eeskirjad, mis käsitlevad sihtmärgiks võtmist, ei sisalda aga selliseid konkreetseid ettekirjutusi. Nende eesmärk on üksnes vältida USA isikute või USAs alaliselt elavate isikute sihtmärgiks võtmist. Lisaks ei ole hüved, mida kohaldatakse PCLOBi andmeil väljastpoolt USAd pärit isikute suhtes, praktikas õiguslikult siduvad ega seadusega paika pandud, sest sihtmärgiks võtmist käsitlevate olemasolevate õigusaktidega ei ole selliseid konkreetseid eeskirju ette nähtud, vaid on üksnes püütud vältida USA isikute või USAs alaliselt elavate isikute sihtmärgiks võtmist.

Samuti tuletab artikli 29 töörühm meelde, et paragrahvi 702 tähenduses ei ole isik mitte üksnes üksikisik, vaid ka rühm, üksus, ühendus, korporatsioon või võõrvõim. Pealegi jätab kogumise õigustamine väitega, et „kogumise oluliseks eesmärgiks on saada välisluureinfot“, teatava ebakindluse eesmärgi ja vajalikkuse suhtes. Töörühmale valmistab siiski heameelt VI lisas esitatud teave, et 2014. aastal jälgiti paragrahvi 702 alusel kokku ligikaudu 90 000 isikut[49]. Privacy Shieldi esimesel läbivaatamisel on võimalik esitada sihtmärgiks võtmise eeskirjade kohta lisatõendeid.

Siiani ei ole olemas otsustavat kohtupraktikat, milles oleks käsitletud isikuandmete massilise ja valimatu kogumise ning kuritegevuse vastase võitluse eesmärgil edaspidise töötlemise seaduslikkust, sealhulgas küsimust, millistel tingimustel selline isikuandmete kogumine ja

[48] PCLOBi aruanne FISA paragrahvi 702 kohaselt rakendatava jälgimisprogrammi kohta, lk 32.
[49] VI lisa, lk 11.

kasutamine võib toimuda. Euroopa Liidu Kohus peaks käsitlema seda küsimust 2016. aasta jooksul vähemalt mõnel määral nii liidetud kohtuasjades Tele2 Sverige AB *vs.* Post- och telestyrelsen ja Secretary of State for the Home Department *vs.* Davis jt[50] kui ka nõuannetes, mida antakse Kanadaga sõlmitud broneeringuinfo vahetamise lepingu kehtivuse kohta[51]. Seni tuletab artikli 29 töörühm meelde oma korduvalt väljendatud seisukohta, et andmete massilist ja valimatut kogumist ei saa mingil juhul lugeda proportsionaalseks[52].

3.3.3. Järeldused

Hoolimata PPD-28 vastuvõtmisega kehtestatud piirangutest ei ole artikli 29 töörühm lakanud muretsemast, eeskätt andmete kogumise proportsionaalsuse pärast. Esiteks leidub märke sellest, et USA jätkab andmete massilist ja valimatut kogumist või vähemalt ei välista võimalust, et ta võib seda tulevikus teha. Artikli 29 töörühm on korduvalt leidnud, et selline andmete kogumine ei ole ELi õigusega kooskõlas ja on seetõttu lubamatu.

Teiseks märgib artikli 29 töörühm, et massiliseks võib pidada ka andmete sihipärast töötlemist või töötlemist, mida teostatakse „nii kohandatud kujul kui võimalik“. Seda, kas sellist andmete massilist kogumist tuleks lubada või mitte, arutatakse praegu Euroopa Liidu Kohtus pooleli olevates menetlustes. Seepärast ei anna töörühm andmete sihipärase, ent massilise töötlemise seaduslikkuse kohta lõplikku hinnangut. Sellegipoolest rõhutab ta, et andmete sihipärase, kuid massilise töötlemise lubamise korral ei tuleks sihtmärgiks võtmise põhimõtet kohaldada mitte ainult lihtsalt kasutamisel, vaid ka andmete kogumisel ja edaspidisel kasutamisel. Igal juhul tuleb piisavusotsuse eelnõus selgitada suunises PPD-28 nimetatud kuut eesmärki, mille jaoks võib andmeid laiaulatuslikult koguda. Artikli 29 töörühm ei ole praeguses etapis veendunud, et need eesmärgid on piisavalt piiratud tagamaks, et andmete kogumisel piirdutakse tõepoolest sellega, mis on vajalik ja proportsionaalne.

3.4. Tagatis C. Olemas peaks olema sõltumatu järelevalvemehhanism

USA-l ei ole föderaaltasandil üht ühtset järelevalvemehhanismi, mille ülesanne oleks jälgida luure- ja jälgimisprogrammide mõju eraelu puutumatusele ja andmekaitsele. Pigem tehakse USA luuretegevuse üle mitmetasandilist järelevalvet, mille puhul saab eristada sise- ja välisjärelevalvet. Artikli 29 töörühm tunnistab, et USA järelevalveorganite aruandluskord on väga üksikasjalik ja enamasti avalik.

3.4.1. Sisejärelevalve

Kõikidel luure- ja julgeolekuasutustel on töötajad, kes vastutavad selle eest, et oleks tagatud kooskõla asjaomase õigusraamistikuga, sealhulgas peainspektor, kelle esmane ülesanne on hinnata asutuste töö üldist kooskõla õigusaktidega, sealhulgas nendega, mis on seotud eraelu puutumatuse ja andmekaitsega. Peainspektori ametikoht on kindlaks määratud statuudiga ja kõik peainspektorid on nimetanud (või varsti nimetab) ametisse president pärast senati

[50] Euroopa Liidu Kohus, liidetud kohtuasjad C-203/15 ja C-698/15.
[51] Euroopa Liidu Kohus, kohtuasi A-1/15.
[52] WP215, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_et.pdf.

kinnitust. Sellega püütakse tagada, et peainspektorid on organisatsiooniliselt sõltumatud ja annavad aru kongressile. Seepärast leiab artikli 29 töörühm, et peainspektorid vastavad tõenäoliselt Euroopa Liidu Kohtu ja Euroopa Inimõiguste Kohtu määratletud organisatsioonilise sõltumatuse kriteeriumile, vähemalt alates hetkest, mil kõigi suhtes kohaldatakse uut ametisse nimetamise korda. Esialgu on veel põhjust muret tunda seoses peainspektoritega, kelle nimetab ametisse selle asutuse direktor, mille üle nad järelevalvet teostavad.

Peainspektorid võivad esitada soovitusi, mis võidakse edastada justiitsministeeriumile ja PCLOBile või isegi kongressi komiteele, kes võib soovitused ellu viia. Kui peainspektor avastab rikkumise, võidakse sellega tegeleda sise- ja poliitikameetmete abil ning sellest võidakse teada anda kongressile. Peainspektoril on näiteks õigus teha nii auditeid kui ka kontrolle.

Artikli 29 töörühm märgib, et peainspektori aruanded võib jätta avalikustamata ja samuti võidakse teda takistada aru andmast, kui kontrollitav teave on salastatud. Samal ajal on aruanded alati kongressi järelevalve all, mis on oluline kaitsemeede, isegi kui see ei anna alust saada individuaalset õiguskaitset.

Kõikides asutustes on eraelu puutumatuse ja kodanikuvabadustega tegelevad ametnikud, kes aitavad kongressil teostada järelevalvet kohustusliku aruandlussüsteemi üle.

Kasutusele võetud sisejärelevalvemehhanisme võib üldjoontes pidada võrdlemisi usaldusväärseteks. Et õigustada sekkumist eraelu puutumatuse ja andmekaitsega seotud põhiõigustesse, peaks järelevalve olema siiski täiesti sõltumatu. Ehkki artikli 29 töörühm austab ja hindab eraelu puutumatuse ja kodanikuvabadustega tegelevate eri ametnike tööd, ei saa ta järeldada, et kõnealuste ametnike sõltumatus küündib tasemeni, mis on vajalik tegutsemiseks sõltumatu järelevalvajana.

3.4.2. Välisjärelevalve

Välisjärelevalve koosneb mitmest mehhanismist: FISA paragrahvide 501 ja 702 kohane FISA kohtu tagatud kohtulik järelevalve, kongressi luurekomiteede teostatav järelevalve ja PCLOBi täidetavad ülesanded.

Artikli 29 töörühm tuletab meelde, et menetluse sõltumatuse ja erapooletuse tagamiseks peaks järelevalve olema kohtuniku käsutuses, mida on väitnud ka Euroopa Liidu Kohus ja Euroopa Inimõiguste Kohus. Veel hiljuti oli FISA kohtu menetlus *ex parte* menetlus, mille puhul asjaomastel isikutel puudus võimalus arvamust avaldada või isegi juhtumist teadlik olla. Ka praegu on FISA kohtu menetlus *ex parte* menetlus, kuid pärast USA vabadusseaduse vastuvõtmist võeti FISA kohtus kasutusele *amicus curiae* rolli täitvad isikud. *Amicus curiae* tegutseb sõltumatult, kuid ei ole mõeldud kaitsma konkreetseid isikuid, keda kohtuasi võib puudutada.

