II

*(Muud kui seadusandlikud aktid)*

# OTSUSED

## KOMISJONI RAKENDUSOTSUS (EL) 2016/1250,

## 12. juuli 2016,

## isikuandmete kaitse piisavuse kohta ELi-USA andmekaitseraamistikus Privacy Shield vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ

*(teatavaks tehtud numbri C(2016) 4176 all)*

**(EMPs kohaldatav tekst)**

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiivi 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta, ([1]) eriti selle artikli 25 lõiget 6,

pärast konsulteerimist Euroopa Andmekaitseinspektoriga ([2]),

### 1. SISSEJUHATUS

(1) Direktiiviga 95/46/EÜ on kehtestatud eeskirjad isikuandmete edastamiseks liikmesriikidest kolmandatesse riikidesse, kuivõrd edastamine kuulub direktiivi kohaldamisalasse.

(2) Direktiivi 95/46/EÜ artikli 1 ning põhjenduste 2 ja 10 eesmärk on tagada mitte ainult füüsiliste isikute põhiõiguste ja -vabaduste ning eelkõige eraelu puutumatuse põhiõiguse tõhus ja täielik kaitse isikuandmete töötlemisel, vaid ka nende põhiõiguste ja -vabaduste kaitse kõrge tase ([3]).

(3) Seda, et nii Euroopa Liidu põhiõiguste harta artikliga 7 tagatud põhiõigus eraelu puutumatusele kui ka artikliga 8 tagatud põhiõigus isikuandmete kaitsele on olulised, on lisaks rõhutatud ka Euroopa Kohtu praktikas ([4]).

(4) Direktiivi 95/46/EÜ artikli 25 lõike 1 kohaselt peavad liikmesriigid sätestama, et isikuandmeid võib kolmandasse riiki edastada üksnes juhul, kui kõnealuses kolmandas riigis on tagatud nende kaitse piisav tase ning enne andmete edastamist järgitakse direktiivi muude sätete rakendamist käsitlevaid liikmesriigi õigusakte. Komisjon võib leida, et kolmas riik tagab kaitse piisava taseme oma siseriikliku õigusega või endale võetud rahvusvaheliste kohustustega eraelu puutumatuse ja üksikisikute põhivabaduste ja -õiguste kaitsmisel. Sel juhul võib liikmesriikidest isikuandmeid edastada ilma lisatagatisteta, kui direktiivi muude sätete kohaselt vastuvõetud siseriiklikest sätetest ei tulene teisiti.

([1]) EÜT L 281, 23.11.1995, lk 31.
([2]) Vt arvamus 4/2016 ELi-USA andmekaitseraamistiku Privacy Shield piisavusotsuse eelnõu kohta, avaldatud 30. mail 2016.
([3]) Kohtuasi C-362/14: Maximillian Schrems *vs.* Data Protection Commissioner (edaspidi „Schrems"), EU:C:2015:650, punkt 39.
([4]) Kohtuasi C-553/07: Rijkeboer, EU:C:2009:293, punkt 47; liidetud kohtuasjad C-293/12 ja C-594/12: Digital Rights Ireland ja teised, EU:C:2014:238, punkt 53; kohtuasi C-131/12: Google Spain ja Google, EU:C:2014:317, punktid 53, 66 ja 74.

(5) Vastavalt direktiivi 95/46/EÜ artikli 25 lõikele 2 tuleks andmekaitse taset kolmandates riikides hinnata, pidades silmas kõiki andmete edastamise toimingute või andmete edastamise toimingute kogumi asjaolusid, sealhulgas kõnealuses kolmandas riigis kehtivaid nii üldiseid kui ka konkreetse sektori õigusnorme.

(6) Komisjoni otsusega 2000/520/EÜ ([5]) leiti, et direktiivi 95/46/EÜ artikli 25 lõike 2 tähenduses tagavad programmi Safe Harbour eraelu puutumatuse kaitse põhimõtted, rakendatuna kooskõlas Ameerika Ühendriikide kaubandusministeeriumi poolt välja antud nn korduma kippuvate küsimustega, piisava kaitse taseme liidust Ameerika Ühendriikides asuvatele organisatsioonidele edastatavatele isikuandmetele.