USA vabadusseadusega loodi *amicus curiae*'de rühm, kes koostab FISA kohtule kokkuvõtteid oluliste juhtumite kohta. Kohus on valinud välja viis juristi, kes on saanud

asjakohase juurdepääsuloa ning kes annavad tehnilist nõu, osalevad FISA kohtu istungitel, koostavad kokkuvõtteid ja vaatlevad kohtuasja põhjendatust eraelu puutumatuse ja kodanikuõiguste vaatenurgast. Nad teevad seda siiski vaid oluliste kohtuasjade või uute õigusküsimuste esilekerkimise korral[53].

Paragrahv 215 on allutatud peaaegu täielikult eelnevale (kuid mitte järgnevale) kohtulikule järelevalvele, sest kõikide programmide puhul, mille raames kasutatakse andmete kogumisel õigusliku alusena paragrahvi 215, tuleb saada FISA kohtu heakskiit. PCLOBi aruandes on öeldud, et „paragrahv 702 erineb sellest tavapärasest FISA kohasest elektroonilise jälgimise raamistikust nii kohaldatavate standardite kui ka FISA kohtu individualiseeritud korralduste puudumise poolest. Statuudi alusel korraldavad justiitsminister ja riiklik luurejuht iga-aastase sertifitseerimise, millega lubatakse võtta välisluureinfo kogumise sihtmärgiks isikuid, kes ei ole USA kodanikud ja kelle puhul on piisavalt alust arvata, et nad asuvad väljaspool Ameerika Ühendriike, täpsustamata FISA kohtule, millistelt mittekodanikelt konkreetselt andmeid kogutakse. [---] Samuti ei ole ühtki nõuet, mille kohaselt valitsus oleks kohustatud esitama põhjendatud kahtlused, mis annavad alust uskuda, et paragrahviga 702 on võetud sihikule võõrvõim või võõrvõimu esindaja, nagu nõutakse FISAs“[54].

Kongressis on kongressi luurekomiteedel samuti järelevalveülesanne kiita heaks luuretegevus, eeskätt eelarve hääletamise kaudu. Senati ja esindajatekoja luurekomiteed saavad salastatud kokkuvõtteid luuretegevuse kohta. Justiitsminister peab andma nendele komiteedele iga kuue kuu tagant aru FISA kohasest elektroonilisest jälgimisest. Artikli 29 töörühmale jääb selgusetuks, millises ulatuses saavad nad arutada konkreetsete isikute andmete töötlemist, eriti kui tegemist ei ole USA kodanikega.

PCLOB on USA valitsuse täitevvõimu sõltumatu osa, millele on antud kaks alusõigust: 1) vaadata läbi ja analüüsida meetmeid, mida täitevvõim võtab kaitsmaks riiki (USAd) terrorismi eest, tagades, et vajadus selliste meetmete järele on tasakaalus vajadusega kaitsta eraelu puutumatust ja kodanikuvabadusi, ning 2) tagada, et selliste õigusnormide ja tegevuspõhimõtete väljatöötamisel ja rakendamisel, mis on seotud püüdlustega kaitsta riiki terrorismi eest, võetaks asjakohaselt arvesse ka vabadusi. Artikli 29 töörühm märgib, et PCLOBil on õigus anda kohtukorraldusi ja pääseda ligi salastatud teabele. Oma ülesannete täitmise raames kontrollib PCLOB ka programmide tõhusust. PCLOB ei teosta järelevalvet mitte enne, vaid pärast asjaolu ilmnemist. PCLOB on tõestanud oma sõltumatust, kui ta oli õigusküsimustes Ameerika Ühendriikide presidendiga eri meelt. Eelkõige leidis PCLOB, et paragrahvi 215 kohase telefoniside metaandmete programmi rakendamine ei ole õiguspärane, ja järeldas, et see ei ole tõhus, sest puuduvad tõendid nurjatud rünnakute kohta. Samuti uuris PCLOB aasta vältel paragrahvi 702 kohast programmi ning jõudis järeldusele, et see on õiguspärane ja statuudiga selgelt lubatud ning et paragrahv 702 on osutunud väga tõhusaks, kaasa arvatud terrorismiküsimustes. Lõpuks vaatles PCLOB läbipaistvusnõuet ja leidis, et hulk salastatud asjaolusid ei peaks olema salastatud. Teadaolevalt annab PCLOB

[53] USA vabadusseaduse IV jaotise „Vastuluurekohtu reformid“ paragrahv 401 „*Amicus curiae*’de ametissenimetamine“.
[54] PCLOBi aruanne FISA paragrahvi 702 kohaselt rakendatava jälgimisprogrammi kohta, lk 24 ja 25.

lähitulevikus aru PPD-28 rakendamisest. Sellega seoses leiab PCLOB, et välismaalasega seotud teabe säilitamiseks ei piisa lihtsast asjaolust, et asjaomane isik on välismaalane.

Lõpetuseks märgib artikli 29 töörühm, et korralduses 12333 ei ole selle alusel elluviidavate jälgimisprogrammide jaoks ette nähtud mingit kohtuliku läbivaatamise, järelevalve- ega õiguskaitsemehhanismi.

3.4.3. Järeldused

Piisavusotsuse eelnõust on näha, et USAs rakendatakse nii sise- kui ka välisjärelevalvemehhanisme hõlmavat mitmetasandilist lähenemist. Ehkki järelevalvemehhanismide toimimine võib tekitada segadust, on artikli 29 töörühm rahul sellega, et üldiselt on kehtestatud piisavad sisejärelevalvemehhanismid. Samal ajal tunneb töörühm muret sellepärast, et korralduse 12333 alusel rakendatavate jälgimisprogrammide järelevalve on ebapiisav.

Artikli 29 töörühm märgib, et tema varasemat kriitikat selle kohta, et FISA kohtus toimuvad menetlused ei ole võistlevad, on vaid mõnevõrra leevendanud kasutusele võetud *amici curiae*, kelle ülesanne on suurendada „üksikisiku eraelu puutumatuse ja kodanikuvabaduste kaitset“. Sellegipoolest ei taga FISA kohus tõhusat kohtulikku järelevalvet väljastpoolt USAd pärit isikute andmete kogumise üle. Mõned kahtlused on säilinud ka seoses FISA kohtu suutlikkusega tõhusalt hinnata eesmärgistatud kasutamise ja vähendamisega seotud menetlusi, millele on viidanud ka PCLOB[55].

3.5. Tagatis D. Üksikisikule peavad olema kättesaadavad tõhusad õiguskaitsevahendid

3.5.1. Kohtulikud õiguskaitsevahendid

3.5.1.1. Kaebeõiguse nõue

Kohtulikke õiguskaitsevahendeid käsitlev USA süsteem sisaldab üht olulist piirangut: USA põhiseaduses on nõue, et üksikisik peab tõendama oma kaebeõigust, st „nõue, et hagejad on kandnud või kannavad otsest kahju ja et seda kahju on võimalik heastada. Föderaaltasandil ei ole võimalik pöörduda kohtusse pelgalt põhjusel, et isik või isikute rühm ei ole rahul valitsuse tegevuse või seadusega“[56]. Selle nõude tundub nullivat selliste isikute teavitamatajätmine, kes jäävad jälgimise alla isegi pärast meetmete lõppemist. Euroopa Liidu Kohus ja Euroopa Inimõiguste Kohus on korduvalt sedastanud, et üksikisikutel peaks olema ligipääs halduslikele või kohtulikele õiguskaitsevahenditele. Euroopa Inimõiguste Kohus on Zakharovi otsuses kinnitanud, et kohtupraktika põhjal võib kohtusse minna igaüks, kellel on õiguspärane põhjus kahtlustada sekkumist oma põhiõigustesse[57].

[55] PCLOBi aruanne FISA paragrahvi 702 kohaselt rakendatava jälgimisprogrammi kohta, lk 11.
[56] https://www.law.cornell.edu/wex/standing; https://www.law.cornell.edu/wex/standing; https://www.law.cornell.edu/wex/standing; Clapper *vs.* Amnesty International USA.
[57] Zakharovi kohtuotsus, punkt 171.

Peale selle ei ole Ameerika Ühendriikide ülemkohtu praktika kohaselt tagatud USAs täielikku põhiseaduslikku kaitset väljaspool USAd asuvatele välismaalastele[58]. See on nii eeskätt seoses põhiseaduse neljanda muudatusega, millega kaitstakse USA kodanikke – kuid mitte mittekodanikke – põhjendamatute läbiotsimiste ja konfiskeerimiste eest ning millest tuleneb suur osa USA õigusest eraelu puutumatusele. Euroopa kodanikud ja muud Euroopa isikud, kes elavad väljaspool USAd, on neljanda muudatusega ette nähtud kaitse alt lihtsalt välja jäetud[59].

Õiguskaitseseaduse (*Judicial Redress Act*) piiratud kohaldamine (nii sisulisest küljest, kuna sellest on välja jäetud riiklik julgeolek, kui ka pidades silmas isikuid, kes saavad sellele seadusele tugineda), arvukad erandid ja õiguslik ebakindlus seoses asutustega, mille suhtes seda seadust kohaldatakse, ei vasta nõudele tagada tõhus õiguskaitsemehhanism kõikidele üksikisikutele, kes on seotud jälgimisjuhtumitega riikliku julgeoleku huvides toimuva luuretegevuse raames.

3.5.1.2. Presidendi poliitikasuunis nr 28

Artikli 29 töörühm märgib, et PPD-28 on üksnes suunis ja seepärast ei saa luua sellega üksikisikutele mingeid õigusi. Seda saab teha üksnes õigusaktiga. Seepärast ei ole üksikisikutel võimalik minna suunisega PPD-28 ette nähtud kaitsemeetmete väidetava rikkumise korral kohtusse.