(7) Oma 27. novembri 2013. aasta teatistes COM(2013) 846 final ([6]) ja COM(2013) 847 final ([7]) leidis komisjon, et tulenevalt mitmest erinevast tegurist, sealhulgas andmevoogude eksponentsiaalsest kasvust, nende väga suurest tähtsusest Atlandi-ülesele majandusele, programmiga Safe Harbour liituvate USA äriühingute arvu kiirest kasvust ja uuest teabest mõnede USA järelevalveprogrammide ulatuse ja eesmärgi kohta, millega seoses tekkisid küsimused seoses Safe Harbour süsteemiga tagatava kaitse tasemega, tuleb programmi Safe Harbour põhimõtted uuesti üle vaadata ja neid tõhustada. Lisaks tuvastas komisjon programmis Safe Harbour mitmeid puudusi ja vigu.

(8) Tuginedes komisjoni poolt kogutud tõenditele, sealhulgas ELi-USA eraelu puutumatusega tegeleva kontaktrühma ([8]) töötulemustele ning ELi ja USA *ad hoc* töörühmalt ([9]) saadud andmetele USA järelevalveprogrammide kohta, sõnastas komisjon 13 soovitust programmi Safe Harbour läbivaatamiseks. Nimetatud soovitused keskendusid eraelu puutumatust käsitlevate aluspõhimõtete tugevdamisele, eraelu puutumatuse normide läbipaistvuse suurendamisele põhimõtete järgimist kinnitanud USA äriühingutes, USA ametiasutuste paremale järelevalvele, seirele ja kontrollile selle üle, kuidas neid põhimõtteid järgitakse, võimalusele kasutada taskukohaseid vaidluste lahendamise mehhanisme ja vajadusele tagada, et otsuses 2000/520/EÜ sätestatud riikliku julgeoleku ja õiguskaitse erandit kasutatakse ainult rangelt vajalikus ja proportsionaalses ulatuses.

(9) Oma 6. oktoobri 2015. aasta otsusega kohtuasjas C-362/14, Maximillian Schrems *vs.* Data Protection Commissioner, ([10]) tunnistas Euroopa Liidu Kohus otsuse 2000/520/EÜ kehtetuks. Kohus, kes ei analüüsinud programmi Safe Harbour eraelu puutumatuse põhimõtteid sisuliselt, leidis, et komisjon ei tõdenud nimetatud otsuses, et Ameerika Ühendriigid siseriikliku õigusega või endale võetud rahvusvaheliste kohustustega tõepoolest „tagavad" kaitse piisava taseme ([11]).

(10) Euroopa Kohus selgitas sellega seoses, et ehkki direktiivi 95/46/EÜ artikli 25 lõike 6 mõiste „kaitse piisav tase" ei tähenda, et kaitse tase peab olema ELi õiguskorraga tagatuga identne, tuleb seda siiski mõista kui nõuet, et kolmas riik tõepoolest tagaks 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/EÜ koostoimes põhiõiguste hartaga. Kuigi vahendid, mida kolmas riik sellega seoses kasutab, võivad olla erinevad nendest, mida liidus rakendatakse, peavad need vahendid siiski praktikas osutuma tõhusaks ([12]).

(11) Euroopa Kohus heitis otsuse 2000/520/EÜ suhtes ette asjaolu, et see ei sisaldanud piisavalt järeldusi selle kohta, kas Ameerika Ühendriikides kehtib riigi tasandil õigusnorme, mille eesmärk oleks piirata võimalikke sekkumisi nende isikute põhiõigustesse, kelle andmeid edastatakse liidust Ameerika Ühendriikidesse, kusjuures neid sekkumisi on selle riigi asutustel lubatud toime panna, kui nad taotlevad õiguspäraseid eesmärke, nagu riiklik julgeolek, ja kas selliste sekkumiste vastu on olemas tõhus õiguslik kaitse ([13]).

---

([5]) Komisjoni 26. juuli 2000. aasta otsus 2000/520/EÜ vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ piisava kaitse kohta, mis on ette nähtud programmi Safe Harbour eraelu puutumatuse kaitse põhimõtetega ja sellega seotud korduma kippuvate küsimustega, mille on välja andnud Ameerika Ühendriikide kaubandusministeerium (EÜT L 215, 28.8.2000, lk 7).

([6]) Komisjoni teatis Euroopa Parlamendile ja nõukogule: „Usalduse taastamine ELi ja Ameerika Ühendriikide vaheliste andmevoogude vastu", COM(2013) 846 (final), 27. november 2013.

([7]) Komisjoni teatis Euroopa Parlamendile ja nõukogule, mis käsitleb programmi Safe Harbour toimimist ELi kodanike ja ELis asutatud äriühingute seisukohast, COM(2013) 847 (final), 27. november 2013.

([8]) Vt nt Euroopa Liidu Nõukogu, ELi-USA kõrgetasemelise teabevahetuse, eraelu puutumatuse kaitse ja isikuandmete kaitse kontaktrühma lõpparuanne, teatis 9831/08, 28. mai 2008, kättesaadav Internetis aadressil: http://www.europarl.europa.eu/document/activities/cont/201010/20101019ATT88359/20101019ATT88359EN.pdf.

([9]) Aruanne ELi-USA *ad hoc* andmekaitse töörühma Euroopa Liidu kaasesimeeste järelduste kohta, 27. november 2013, kättesaadav Internetis aadressil: http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf.

([10]) Vt joonealune märkus 3.

([11]) Schrems, punkt 97.

([12]) Schrems, punktid 73–74.

([13]) Schrems, punktid 88–89.

(12) Komisjon alustas 2014. aastal USA ametiasutustega läbirääkimisi, et arutada programmi Safe Harbour tugevdamist vastavalt teatises COM(2013) 847 final esitatud 13 soovitusele. Pärast Euroopa Liidu Kohtu otsust kohtuasjas Schrems neid läbirääkimisi elavdati eesmärgiga jõuda võimaluse korral uue piisavusotsuseni, mis vastaks direktiivi 95/46/EÜ artikli 25 nõuetele kooskõlas Euroopa Liidu Kohtu tõlgendusega. Nende läbirääkimiste tulemuseks on käesolevale otsusele lisatud dokumendid, mis avaldatakse ka USA ametlikus teatajas *Federal Register*. Eraelu puutumatuse põhimõtted (II lisa) ning lisade I ja III–VII koosseisu kuuluvates dokumentides esitatud erinevate USA ametiasutuste antud kinnitused ja tagatised moodustavad ELi-USA andmekaitseraamistiku Privacy Shield.

(13) Komisjon on põhjalikult uurinud USA seadust ja tava, sealhulgas nimetatud ametlikke kinnitusi ja kohustusi. Põhjendustes 136–140 kirjeldatud järeldusi arvestades leiab komisjon, et Ameerika Ühendriigid tagavad piisava kaitsetaseme isikuandmetele, mis edastatakse ELi-USA andmekaitseraamistiku Privacy Shield alusel liidust põhimõtete järgimist kinnitanud organisatsioonidele Ameerika Ühendriikides.

## 2. ELI-USA ANDMEKAITSERAAMISTIK PRIVACY SHIELD

(14) ELi-USA andmekaitseraamistik Privacy Shield põhineb kinnituste süsteemil, mille kohaselt USA organisatsioonid kohustuvad järgima teatavaid eraelu puutumatuse põhimõtteid ehk ELi-USA andmekaitseraamistiku Privacy Shield põhimõtteid, sealhulgas täiendavaid põhimõtteid (edaspidi üheskoos „põhimõtted"), mille on välja andnud Ameerika Ühendriikide kaubandusministeerium ja mis on esitatud käesoleva otsuse II lisas. See kehtib nii vastutavatele töötlejatele kui ka volitatud töötlejatele (esindajatele), selle erinevusega, et volitatud töötlejad peavad olema sõlminud lepingu, mille kohaselt nad tegutsevad ainult vastavalt juhistele ELi vastutavalt töötlejalt, keda nad abistavad põhimõtete kohaseid õigusi kasutavate isikute taotlustele reageerimisel ([14]).

(15) Ilma et see piiraks siseriiklikke sätted, mis on vastu võetud direktiivi 95/46/EÜ alusel, on käesolev otsus sellise toimega, et liidu vastutaval töötlejal või volitatud töötlejal on lubatud andmeid edastada USA organisatsioonidele, kes on kinnitanud Ameerika Ühendriikide kaubandusministeeriumile põhimõtete järgmist ja on kohustunud neid järgima. Põhimõtted kehtivad ainult isikuandmete töötlemisele USA organisatsiooni poolt, kuna selliste organisatsioonide poolne andmete töötlemine ei kuulu liidu õigusaktide kohaldamisalasse ([15]). Raamistik Privacy Shield ei mõjuta nende liidu õigusaktide kohaldamist, mis käsitlevad isikuandmete töötlemist liikmesriikides ([16]).