3.5.1.3. Välisluure jälitustegevuse seadus

FISA alusel on üksikisikutel ebaseadusliku jälgimise korral teatavad õiguskaitsevahendid. FISAs on sätestatud, et „kahju kannatanud isikul, välja arvatud võõrvõimul või selle esindajal [---], kelle puhul on teostatud elektroonilist jälitustegevust või kelle kohta elektroonilise jälitustegevuse raames saadud teave on avalikustatud või seda kasutatud käesoleva jao paragrahvi 1809 rikkudes, on õigus esitada hagi sellise rikkumise toime pannud isiku suhtes“. Selle sättega on sõnaselgelt välja jäetud meetmega hõlmatud võõrvõim või selle esindaja. Nagu juba öeldud, tuleb hagejal sellegipoolest tõendada, et tal on kaebeõigus, mis ei ole praktikas võimalik.

USA vabadusseadusega on loodud FISA kohtu juurde *amicus curiae*’dest koosnev nõuandekomisjon, kes annab (soovi korral) nõu oluliste uute õigusküsimuste tõlgendamisel. Selle komisjoni ülesanne on aga pakkuda erapooletut nõu, mitte kaitsta konkreetse üksikisiku taotlusel tema huve.

3.5.2. Halduslikud õiguskaitsevahendid

3.5.2.1. Peainspektorid

Teine võimalus saada õiguskaitset on esitada kaebus peainspektorile. Peainspektorid ei ole siiski kohustatud käsitlema iga kaebust – õigust olla ära kuulatud ei ole, küll aga kehtib

[58] USA *vs.* Verdugo-Urquidez, lk 264–266.
[59] ELi kaasesimeeste aruanne, 2. jagu.

kaalutlusõigus. Peainspektor võib avaldada rikkumisi käsitlevate järelduste kohta ka aruandeid, kui teave ei ole salastatud. Kui üksikisikul on põhjust eeldada, et aruanne mõjutab teda, saab ta pöörduda seaduse rikkumise kohta tehtud järelduse põhjal kohtusse.

3.5.2.2. Teabevabaduse seadus

Kõikidele isikutele kättesaadavaks õiguskaitsevahendiks on võimalus esitada teabevabaduse seadusel (FOIA) põhinev taotlus. USA valitsuse sõnul võib FOIA-l põhineva taotluse esitada sisuliselt iga isik, ükskõik kas ta on USA kodanik või mitte, küsides lihtsalt asutuse käsutuses olevaid andmeid. Siia kuuluvad ka andmed üksikisiku kohta, ehkki sellisel juhul on vajalik tõendada oma isikut. Kui aga teave on riikliku julgeoleku kaitsmiseks salastatud, on ebatõenäoline, et FOIA-l põhinev taotlus rahuldatakse, kuivõrd kehtib erand, mille kohaselt asutused ei ole kohustatud võimaldama juurdepääsu salastatud teabele, sealhulgas juhul, kui teave on seotud isikuga, kes esitas taotluse. FOIA-l põhinevate taotluste alt jääb täielikult välja teave, mis on seotud pooleliolevate õiguskaitsealaste uurimistega. Lõpetuseks ei ole artikli 29 töörühma meelest FOIA-l põhinevate taotlusega tagatud õigust sellele, et töötlemise seaduslikkust kontrolliks sõltumatu asutus.

3.5.3. Privacy Shieldi ombudsman

3.5.3.1. Ombudsmani mehhanismi kasutuselevõtt

Privacy Shieldiga luuakse uus ombudsmani mehhanism, et ELi üksikisikud saaksid esitada USA signaaliluurega seotud taotlusi. Ombudsmani ülesandeid täidab aseriigisekretär Catherine Novelli, nagu on selgitatud riigisekretär John Kerry 2016. aasta 22. veebruari kirjale lisatud memorandumis. Ta teeb seda lisaks PPD-28 punkti 4 alapunktiga d loodud rahvusvahelise infotehnoloogiaalase diplomaatia vanemkoordinaatori ülesannete täitmisele. Kõnealuses kirjas ja memorandumis on rõhutatud: „Ombudsman annab aru otse riigisekretärile ja on luureteenistusest sõltumatu.“

Memorandumis on selgitatud, et hoolimata oma ametinimetusest ei menetle Privacy Shieldi ombudsman üksnes selliseid taotlusi, mis käsitlevad riiklike julgeolekuasutuste juurdepääsu andmetele, mida edastatakse EList USAsse Privacy Shieldi kohaselt, vaid ka taotlusi, mis on seotud andmete edastamisega lepingu tüüptingimuste, siduvate kontsernisiseste eeskirjade, (direktiivi 95/46/EÜ artikli 26 kohaste) erandite või „võimalike tulevaste erandite“ alusel, nagu on kirjas memorandumi joonealuses märkuses 2.

Mehhanismi eeldatava toimimise viisi võib kokku võtta järgmiselt: ELi üksikisik esitab taotluse liikmesriigi ametiasutusele, kes on pädev teostama järelevalvet riiklike julgeolekuteenistuste üle, või kesksele ELi üksikisikute kaebuste menetlemise organile, kui see luuakse või ette nähakse. Asutus, kes edastab taotluse ombudsmanile, peab kõigepealt kontrollima, kas taotlus on kõnealuse kirja punkti 3 alapunktis b määratletud moel täielik[60].

[60] b) ELi üksikisikute kaebuste menetlemise organ hakkab järgmiste tegevustega tagama, et taotlus on täielik:
i) kontrollides üksikisiku isikusamasust ja seda, kas üksikisik tegutseb oma nimel ja mitte mõne valitsuse või valitsustevahelise organisatsiooni esindajana;
ii) kindlustades, et taotlus esitatakse kirjalikult ja et see sisaldab järgmisi põhiandmeid:

Pärast seda, kui taotlus on esitatud Privacy Shieldi ombudsmanile ja see leitakse olevat kooskõlas punkti 3 alapunktiga b, annab ombudsman vastuse, milles ta kinnitab, et "i) taotlust on nõuetekohaselt uuritud ja ii) USA seadusi, statuute, täitevvõimu korraldusi, presidendi suuniseid ja asutuste kordasid, millega nähakse ette piirangud ja kaitsemeetmed, mida kirjeldatakse riikliku luurejuhi ameti (ODNI) kirjas, on järgitud, või kui ei ole järgitud, siis et põhimõtete järgimata jätmine on heastatud"[61]. Ombudsman „ei kinnita ega eita, et üksikisik on olnud jälgimise objekt, samuti ei kinnita andmekaitseraamistiku Privacy Shield ombudsman, millist konkreetset õiguskaitsevahendit kohaldati"[62]. Seoses sellega, kuidas ombudsman oma uurimisi teostab, selgitatakse, et Privacy Shieldi ombudsman „töötab tihedas koostöös Ameerika Ühendriikide valitsuse teiste ametnikega, sealhulgas asjakohaste sõltumatute järelevalveasutustega",[63] täpsustades veel, et tal on „võimalik koostööd teha [riikliku luurejuhi ametiga], justiitsministeeriumiga ja teiste Ameerika Ühendriikide asjakohaste rahvusliku julgeoleku tagamisega seotud ministeeriumide ja asutustega, samuti peainspektoritega, teabevabaduse seaduse (Freedom of Information Act) ametnikega ning kodanikuvabaduste ja eraelu puutumatuse küsimustega tegelevate ametnikega"[64]. Selline kooskõlastamine peab tagama, et Privacy Shieldi ombudsman saab saata eespool kirjeldatud kinnitust sisaldava vastuse.

3.5.3.2. Uue ombudsmani mehhanismi hindamine

Artikli 29 töörühm kiidab heaks jõupingutused, mida Euroopa Komisjon ja USA valitsus on teinud, et võtta kasutusele uus mehhanism eesmärgiga parandada õiguskaitset USA jälgimistegevuse korral. Töörühm mõistab selle signaaliluure ja riikliku julgeolekuga seotud suhetes uudse mehhanismi hindamise erilist tähtsust.

Selles punktis hindab töörühm, kuidas Privacy Shieldi ombudsmani mehhanismi loomine on seotud nõudega tagada üksikisikutele võimalus saada õiguskaitset, nagu on ette nähtud hartas, Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis ning Euroopa kohtute praktikas.

3.5.3.3. Kas pelgalt ombudsmani mehhanismi kasutuselevõtust piisab?

Kõigepealt tuleb seada kahtluse alla, kas ombudsmani mehhanismi kasutuselevõttu saab pidada kokkusobivaks harta artikliga 47, kus on nimetatud õigust tõhusale õiguskaitsevahendile erapooletus kohtus[65] – vähemalt juhul, kui tõhusa õiguskaitse saamiseks

---

• kogu teave, mis on taotluse aluseks,
• millist laadi teavet või heastamist taotletakse,
• kas ja milliseid Ameerika Ühendriikide valitsusasutusi arvatakse olevat seotud ja
• milliseid teisi meetmeid on kasutatud taotletava teabe saamiseks või heastamise saavutamiseks ja milline oli nende teiste meetmete kasutamise tulemus;
iii) kontrollides, et taotlus puudutab andmeid, mille kohta on põhjust arvata, et need edastati EList Ameerika Ühendriikidesse andmekaitseraamistiku Privacy Shield, lepingu tüüptingimuste, siduvate kontsernisiseste eeskirjade, erandite või võimalike tulevaste erandite alusel;
iv) tehes esialgse otsuse, et taotlus ei ole põhjendamatu, kiuslik või pahauskselt esitatud.

[61] Raamistiku Privacy Shield III lisa, jagu 4.e.
[62] Raamistiku Privacy Shield III lisa, jagu 4.e.
[63] Raamistiku Privacy Shield III lisa, jagu 2.a.
[64] Raamistiku Privacy Shield III lisa, jagu 2.a.
[65] Põhiõiguste hartat käsitlevates selgitustes on lisaks öeldud, et artiklit 47 tuleb tõlgendada viisil, et see tagab õiguse tõhusale õiguskaitsevahendile kohtus (selgitused põhiõiguste harta kohta, artikli 47 selgitus (2007/C 303/02)).

ei ole muud võimalust. See on tähtis, sest Euroopa Liidu Kohus viitab oma Schremsi kohtuotsuse olulises kaalutluses 95 harta artiklile 47, tehes seda ilma ühegi viiteta sellele, et kõnealust artiklit tuleks jälgimismeetmete kontekstis mõista muudetud kujul. Vastupidi, Euroopa Liidu Kohus kohaldas artiklit 47 juba kohtuasjas Kadi II[66] rahvusvahelise julgeolekuga seotud jälgimismeetmete suhtes[67].

Euroopa Inimõiguste Kohtu praktikas on siiski väga selgeks saanud, et võimalus saada tavalises kohtus õiguskaitset ei ole tingimus, mille alusel võiks jälgimisprogramme lugeda artikliga 8 (ning inimõiguste ja põhivabaduste kaitse konventsiooni artikliga 13) kooskõlas olevaks[68]. Pigem on kohus artikli 8 alusel leidnud, et jälgimistegevuse puhul võib asjakohane kaitsemeede olla õiguskaitse saamine muudes asutustes. Euroopa Inimõiguste Kohtul on muude tõhusat õiguskaitset pakkuvate asutuste suhtes sellegipoolest kõrged ootused – kohus on öelnud, et selline asutus peab olema „järelevalvet teostavatest asutustest sõltumatu ning sel peavad olema piisavad volitused ja pädevused, et teha tõhusat ja pidevat kontrolli“[69].

Kennedy kohtuotsuses ja Klassi kohtuotsuses annab Euroopa Inimõiguste Kohus ülevaate sellest, mida need ootused võivad tähendada salajase jälgimise kontekstis, kui andmesubjekti ei teavitata tema andmete töötlemisest. Mõlemas kohtuotsuses leiab kohus, et asutused olid sõltumatud, eelkõige jälgimist teostanud organitest, ent ka mis tahes muu asutuse ettekirjutustest[70]. Kennedy kohtuotsuses annab kohus heakskiidu sõltumatule ja erapooletule asutusele, kes on vastu võtnud omaenda menetluseeskirjad ja koosneb liikmetest, kes töötavad või on töötanud kohtuasutuses kõrgel ametikohal või on kogenud juristid[71].

Üksikisikute kaebuste läbivaatamisel oli mõlemas kohtuotsuses nimetatud asutustel lisaks juurdepääs kogu asjakohasele teabele, sealhulgas suletud toimikutele. Samuti olid mõlemal volitused põhimõtete järgimata jätmine heastada[72].

Lisaks küsimusele, kas ombudsmani saab käsitada kohtuna, tekib harta artikli 47 teise lõigu kohaldamisel veel üks probleem, kuivõrd selles on sätestatud, et kohus peab olema „seaduse alusel moodustatud“. On aga kaheldav, kas memorandumit, milles on sätestatud uue mehhanismi toimimine, saab pidada seaduseks.

Seetõttu – pidades silmas sisulise samaväärsuse põhimõtet – otsustas artikli 29 töörühm mitte hinnata, kas ombudsmani saab ametlikult käsitada seaduse alusel moodustatud kohtuna, vaid uurida selle asemel põhjalikumalt kohtupraktika peensusi seoses konkreetsete nõuetega, mille

---

[66] Kohtuotsus, Euroopa Kohus, 18. juuli 2013, Euroopa Komisjon ja Ühendkuningriik *vs.* Kadi, liidetud kohtuasjad C-584/10 P, C-593/10 P ja C-595/10 P, ECLI:EU:C:2013:518.

[67] Kadi II kohtuotsus, punktid 97 ja 100: Euroopa Liidu kohtud tagavad kontrolli kõigi liidu õigusaktide seaduslikkuse üle, sealhulgas nende õigusaktide puhul, millega rakendatakse julgeolekunõukogu poolt Ühinenud Rahvaste Organisatsiooni põhikirja VII peatüki alusel vastu võetud resolutsioone (VII peatükk käsitleb tegevust rahu ohustamise, rahu rikkumise ja agressiooniaktide puhul).

[68] Inimõiguste ja põhivabaduste kaitse konventsiooni artikliga 13 kohustatakse liikmesriike tagama, et „[i]gaühel, kelle [---] õigusi ja vabadusi on rikutud, on õigus tõhusale õiguskaitsevahendile riigivõimude ees“. See ei pea olema tingimata kohtuasutus, nagu Euroopa Inimõiguste Kohus on selgitanud Klassi kohtuotsuse punktides 56 ja 67.

69 Klassi kohtuotsus, punktid 56 ja 67.

[70] Klassi kohtuotsus, punktid 21 ja 53.

[71] Komisjonis G 10 oli (kohtuotsuse tegemise ajal) kolm liiget, komisjoni esimehe ülesandeid täitval liikmel pidi olema kohtuasutuses töötamiseks vajalik kvalifikatsioon (Klassi kohtuotsus, punktid 21 ja 53).

[72] Kennedy kohtuotsus, punkt 167; Klassi kohtuotsus, punktid 21 ja 53.

täitmine on vajalik, et õiguskaitsevahendeid saaks lugeda harta artiklites 7, 8 ja 47 ning inimõiguste ja põhivabaduste kaitse konventsiooni artiklis 8 (ja 13) sätestatud põhiõigustega kooskõlas olevaks. Oma edasises analüüsis keskendub töörühm uue mehhanismi kohaldamisala üle arutledes seega järgmistele kriteeriumidele: nõue esitada ombudsmanile taotlus ja saada vastus (kaebeõigus), ombudsmani sõltumatus, ombudsmani volitused pääseda uurimise käigus ligi vajalikele materjalidele, sealhulgas salastatud dokumentidele, ja paluda abi teistelt asutustelt, ning ombudsmani volitused heastada põhimõtete järgimata jätmine.

3.5.3.4. Ombudsmani mehhanismi kohaldamisala

Seoses juurdepääsuga ombudsmani mehhanismile leiab artikli 29 töörühm, et Privacy Shieldi kaitsemeetmed peaksid hõlmama kõiki isikuid, kelle suhtes kohaldatakse ELi õigust. Ei ole vastuvõetav teha vahet kodakondsuse alusel, eriti kui võtta arvesse, et põhiõigused kehtivad ELis kõigile, mitte üksnes ELi passi omanikule. III lisas kõneldakse ELi üksikisikust, ilma et seda isikut oleks lähemalt määratletud. Artikli 29 töörühmal on kahju sellise ebakindluse pärast ja ta soovitab esitada selgituse, et kõikidel isikutel, kelle suhtes kohaldatakse ELi õigust, on õigus sellele, et ombudsman nende taotluse memorandumi tingimustel läbi vaatab. Peale selle peaksid komisjon ja USA esindajad käsitlema küsimust, mil määral kohaldatakse Privacy Shieldi EMP riikide ja Šveitsi kodanikele/elanikele, kes ei olnud varem programmiga Safe Harbor hõlmatud.

Lisaks täheldab artikli 29 töörühm teatavat ebakindlust ombudsmani mehhanismi kohaldamisala suhtes. Memorandumis on sätestatud, et ombudsmani ülesanne on menetleda taotlusi, mis käsitlevad ELi õiguse alusel kõikide kättesaadavate vahendite kaudu EList USAsse edastatavate andmetega seotud riiklikku julgeolekut. Ent samal ajal on memorandumis selgeks tehtud ka see, et sellega luuakse mehhanism „signaaliluure kohta“. Viimati nimetatu annab põhjust eeldada, et hõlmatud on vaid selliste andmete edastamine, mis on kogutud signaaliluure vahendite abil, mis paneb küsima, et kas näiteks FISA alusel kogutud andmeid peetakse signaaliluure andmeteks. See näib olevat nii paragrahvi 702 puhul, nagu on selgitatud ODNI kinnituse leheküljel 10[73]. Töörühmal on siiski kahju, et mõiste „signaaliluure“ kasutamine tekitab selles olukorras tarbetut ebakindlust.

Lisaks ei hõlma ombudsmani mehhanism artikli 29 töörühma meelest taotlusi, mis on seotud õiguskaitseasutuste juurdepääsuga[74]. Kui see on sedasi, siis jääb ebaselgeks, kas sellised asutused nagu Luure Keskagentuur on mehhanismiga hõlmatud.