([14]) Vt II lisa jagu III.10.a. Vastavalt jaos I.8.c. esitatud määratlusele otsustab ELi vastutav töötleja isikuandmete töötlemise eesmärgi ja vahendite üle. Lisaks peab esindajaga sõlmitud lepingus olema selgelt sätestatud, kas andmete edasisaatmine on lubatud (vt jagu III.10.a. ii.2.).

([15]) See kehtib ka seoses personaliandmetega, mida edastatakse liidust töösuhte kontekstis. Põhimõtetes rõhutatakse küll ELis asuva tööandja „esmast vastutust" (vt II lisa jagu III.9.d.i.), ent samal ajal selgub neist, et tema käitumisele kehtivad liidus ja/või vastavas liikmesriigis kohaldatavad eeskirjad ja mitte põhimõtted. Vt II lisa jaod III.9.a.i., b.ii., c.i., d.i.

([16]) See kehtib ka andmete töötlemisele, kui selleks kasutatakse liidus asuvaid vahendeid, ent nende kasutajaks on väljaspool liitu registreeritud organisatsioon (vt direktiivi 95/46/EÜ artikli 4 lõike 1 punkt c). Alates 2018. aasta 25. maist kohaldatakse isikuandmete kaitse üldmäärust isikuandmete töötlemisele i) juhul, kui töötlemine toimub liikmesriigi territooriumil paikneva vastutava töötleja või volitatud töötleja asutuse tegevuse raames (isegi juhul, kui töötlemine toimub Ameerika Ühendriikides) või ii) väljaspool liitu asuva vastutava töötleja või volitatud töötleja poolt liidus olevate andmesubjektide isikuandmete töötlemisele, kui töötlemistoimingud on seotud a) kaupade või teenuste pakkumisega liidus asuvatele andmesubjektidele, sõltumata sellest, kas see on seotud maksega või mitte või b) nende tegevuse jälgimisega, kui see tegevus toimub liidus. Vt Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määruse (EL) 2016/679 (füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)) artikli 3 lõiked 1 ja 2 (ELT L 119, 4.5.2016, lk 1).

(16) Raamistikuga Privacy Shield isikuandmetele tagatud kaitse laieneb kõikidele ELi andmesubjektidele, ([17]) kelle isikuandmed on edastatud sellistele USA organisatsioonidele, kes on kinnitanud Ameerika Ühendriikide kaubandusministeeriumile põhimõtete järgmist.

(17) Põhimõtteid kohaldatakse pärast nende kinnitamist viivitamata. On üks erand seoses edasisaatmise põhimõttega seotud vastutusega, seda juhul, kui raamistiku Privacy Shield põhimõtete järgimist kinnitaval organisatsioonil on eelnevalt olemas kaubandussidemed kolmandate isikutega. Kuna nimetatud kaubandussidemete vastavusse viimine andmete edasisaatmise põhimõtte alusel kehtivate eeskirjadega võib osutuda aeganõudvaks, on organisatsioonil kohustus teha seda nii kiiresti kui võimalik ja igal juhul mitte hiljem kui üheksa kuud pärast põhimõtete järgimise kinnitamist (tingimusel et see toimub raamistiku Privacy Shield käivitumispäevale järgneva kahe kuu jooksul). Selle üleminekuaja kestel peab organisatsioon kohaldama teate ja valikuvõimaluse põhimõtet (mis tähendab, et ELi andmesubjektil on keeldumisvõimalus) ja kui isikuandmeid edastatakse kolmandale isikule, kes on esindaja, peab ta tagama, et nimetatud kolmas isik tagab vähemalt samal tasemel kaitse, kui on nõutud põhimõtetes ([18]). See üleminekuperiood loob mõistliku ja sobiva tasakaalu ühelt poolt andmekaitset käsitleva põhiõiguse järgimise ja teiselt poolt ettevõtjate põhjendatud vajaduse vahel saada piisavalt aega uue raamistikuga kohanemiseks, kuna see sõltub ka nende ärisuhetest kolmandate isikutega.