3.5.3.5. Kaebeõigus ja taotluse menetlemine

USA valitsuse jälgimismeetmega seotud menetluse algatamine Ameerika Ühendriikide tavakohtus on väga keeruline. Artikli 29 töörühm on teadlik, et ülemkohus on eitanud kaebeõiguse olemasolu luurejuhtumite puhul, kus taotluse esitaja ei ole suutnud tõestada „konkreetset, üksikasjalikku ja tegelikku või otsest kahju“[75]. Seepärast on ombudsmani

[73] Privacy Shieldi VI lisa, lk 10.
[74] Memorandum ombudsmani mehhanismi loomise kohta, lk 1.
[75] Clapper *vs.* Amnesty International USA, 568 U.S.(2013) II, lk 10.

mehhanismi loomine tähtis samm, sest sellega tekitatakse võimalus saada mingiski vormis õiguskaitset, mida muidu ei oleks. Seepärast on töörühmal hea meel jaos 3.c esitatud selgituse üle. Selle jao kohaselt ei ole uue mehhanismi kaudu taotluse esitamiseks vaja tõestada, et taotleja andmetele on pääsetud ligi signaaliluuretegevuse kaudu.

Artikli 29 töörühm kiidab üldjoontes heaks ombudsmani mehhanismi raames taotluse esitanud isiku isikusamasuse kontrollimise korra. On igati mõistlik, et selle isiku isikusamasust kontrollitakse ELi territooriumil, nagu seda tehakse ka ELi-USA terrorismi rahastamise jälgimise teise programmi kohase juurdepääsumehhanismi puhul. Küll aga ei saa töörühm aru, miks ELis toimuva kontrolli peaks usaldama „liikmesriigi järelevalveasutustele, kes on pädevad teostama järelevalvet riiklike julgeolekuteenistuste üle“. Esmajoones on Euroopa Liidu lepingu artikli 4 lõike 2 alusel ebatõenäoline, et Euroopa Komisjon saab määrata kõnealustele asutustele ülesandeid, kuivõrd see kuulub selgelt liikmesriikide pädevusse.

Lisaks, võttes arvesse liikmesriikide julgeolekuteenistuste järelevalvemehhanismide mitmekesisust, võib vastavate asutuste kaasamine kahjustada tõsiselt süsteemi tõhusust liikmesriikide kodanike seisukohast. See võib olla nii näiteks juhul, kui ülesanne teostada riiklike julgeolekuteenistuste üle järelevalvet on antud mitmele asutusele ja üksikisikul võib olla keeruline kindlaks teha, milline neist on asjakohane; kui kohaldatavates riigisisestes õigusnormides ei ole ette nähtud võimalust, et üksikisikud võivad võtta ühendust asjakohase järelevalveasutusega, või kui need asutused ei ole loodud nii, et nad sobiksid neile piisavusotsuse eelnõus määratud ülesannete täitmiseks[76]. Võttes arvesse andmekaitseasutuste osalemist Privacy Shieldi kohaldamises ja järelevalves ning nende sarnast rolli terrorismi rahastamise jälgimise teist programmi käsitleva lepingu alusel, oleks mõistlikum määrata see ülesanne liikmesriikide andmekaitseasutustele. Artikli 29 töörühma sõnul on ebatõenäoline, et Privacy Shieldi ombudsmani mehhanismi raames toimuva menetluse käigus hakatakse töötlema salastatud teavet, sest vastuseks saab olla üksnes „põhimõtetega kooskõlas või mitte, kuid heastatud“.

3.5.3.6. Sõltumatus

Riigisekretäri kinnitustes on selgeks tehtud, et ombudsmani ülesandeid hakkab täitma aseriigisekretär, kes allub välisministeeriumile. Ombudsmani nimetab ametisse president ja nõutav on senati kinnitus. Ombudsmani rolli vastuvõtmist ei tule eraldi kinnitada – piisab selle rolli määramisest. Aseriigisekretäri nimetab ametisse USA president, ombudsmani ametis juhendab teda riigisekretär ja tema aseriigisekretäri rolli kinnitab senat. Nagu kirjas ja memorandumis esitatud kinnituses on rõhutatud, on ombudsman „USA luureühendusest sõltumatu“. Artikli 29 töörühmal on siiski kahtlusi, kas ombudsmani mehhanism on loodud kõige sobivama ministeeriumi juurde. Ombudsmani rolli tõhusaks täitmiseks tundub vaja minevat mõningaid teadmisi ja teatavat arusaamist luureteenistuse toimimisest, ent samal ajal on tõepoolest vaja ka piisavat distantsi luureteenistustest, et olla võimeline tegutsema sõltumatult.

[76] Näiteks mõnes ELi liikmesriigis saavad üksikisikud tutvuda riiklike julgeolekuteenistuste käsutuses olevate andmetega üksnes taotluse esitamisel ülemkohtule.

Privacy Shieldiga ei ole ette nähtud erikriteeriume ombudsmani vallandamiseks. Seetõttu on artikli 29 töörühma arusaama kohaselt võimalik isik ombudsmani rollist vabastada samal viisil, nagu ta võidakse vabastada välisministeeriumis aseriigisekretäri rollist, mis võib kahjustada ombudsmani positsiooni sõltumatust.

Aseriigisekretäri määramine välisministeeriumis ombudsmaniks erineb sõltumatuse vaatenurgast ilmselgelt üksikisikule õiguskaitse tagamiseks tavakohtu jurisdiktsiooni kindlaksmääramisest. Seega on küsimus selles, kas ombudsmani saab pidada sõltumatust silmas pidades samaväärseks teiste sõltumatute järelevalveasutustega, mille puhul põhimõtete järgimine on kinnitust leidnud. Jälgimistegevuse puhul on sellisteks asutusteks eeskätt uurimisvolitustega kohus Ühendkuningriigis ja komisjon G 10 Saksamaal.

Seda, kas siin on tegu sama asjaga, tuleb lähemalt hinnata, analüüsides ombudsmanile antud volitusi.

3.5.3.7. Uurimisvolitused

Kohtuasjas Kadi II tehtud otsuses leiab Euroopa Liidu Kohus seoses harta artikliga 47, et „puudutatud isik saab tutvuda tema suhtes tehtud otsuse põhjendustega, lugedes kas otsust ennast või saades oma sellekohase taotluse põhjal teada selle põhjendused, kusjuures pädev kohus võib asjaomaselt ametiasutuselt nõuda kõnealuste põhjenduste teatavaks tegemist, et võimaldada puudutatud isikul kaitsta oma õigusi parimates võimalikes tingimustes“[77]. Euroopa Liidu kohtud peavad tagama, et see otsus põhineb arvestataval faktilisel alusel[78]. Kohtuotsuses on selgelt öeldud, et vähemalt Euroopa Liidu kohtute suhtes „ei saa esitada [---] andmete või tõendite salastatuse või konfidentsiaalsuse vastuväidet“[79]. Seepärast järeldab artikli 29 töörühm, et Euroopa Liidu Kohtu nõuete täitmiseks tuleb ombudsmanile esitada teave ja tõendid, mis toetavad meetme võtmisel kasutatud põhjendusi[80].

Praeguse seisuga on ebaselge, milline on ombudsmani uurimisvolituste ulatus. Ei komisjoni otsuse eelnõus ega ka III lisas olevas välisministeeriumi kirjas ei ole selles küsimuses erilist selgust. Artikli 29 töörühma arusaamise kohaselt peaks ombudsman saama piisavalt teavet, et olla võimeline otsustama, kas julgeolekuteenistuste andmetöötlustoiming sooritatakse kooskõlas seadusega, ja kui mitte, siis kanda hoolt selle eest, et eeskirjade rikkumine saab heastatud. Samal ajal ei ole ei välisministeeriumi kirjas ega komisjoni otsuse eelnõus täpsustatud, kas ombudsmanil on otsene juurdepääs asjaomase isiku kohta säilitatavatele andmetele ja kas ta saab seega korraldada uurimise ise või peab tuginema teiste USA valitsuse ametnike aruannetele.

[77] Kadi II kohtuotsus, punkt 100.
78 Kadi II kohtuotsus, punkt 119.
79 Kadi II kohtuotsus, punkt 125.
[80] Kadi II kohtuotsus, punkt 122; ehkki asjassepuutuv asutus ei pea esitama kogu teavet ja kõiki tõendeid, millel rajanevad meetme võtmisel kasutatud põhjendused.

3.5.3.8. Heastamisvolitused

Memorandumi põhjal jääb võrdlemisi ebaselgeks, millisel moel saab ombudsman nõuda eeskirjade rikkumise heastamist. Peale selle, et puudub selgus uurimisvolituste suhtes, on arusaamatu ka see, kui suures ulatuses saab ombudsman tõhusalt nõuda eeskirjade rikkumise heastamist ja mis on selle tulemus. Kas see tähendab, et andmeid, mis on hangitud eeskirju rikkudes (st ebaseaduslikult), ei tohi enam üheski toimingus kasutada ja need tuleks kustutada?

Peale selle on artikli 29 töörühm aru saanud, et Privacy Shieldiga ei ole ette nähtud võimalust ombudsmani otsust edasi kaevata või taotleda selle läbivaatamist.

Viimaks – kui ombudsman esitab pärast kaebuse läbivaatamist kaebuse esitajale teavet, ei tohi ta paljastada, kas luureteenistuse käitumises on olnud midagi ebaseaduslikku. Antav vastus on alati sama ja ebamäärane. Kadi II kohtuasjas leidis Euroopa Liidu Kohus, et pädev asutus (kui järelevalveasutus) on kohustatud esitama põhjendused, mis sisaldavad kõiki üksikasju, kuigi ELi toimimise lepingu artiklis 296 ei nõuta üksikasjaliku vastuse andmist[81].

3.5.4. Järeldused

Artikli 29 töörühmale valmistab endiselt muret üksikisikutele ette nähtud tõhusate õiguskaitsevahendite puudulikkus. Esmajoones ei ole piisavusotsuse eelnõus antud selget vastust küsimusele, millises olukorras ja millistel tingimustel saavad üksikisikud algatada oma õiguste kindlaksmääramiseks menetluse.

Töörühm kiidab heaks ombudsmani mehhanismis väljenduva alternatiivse õiguskaitsemehhanismi kasutuselevõtu, mis on erakordne muutus ELi ja kolmanda riigi vahelistes suhetes. Kui jätta kõrvale eespool nimetatud vajadus selgitada mõistet „ELi üksikisikud“, luuakse mehhanismiga kõnealustele isikutele lisavõimalus taotleda USA valitsuselt õiguskaitset, tagamaks et taotluse esitaja kõiki isikuandmeid töödeldakse kooskõlas USA seadustega.

Võttes aga ombudsmani mehhanismi hindamisel arvesse sõltumatu kohtuniku standardeid harta artikli 47 tähenduses ning jälgimistegevusega seotud kohtuasjades kehtestatud Euroopa Liidu Kohtu ja Euroopa Inimõiguste Kohtu nõudeid, täheldab artikli 29 töörühm märkimisväärseid puudujääke. Esiteks valitseb mure selle pärast, kas ombudsmani saab pidada (ametlikult ja täielikult) sõltumatuks, eriti kui arvestada poliitilistele ametikohtadele määratud isikute ametist kõrvaldamise suhtelist lihtsust. Teiseks jäävad püsima kahtlused ombudsmani volituste suhtes teostada tõhusat ja pidevat kontrolli. III lisas esitatud teabe põhjal ei ole töörühmal võimalik järeldada, et ombudsmanil on alati otsene juurdepääs kogu teabele ning kõikidele toimikutele ja IT-süsteemidele, mida ta oma hindamiseks vajab, või et ta saaks ka tegelikult kohustada asjassepuutuvaid luureasutusi lõpetama andmetöötlus, mille puhul ei järgita kehtestatud põhimõtteid, eriti lahkarvamuse korral küsimuses, kas andmete

[81] Kadi II kohtuotsus, punkt 116.

töötlemine on kooskõlas seadusega. Võimalik, et lisaselgitused ombudsmani positsiooni ja volituste kohta suudavad artikli 29 töörühma mured hajutada.

3.6. Kokkuvõtvad märkused USA riiklike julgeolekuasutuste suhtes kohaldatavate kaitsemeetmete ja piirangute kohta

Kõigepealt avaldab artikli 29 töörühm komisjonile ja USA ametiasutustele tunnustust kõikide jõupingutuste eest, mis on tehtud selleks, et suurendada läbipaistvust seoses USA jälgimisprogrammide võimaliku mõjuga Privacy Shieldi või ükskõik millise teise vahendi abil edastatud andmetele. Pärast esimesi Snowdeni paljastusi 2013. aasta juunis on astutud märkimisväärseid samme. Sellegipoolest märgib töörühm, et mõni küsimus valmistab endiselt muret. Vaja oleks vähemalt lisaselgitusi Privacy Shieldi kohaste õiguste ja kohustuste kohta.

Artikli 29 töörühma kaks peamist murekohta seisnevad selles, et USA ametiasutused ei ole andmete massilist ja valimatut kogumist täielikult välistanud ning et ombudsmani volitused ja positsioon ei ole esitatud üksikasjalikumalt. Pealegi ei peaks üksikisikute nimel ombudsmani juures menetluse algatamiseks olema pädevad mitte luureteenistuste üle järelevalvet teostavad asutused, vaid riiklikud andmekaitseasutused. Peale selle – ehkki töörühm kahtlemata avaldab tunnustust püüdluste eest lahendada andmekaitseasutuste tõstatatud probleemid – oleksid tervitatavad edasised kaitsemeetmed, mis tagaksid, et USA jälgimisprogrammide põhjustatud võimalik sekkumine oleks demokraatlikus ühiskonnas vajalik.

4. PRIVACY SHIELDI ÕIGUSKAITSETAGATISTE HINDAMINE

4.1. Sissejuhatus

Seoses avaliku sektori asutuste juurdepääsuga isikuandmetele õiguskaitse eesmärgil märgib artikli 29 töörühm, et Privacy Shieldi II lisas esitatud eraelu puutumatusega seotud põhimõtted sisaldavad erandit, mis on identne programmi Safe Harbor eraelu puutumatust käsitlevates põhimõtetes sätestatud erandiga. Seega on erandi üldine laad säilitatud, mis tähendab, et uued Privacy Shieldi põhimõtted muudavad võimalikuks „Ameerika Ühendriikide riiklikku julgeolekut ja avalikku huvi puudutavatel nõuetel või selle riigi sisemisel õigusel põhinevad“ sekkumised nende isikute põhiõigustesse, kelle isikuandmeid edastatakse EList USAsse[82].

Euroopa Kohus heidab Schremsi otsuses ette eeskätt seda, et programmi Safe Harbor käsitlev otsus ei sisalda „mingeid järeldusi selle kohta, et Ameerika Ühendriikides kehtiks riigi tasandil õigusnorme, mille eesmärk oleks piirata võimalikke sekkumisi nende isikute põhiõigustesse, kelle andmeid edastatakse liidust Ameerika Ühendriikidesse“.

Seepärast valmistavad artikli 29 töörühmale rõõmu USA valitsuse püüdlused anda rohkem teavet õigusraamistiku kohta, millele tuginetakse õiguskaitse eesmärgil toimuval sekkumisel Privacy Shieldi alusel edastatavatesse isikuandmetesse, sealhulgas kohaldatavate piirangute ja kaitsemeetmete kohta. Samal ajal rõhutab töörühm, et ta võtab avaliku sektori asutuste

[82] Schremsi kohtuotsus, punkt 87.

juurdepääsu käsitledes arvesse seda, et igasugune sekkumine eraelu ja andmekaitsega seotud põhiõigustesse peab olema demokraatlikus ühiskonnas põhjendatav. Seepärast on töörühm analüüsinud Privacy Shieldi õiguskaitsega seotud tagatisi, kasutades käesoleva arvamuse punktis 1.2 sätestatud raamistikku.

4.2. Euroopa oluliste tagatiste kohaldamine õiguskaitseasutuste juurdepääsul ettevõtete käsutuses olevatele andmetele

4.2.1. Õiguskaitseaustuste juurdepääs isikuandmetele peab olema kooskõlas õigusaktidega ning põhinema selgetel, täpsetel ja ligipääsetavatel eeskirjadel

Privacy Shieldi VII lisa sisaldab USA justiitsministeeriumi kirja, milles „antakse lühike ülevaade peamistest uurimisvahenditest, mida kasutatakse selleks, et saada kaubanduslikke andmeid ja muid registrite andmeid Ameerika Ühendriikide ettevõtetelt kriminaalõiguse täitmise või avaliku huvi (tsiviil- ja regulatiivne) eesmärgil, sealhulgas nende asutuste kehtestatud juurdepääsupiirangutest“.

Kõik VII lisas nimetatud menetlused tulenevad kas otse Ameerika Ühendriikide põhiseadusest (neljas muudatus), õigusaktidest ja menetlusõigusest või justiitsministeeriumi suunistest ja tegevuspõhimõtetest. VII lisas ei ole siiski viidatud eraldi kõikidele õigusaktidele, milles kõnealused menetlused on sätestatud, vaid selle asemel on kirjeldatud lühidalt menetlusi endid. VII lisas on öeldud veel: „Ettevõtjatel on muid õiguslikke aluseid, et vaidlustada haldusasutustest pärit andmetaotlusi, mis põhinevad nende konkreetsel sektoril ja olemasolevate andmete liigil.“ Näidetena on toodud pangasaladuse seadus, õiglase krediidiinfo seadus ja finantsandmetega seotud eraelu puutumatuse seadus.

Artikli 29 töörühm märgib, et õigusaktide, menetluste ja tegevuspõhimõtete raamistik on killustunud ning see, millist õiguslikku alust konkreetse juurdepääsutaotluse suhtes kohaldatakse, sõltub nende andmete laadist, millele juurdepääsu taotletakse, äriühingu liigist, õigusmenetluse tüübist (kriminaal- või haldusmenetlus või muu avaliku huviga seotud menetlus) ja juurdepääsu taotleva üksuse laadist.

Kuna kõik piirangud, mida saab kohaldada piiramaks õiguskaitseasutuste juurdepääsu Privacy Shieldi alusel edastatavatele andmetele, põhinevad põhiseadusel, õigusaktidel ja justiitsministeeriumi läbipaistvatel tegevuspõhimõtetel, võtab artikli 29 töörühm arvesse eeldust, et neile eeskirjadele pääseb ligi. Nende eeskirjade selgust ja täpsust saab siiski hinnata üksnes konkreetse menetlusliigi ja juurdepääsutaotluse järgi eraldi. Seepärast märgib töörühm kahetsusega, et Privacy Shieldi VII lisas esitatud üksikasjade ja otsuse eelnõu järelduste põhjal ei ole võimalik sellist hindamist praegu teha.