(18) Süsteemi haldab ja kontrollib kaubandusministeerium vastavalt oma kohustustele, mis on esitatud Ameerika Ühendriikide kaubandusministri kinnitustes (käesoleva otsuse I lisa). Seoses põhimõtete järgimise tagamisega on föderaalne kaubanduskomisjon (edaspidi „FTC“) ja transpordiministeerium andnud kinnitused, mis on esitatud käesoleva otsuse lisas IV ja lisas V.

2.1. *Eraelu puutumatuse põhimõtted*

(19) Osana ELi-USA andmekaitseraamistiku Privacy Shield põhimõtete järgimise kohta antavast kinnitusest peavad organisatsioonid kohustuma neid põhimõtteid järgima ([19]).

(20) Vastavalt *teate põhimõttele* kohustuvad organisatsioonid andma andmesubjektidele teavet nende isikuandmete töötlemise mitmete tähtsaimate aspektide kohta (nt kogutavate andmete liik, töötlemise eesmärk, juurdepääsu- ja valikuõigus, edasisaatmise tingimused ja vastutus). Kaitsemeetmeid on veel, eelkõige organisatsioonidele esitatav nõue avalikustada oma eraelu puutumatuse normid (mis on kooskõlas põhimõtetega) ja esitada lingid kaubandusministeeriumi veebisaidile (millel on üksikasjalikumalt kirjeldatud põhimõtete järgimise kinnitust, andmesubjektide õigusi ja olemasolevaid kaebuste käsitlemise mehhanisme), Privacy Shieldi nimekirjale (millele on viidatud põhjenduses 30) ning sobiliku alternatiivse vaidluste lahendamise organi veebisaidile.

(21) Vastavalt *andmete terviklikkuse ja eesmärgi piiramise põhimõttele* tohib koguda üksnes töötlemise eesmärgile vastavaid isikuandmeid, mis on kavatsetud kasutuseks usaldusväärsed, täpsed, täielikud ja ajakohased. Organisatsioon ei tohi isikuandmeid töödelda viisil, mis ei vasta eesmärgile, milleks need koguti või milleks andmesubjekt seejärel loa andis. Organisatsioonid peavad veenduma, et isikuandmed on kavatsetud kasutuseks usaldusväärsed, täpsed, täielikud ja ajakohased.

([17]) Käesolev otsus on EMPs kohaldatav. Euroopa Majanduspiirkonna lepinguga (edaspidi „EMP leping“) on ette nähtud Euroopa Liidu siseturu laiendamine kolmele EMP liikmesriigile Islandile, Liechtensteinile ja Norrale. Andmekaitset käsitlevad liidu õigusaktid, sealhulgas direktiiv 95/46/EÜ, on EMP lepinguga hõlmatud ja need on kaasatud selle XI lisasse. EMP ühiskomitee peab otsustama käesoleva otsuse kaasamise kohta EMP lepingusse. Niipea kui käesolevat otsust hakatakse kohaldama Islandi, Liechtensteini ja Norra suhtes, laieneb ELi-USA andmekaitseraamistik Privacy Shield ka neile kolmele riigile ning raamistikku Privacy Shield käsitlevas paketis esitatud viiteid ELile ja selle liikmesriikidele mõistetakse Islandit, Liechtensteini ja Norrat hõlmavana.

([18]) Vt II lisa jagu III.6.e.

([19]) Lisatagatisi andvad erieeskirjad kehtivad seoses personaliandmetega, mida edastatakse liidust töösuhte kontekstis, nagu on ette nähtud eraelu puutumatuse põhimõtete täienduspõhimõttes „Personaliandmed“ (vt II lisa jagu III.9). Näiteks peaksid tööandjad arvestama töötajate eraelu puutumatuse eelistusi, piirates juurdepääsu isikuandmetele, tehes anonüümseks teatavaid andmeid või määrates neile koode või pseudonüüme. Eelkõige peavad organisatsioonid seda liiki andmetega seoses tegema koostööd liidu andmekaitseasutustega ja järgima nende nõuandeid.

(22) Kui andmete kasutamise uus (muudetud) eesmärk on algsest eesmärgist oluliselt erinev, ent siiski sellega kooskõlas, annab *valikuvõimaluse põhimõte* andmesubjektidele õiguse esitada vastuväide (*opt out*). *Valikuvõimaluse põhimõte* ei asenda sõnaselgelt eesmärgiga vastuolus oleva andmete töötlemise keeldu ([20]). Otseturundusele kehtivad erieeskirjad, mis võimaldavad keelduda isikuandmete kasutamise lubamisest „igal ajal" ([21]). Tundlike andmete korral peab organisatsioonidel üldjuhul olema andmesubjekti konkreetne nõusolek (*opt in*).

(23) Samuti vastavalt *andmete terviklikkuse ja eesmärgi piiramise põhimõttele* võib isikuandmeid säilitada kujul, mis võimaldab isikut tuvastada või muuta isiku tuvastatavaks (ja seega isikuandmete kujul) ainult seni, kuni see vastab eesmärgile või eesmärkidele, milleks need algselt koguti või milleks seejärel luba anti. See kohustus ei takista raamistiku Privacy Shield alusel tegutsevatel organisatsioonidel jätkata isikuandmete töötlemist pikema aja vältel, ent ainult nii kaua ja sellises ulatuses, kui see on mõistlikult vajalik järgnevatel konkreetsetel eesmärkidel: arhiveerimine avaliku huvi eesmärgil, ajakirjandus, kirjandus ja kunst, teadus- ja ajaloouuringud ning statistiline analüüs. Andmete pikaajalisemale säilitamisele ühel neist eesmärkidest kohaldatakse põhimõtetega kehtestatud kaitsemeetmeid.

(24) Vastavalt *turvalisuse põhimõttele* peavad organisatsioonid, mis tekitavad, säilitavad, kasutavad või levitavad isikuandmeid, rakendama „mõistlikke ja kohaseid" turvameetmeid, võttes arvesse töötlemisega seotud riske ning andmete laadi. Edasise töötlemise korral peavad organisatsioonid sõlmima alltöötlejaga lepingu, millega tagatakse põhimõtetes kehtestatuga samal tasemel kaitse, ja astuma samme selle nõuetekohase rakendamise tagamiseks.

(25) *Juurdepääsu põhimõtte* ([22]) alusel on andmesubjektidel õigus ilma põhjendusi esitamata ja ainult mõõduka tasu eest saada organisatsioonilt kinnitus selle kohta, kas kõnealune organisatsioon töötleb nendega seotud isikuandmeid, ja saada mõistliku aja jooksul teavet nende andmete kohta. Seda õigust võib piirata üksnes erandlikel asjaoludel; juurdepääsuõiguse keelamine või piiramine peab olema vajalik ja nõuetekohaselt põhjendatud ning organisatsioonil on kohustus tõendada, et need tingimused on täidetud. Andmesubjektidel peab olema võimalus parandada, muuta või kustutada isikuandmed, mis on ebatäpsed või kui neid on töödeldud põhimõtteid rikkudes. Neis valdkondades, kus on kõige suurem tõenäosus, et ettevõtted töötlevad isikuandmeid automatiseeritult isikut mõjutavate otsuste tegemiseks (näiteks krediidiandmine, hüpoteeklaenud, tööpakkumised), on USA õigusaktidega ette nähtud konkreetsed kaitsemeetmed negatiivsete otsuste eest ([23]). Nendega on üldjuhul sätestatud, et isikul on õigus saada teavet otsuse (näiteks krediidi andmisest keeldumine) aluseks olevate konkreetsete põhjuste kohta, vaidlustada puudulik või ebatäpne teave (samuti toetumine ebaseaduslikele teguritele) ja nõuda heastamist. Nimetatud eeskirjad tagavad kaitse neil tõenäoliselt piiratud arvuga juhtudel, kui automatiseeritud otsused on teinud raamistiku Privacy Shield alusel tegutsev organisatsioon ise ([24]). Sellest hoolimata, kuna kaasaegses digitaalmajanduses tehakse isikut mõjutavaid otsuseid üha rohkem automatiseeritud andmetöötluse (muu hulgas profiilianalüüs) abil, tuleb seda valdkonda tähelepanelikult jälgida. Jälgimise hõlbustamiseks on USA ametiasutustega kokku lepitud, et automatiseeritud otsustusprotsess, sealhulgas ELi ja USA sellega seonduva lähenemisviisi sarnasused ja erinevused, kuulub esimese iga-aastase läbivaatamise ja vajaduse korral ka järgmiste läbivaatamiste päevakorda.