4.2.2. Tõestada tuleb vajalikkust ja proportsionaalsust taotletavate õiguspäraste eesmärkide vaatenurgast

Artikli 29 töörühm märgib, et andmetele juurdepääsu taotlemist õiguskaitse eesmärgil võidakse käsitada õiguspärase eesmärgi järgimisena. Näiteks inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 lõikes 2 ollakse nõus avaliku sektori sekkumisega õigusesse

eraelu kaitsele „ühiskondliku turvalisuse [---] huvides, korratuse või kuriteo ärahoidmiseks“. Selline sekkumine on lubatav siiski vaid juhul, kui see on vajalik ja proportsionaalne[83].

Vastavalt Euroopa Liidu Kohtu väljakujunenud praktikale on proportsionaalsuse põhimõtte alusel nõutav, et seadusandlikud meetmed, millega kavandatakse sekkumist õigusesse eraelule ja isikuandmete kaitsmisele, oleksid „*vastava õigusaktiga* taotletavate õiguspäraste eesmärkide saavutamiseks sobivad ega läheks kaugemale sellest, mis on nende eesmärkide saavutamiseks sobiv ja vajalik“[84] (esiletõst lisatud). Seepärast hinnatakse vajalikkust ja proportsionaalsust alati õigusaktis ette nähtud konkreetse meetme alusel.

USA ametiasutused on VII lisas öelnud, et riigiprokurörid ja föderaalsete uurimisasutuste agendid saavad juurdepääsu ettevõtete dokumentidele ja muudele registriandmetele „mitut liiki kohustuslike õigusprotsesside kaudu, sealhulgas vandemeeste kogu (*grand jury*) kohtukorraldused, halduskorraldused ja läbiotsimisorderid“, ning nad võivad saada enda valdusesse muud teabevahetust vastavalt föderaalse kriminaalmenetluse raames antud pealtkuulamise volitustele[85]. Lisaks võivad tsiviilametkonnad ja reguleerivad asutused väljastada organisatsioonidele kohtumääruseid „äridokumentide, elektrooniliselt säilitatud teabe või muude materiaalsete objektide kohta“[86]. Veel on VII lisas sätestatud, et neid õiguslikke menetlusi kasutatakse üldiselt USA ettevõtetelt teabe saamiseks, olenemata sellest, kas ettevõtted on kinnitanud Privacy Shieldi põhimõtete järgimist või mitte, ja „sõltumata andmesubjekti rahvusest“. Teisisõnu tundub, et selle kaitse alla kuuluvad organisatsioonid, mitte üksikisikud ise.

VII lisa kõrval sisaldab Privacy Shieldi põhimõtetele tugineva otsuse eelnõu komisjoni järeldusi selliste USA eeskirjade olemasolu kohta, millega piiratakse sekkumist nende isikute põhiõigustesse, kelle isikuandmeid edastatakse Privacy Shieldi alusel EList USAsse.

Otsuse eelnõus esitatud järeldustes on eeskätt viidatud piirangutele ja kaitsemeetmetele, mida kohaldatakse USA põhiseaduse neljanda muudatuse alusel, mille alusel eeldab õiguskaitseasutuste poolne läbiotsimine ja konfiskeerimine põhimõtteliselt kohtu määrust, mille saamiseks tuleb tõendada „põhjendatud kahtlust“[87]. Samuti on järeldustes viidatud asjaolule, et erandjuhtudel, mil kohtu määrust ei nõuta, peavad õiguskaitseasutused juhinduma mõistlikkuse põhimõttest[88].

Siiski ei selgu nendest järeldustest, kuidas kohaldatakse neid kaitsemeetmeid isikute suhtes, kes ei ole USA kodanikud. Õigupoolest on otsuse eelnõu põhjenduses tunnistatud, et „neljanda parandusega antavad õigused ei laiene USA-välistele isikutele, kes ei ela Ameerika Ühendriikides“[89]. Otsuse eelnõu samas punktis on öeldud, et väljastpoolt USAd pärit isikud

[83] Vt töödokument Euroopa oluliste tagatiste kohta, lk 7–9. Vajalikkuse ja proportsionaalsuse põhimõtete üldise hinnangu leiab artikli 29 töörühma 27. veebruari 2014. aasta arvamusest 01/2014 vajalikkuse ja proportsionaalsuse põhimõtete kohaldamise ja isikuandmete kaitse kohta õigussektoris.
[84] Digital Rights Irelandi kohtutotsus, punkt 46, ja seal viidatud kohtulahendid.
[85] VII lisa, lk 2.
[86] VII lisa, lk 4.
[87] Piisavusotsuse eelnõu, punkt 107.
[88] Privacy Shield, punkt 107.
[89] Piisavusotsuse eelnõu, punkt 108.

saavad „kaudselt kasu kaitse kaudu, mida pakutakse isikuandmeid säilitavatele USA ettevõtetele, kellele laekuvad õiguskaitseasutuste taotlused“. Artikli 29 töörühm peab siiski kahetsusega täheldama, et selles järelduses ei ole viidatud ühelegi õiguslikule allikale – ei õigusaktile ega kohtupraktikale.

Kokkuvõttes märgib artikli 29 töörühm, et uurimisvahendid, mida kasutatakse Ameerika Ühendriikide ettevõtetelt kaubanduslike andmete ja muude registriandmete saamiseks kriminaalõiguse jõustamise või avaliku huvi eesmärgil – sealhulgas piirangud ja kaitsemeetmed, mida kohaldatakse juurdepääsul andmetele – moodustavad keeruka meetmekogumi. Kättesaadava teabe põhjal ei ole võimalik seda süsteemi praegu üldiselt hinnata. Et teha tegelikult kindlaks õiguskaitseasutuste uurimismeetmete vajalikkus ja proportsionaalsus eraelu ja andmekaitsega seotud põhiõiguste puhul, tuleb hinnata iga üksikjuhtumit eraldi.

4.2.3. Olemas peaks olema sõltumatu järelevalvemehhanism

Artikli 29 töörühm juhib tähelepanu asjaolule, et enamiku VII lisas kirjeldatud menetluste jaoks on vaja kohtu otsust, enne kui ametiasutus saab juurdepääsu andmetele (nt kohtu korraldus pealtkuulamis- ja jälgimisseadmete kasutamiseks, kohtu korraldus föderaalse pealtkuulamisseaduse kohaseks jälgimistegevuseks, läbiotsimisorder (artikkel 41)). Tundub siiski, et kõik neist ei eelda kohtu kaasamist. Näiteks võivad „väljastada kohtumääruseid“ tsiviilametkonnad ja reguleerivad asutused[90]. Sellistel juhtudel on võimalus teha kohtumääruse põhjendatuse kohtulik järelkontroll, kuivõrd „halduskorralduse saaja [võib] vaidlustada selle korralduse jõustamise kohtus“[91].

Artikli 29 töörühm märgib olemasoleva teabe põhjal, et seoses õiguskaitseasutuste juurdepääsuga USA ettevõtete käsutuses olevatele andmetele tundub olevat sisse seatud võrdlemisi usaldusväärne sõltumatu järelevalvemehhanism.

4.2.4. Üksikisikule peavad olema kättesaadavad tõhusad õiguskaitsevahendid

Nagu eespool märgitud, ei laiene „neljanda parandusega antavad õigused [---] USA-välistele isikutele, kes ei ela Ameerika Ühendriikides“[92]. See tähendab, et isik, kes ei ole USA kodanik, ei saa vaidlustada läbiotsimisorderit ega kohtumäärust kohtus neljanda paranduse põhjal. Piisavusotsuse eelnõus on öeldud, et väljastpoolt USAd pärit isikud saavad kaudselt kasu kaitse kaudu, mida pakutakse isikuandmeid säilitavatele USA ettevõtetele, kellele laekuvad õiguskaitseasutuste taotlused. Artikli 29 töörühm märgib siiski, et isegi kui see kaitse on tõhus, ei tähenda see, et üksikisikutele on kättesaadavad tõhusad õiguskaitsevahendid, sest õigus tõhusale õiguskaitsevahendile tundub selle stsenaariumi puhul olevat juurdepääsutaotluse saaval ettevõttel, mitte üksikisikul, kelle andmetele juurdepääsu taotletakse.

[90] VII lisa, lk 4.
[91] VII lisa, lk 4.
[92] Piisavusotsuse eelnõu, punkt 108.

VII lisa ei sisalda mingit lisateavet õigusaktidest tulenevate võimalike õiguskaitsevahendite kohta, mis on kättesaadavad väljastpoolt USAd pärit isikutele, juhul kui ametiasutused või ettevõtted tagavad või saavad ebaseaduslikult juurdepääsu nende andmetele.

Artikli 29 töörühm tunneb heameelt selle üle, et hiljuti vastu võetud õiguskaitseseaduses[93] on väljastpoolt USAd pärit isikutele ette nähtud õigused õiguskaitsele. Siiski piirduvad need õigused vaid selgelt kindlaks määratud õiguskaitsevahenditega: õigusega andmete parandamisele ning õigusega juurdepääsule andmetele ja advokaaditasudele, kui „määratud föderaalasutus või selle osa“ keeldub andmete muutmisest või andmetele juurdepääsu võimaldamisest, ning õigus tsiviilõiguskaitsevahenditele andmete „tahtliku ja ettekavatsetud“ avalikustamise korral.

Peale selle ei sobi otsuse eelnõu asjakohaste põhjenduste joonealustes märkustes viidatud USA kohtupraktika, eelkõige City of Ontario *vs.* Quon,[94] Maryland *vs.* King[95] ja Samson *vs.* California,[96] selle hindamiseks, kas isikud, kes ei ole USA kodanikud, saavad esitada kohtusse hagi, et vaidlustada oma eraelu puutumatuse rikkumise seaduslikkus[97]. Kõikides nendes kohtuasjades on käsitletud USA kodanike õigust eraelule ja kõik nad sisaldavad USA ülemkohtu otsuseid, millega piiratakse neljanda muudatuse kohaldamist.

Kokkuvõttes on artikli 29 töörühmal õiguskaitseseaduse vastuvõtmise üle hea meel, ehkki püsima jääb kahtlus, kas tõhusad õiguskaitsevahendid on üksikutele andmesubjektidele tegelikult kättesaadavad.

4.3. Kokkuvõtvad märkused

Artikli 29 töörühmale valmistavad rõõmu USA valitsuse püüdlused anda rohkem teavet õigusraamistiku kohta, millele tuginetakse õiguskaitse huvides toimuval sekkumisel ELi-USA andmekaitseraamistiku Privacy Shield alusel edastatavatesse isikuandmetesse, sealhulgas kohaldatavate piirangute ja kaitsemeetmete kohta.

Artikli 29 töörühm märgib, et õiguskaitseasutuste uurimisvahendite süsteem, mille hulka kuuluvad kohaldatavad piirangud ja kaitsemeetmed, on nii ulatuslik kui ka keerukas ning Privacy Shieldi raames esitatud teave napp. Töörühmal on kahju, et selle piiratud teabe põhjal (st Privacy Shieldi VII lisa ja otsuse eelnõu järeldused) ei saa ta seekord põhjalikult hinnata kohaldatavate eeskirjade ligipääsetavust, etteaimatavust, vajalikkust ja proportsionaalsust.

[93] Õiguskaitseseadus, 2015, H.R. 1428.
[94] City of Ontario, Cal. *vs.* Quon, 130 S. Ct. 2619, 2630 (2010).
[95] Maryland *vs.* King, 133 S. Ct. 1958, 1970 (2013).
[96] Samson *vs.* California, 547 U.S. 843, 848 (2006).
[97] Kohtuasjas Ontario *vs.* Quon leidis kohus, et Ontario linn ei rikkunud oma töötaja neljandast muudatusest tulenevaid õigusi, sest linna juurdepääs asjaomase töötaja erasõnumite sisule oli mõistlik, kuivõrd sellel oli tööga seotud õiguspärane eesmärk ja selle ulatus ei olnud ülemäärane. Seoses kohtuasjaga Samson *vs.* California sedastas kohus, et „neljas muudatus ei keela politseinikul korraldada tingimisi vabastatud isiku läbiotsimist ilma kahtlustuseta “. Kohtuasjas Maryland *vs.* King oli kohus seisukohal, et kui politseinikud sooritavad vahistamise, mille taga on tõenäoline põhjus kahtlusalune tõsise rikkumise eest kinni võtta, ja viivad ta kinnipidamiseks jaoskonda, on vahistatu põse limaskestalt DNA võtmine ja selle analüüsimine, nagu ka sõrmejälgede võtmine ja pildistamine, õiguspärane registreerimisprotseduur, mis on neljanda muudatuse alusel mõistlik.

Olenemata käesolevas arvamuses esitatud töörühma muudest järeldustest Privacy Shieldi kohta võib selline hindamine olla osa raamistiku iga-aastasest läbivaatamisest.

Õiguskaitseasutuste juurdepääsu kohta märgib artikli 29 töörühm, et sisse tundub olevat seatud võrdlemisi usaldusväärne sõltumatu järelevalvemehhanism. Samuti on töörühmal hea meel selle üle, et vastu on võetud õiguskaitseseadus, millega antakse õiguskaitse õigused isikutele, kes ei ole USA kodanikud. Siiski märgib töörühm, et need õigused on oma olemuselt piiratud. Lisaks järeldusele, et isik, kes ei ole USA kodanik, ei saa vaidlustada läbiotsimisorderit ega kohtumäärust neljanda muudatuse põhjal kohtus, püsib mure selle pärast, kas tõhusad õiguskaitsevahendid on üksikutele andmesubjektidele tegelikult kättesaadavad.

5. JÄRELDUSED JA SOOVITUSED

Artikli 29 töörühm rõõmustab eelkõige selle üle, et viis kuud pärast programmi Safe Harbor kehtetuks tunnistamist esitati uus piisavusotsuse eelnõu, mis sisaldab varasema mehhanismiga võrreldes mitut täiustust. Iseäranis meeltmööda on töörühmale suurenenud läbipaistvus, mis on tagatud kaubandusministeeriumi veebisaidil esitatud kahe Privacy Shieldiga ühinenute nimekirjaga, millest üks sisaldab raamistiku põhimõtteid järgivate organisatsioonide andmeid ja teine nende organisatsioonide andmeid, kes on varem kõnealuseid põhimõtteid järginud, kuid enam seda ei tee. Tervitatav on ka suurem läbipaistvus seoses avaliku sektori asutuste juurdepääsuga Privacy Shieldi alusel edastatavatele andmetele kas riikliku julgeoleku või õiguskaitse eesmärgil. Lõpetuseks on töörühmal hea meel teada saada, et nüüdsest on kõikide andmete edastamisel USAsse tagatud sama kaitse – ühe või teise vahendi eelistamiseks ei ole kehtestatud ühtki spetsiaalset õigusnormi.

5.1. Kolm mureküsimust

Jäänud on siiski kolm mureküsimust, mis vajavad artikli 29 töörühma arvates lahendamist.

Esiteks ei kohustata piisavusotsuse eelnõus kasutatud sõnastusega organisatsioone andmeid kustutama, kui need ei ole enam vajalikud. ELi andmekaitseõiguse peamine põhimõte on tagada, et andmeid ei säilitataks kauem, kui on vajalik nende kogumise eesmärgi saavutamiseks. Teiseks järeldab töörühm VI lisa põhjal, et USA valitsus ei välista täielikult andmete massilise ja valimatu kogumise jätkumist. Töörühm on korduvalt leidnud, et selline andmete kogumine on põhjendamatu sekkumine üksikisikute põhiõigustesse. Kolmas mureküsimus on seotud ombudsmani mehhanismi kasutuselevõtuga. Ehkki töörühm tunnustab seda enneolematut sammu, millega luuakse üksikisikutele lisanduv õiguskaitse- ja järelevalvemehhanism, on põhjust muret tunda selle pärast, kas ombudsmanil on tõhusaks toimimiseks piisavad volitused. Vähemalt tuleks selgitada ombudsmani volitusi ja positsiooni tõestamaks, et ombudsman on oma rollis tõeliselt sõltumatu ja et ta suudab pakkuda eeskirjadevastase andmetöötluse puhul tõhusat õiguskaitset.

5.2. Soovituslikud selgitused

Lisaks eespool nimetatud küsimustele on artikli 29 töörühm viidanud käesolevas arvamuses mitmele küsimusele, mille puhul tasub piisavusotsust lähemalt selgitada. Kõige olulisem on vajadus tagada, et Privacy Shieldi alusel kasutatavaid peamisi andmekaitsemõisteid määratletaks ja kohaldataks järjekindlalt. Praegu see nii ei ole. Teretulnud samm oleks lisada Privacy Shieldi korduma kippuvatesse küsimustesse mõistete loetelu koos määratlustega, milles EL ja USA on ideaalis kokku leppinud. Samuti on töörühm jõudnud järeldusele, et ELi isikuandmete edasisaatmist, eriti andmete ulatust, eesmärgi piiramist ja tagatisi, mida kohaldatakse andmete edastamisel esindajatele, reguleeritakse ebapiisavalt. Õiguskaitseasutuste juurdepääsul Privacy Shieldi andmetele valmistab USA õiguskaitsesüsteemi ulatuslikkuse ja keerukuse tõttu nii föderaalsel kui ka osariigi tasandil muret eelkõige õigusaktide vähene etteaimatavus ja piisavusotsuses esitatud teabe piiratus.

Privacy Shieldi piisavusotsus on esimene otsus, mis on koostatud pärast põhimõttelist kokkuleppimist isikuandmete kaitse üldmääruse tekstis. Paljud üksikisikutele tagatud andmekaitse taseme täiustused Privacy Shieldis siiski ei kajastu. Seepärast soovitab artikli 29 töörühm kõnealuse piisavusotsuse – nagu ka teised kolmandate riikide jaoks välja antud piisavusotsused – üsna pea pärast isikuandmete kaitse üldmääruse jõustumist läbi vaadata.

Viimane siin esile tõstetav artikli 29 töörühma soovitus puudutab ühist läbivaatamist. Töörühmal on hea meel, et Privacy Shieldi piisavusotsus vaadatakse kord aastas läbi ning sellesse kaasatakse ulatuslikult andmekaitseasutusi ja teisi asjakohaseid isikuid. Töörühmale meeldiks, kui kõik osalised lepiksid aegsasti enne esimest läbivaatamist kokku ühise läbivaatamise üksikasjades, sealhulgas läbivaatamise aruande koostamises ja esitamises.