([20]) See kehtib igasugusele raamistiku Privacy Shield alusel andmete edastamisele, sealhulgas juhul, kui see seondub töösuhte kaudu kogutud andmetega. Ehkki põhimõtete järgimist kinnitanud USA organisatsioonil on põhimõtteliselt lubatud kasutada personaliandmeid muudel, töösuhtega mitteseotud eesmärkidel, näiteks teatud turunduskommunikatsioonis, peab ta järgima eesmärgiga vastuolus oleva töötlemise keeldu; lisaks on see lubatud ainult kooskõlas *teate* ja *valikuvõimaluse põhimõtetega*. USA organisatsioonidel on keelatud rakendada sellise valiku teinud töötajate suhtes karistusmeetmeid, sealhulgas töövõimaluste piiramist, ja see tagab, et hoolimata alluvussuhtest ja sellega kaasnevast sõltuvusest ei survestata töötajat ning seega on tema valik ka tegelikult vaba.

([21]) Vt II lisa jagu III.12.

([22]) Vt ka täienduspõhimõte „Juurdepääs" (II lisa jagu III.8).

([23]) Vt näiteks Equal Credit Opportunity Act (ECOA, 15 U.S.C. 1691 et seq.), Fair Credit Reporting Act (FRCA, 15 USC § 1681 et seq.) või Fair Housing Act (FHA, 42 U.S.C. 3601 et seq.).

([24]) Seoses ELis kogutud isikuandmete edastamisega on üksikisikul (kliendil) enamikul juhtudest lepinguline suhe ELi vastutava töötlejaga (kes teeb seega reeglina automatiseeritud töötlemisega seonduvad otsused), kes peab järgima ELi andmekaitsenorme. See hõlmab juhtusid, kui andmeid töötleb raamistiku Privacy Shield alusel tegutsev organisatsioon, kes tegutseb esindajana ELi vastutava töötleja nimel.

(26) Vastavalt *kaebuste käsitlemise, nõuete täitmise tagamise ja vastutuse põhimõttele* ([25]) peavad liikmesorganisatsioonid nägema ette tõhusad mehhanismid, millega tagatakse vastavus muudele põhimõtetele ja kaebuste käsitlemise võimalus ELi andmesubjektidele, kelle isikuandmeid on töödeldud põhimõtteid eirates, sealhulgas tõhusad õiguskaitsevahendid. Kui organisatsioon otsustab ELi-USA raamistiku Privacy Shield raames põhimõtete järgimist kinnitada, ([26]) on tal kohustus põhimõtteid tegelikult järgida. Et organisatsioonil oleks õigus andmekaitseraamistikule Privacy Shield tuginedes jätkuvalt liidust isikuandmeid saada, peab ta enda osalemise raamistikus igal aastal üle kinnitama. Samuti peavad organisatsioonid võtma meetmeid, et kontrollida ([27]) nende poolt avaldatud eraelu puutumatuse normide vastavust põhimõtetele ja seda, et neid ka tegelikult järgitakse. Selleks saab kasutada enesehindamise süsteemi, mis peab hõlmama sisemenetlusi töötajate koolitamiseks organisatsiooni eraelu puutumatuse normide alal ja nõuete täitmise korrapäraseks objektiivseks kontrollimiseks, või välist vastavuskontrolli, mis võib hõlmata muu hulgas auditeerimist ja pistelist kontrolli. Lisaks peavad organisatsioonid kehtestama kaebuste käsitlemiseks tõhusa õiguskaitsemehhanismi (sellega seoses vt ka põhjendus 43) ning tunnustama uurimis- ja nõuete täitmise tagamise õigusi, mis on FTC-l, transpordiministeeriumil või muul Ameerika Ühendriikide volitatud täitevasutusel, kes tagab praktikas põhimõtete järgimise.

(27) Erieeskirjad kehtivad nn edastamisele, st organisatsiooni poolsele isikuandmete edasisaatmisele kolmandast isikust vastutavale või volitatud töötlejale sõltumata sellest, kas nimetatud töötleja asub Ameerika Ühendriikides või kolmandas riigis väljaspool Ameerika Ühendriike (ja Euroopa Liitu). Nende eeskirjade eesmärk on tagada, et ELi andmesubjektide isikuandmetele tagatud kaitsemeetmeid ei kahjustata ega neist ei saa mööda hiilida andmete edastamisega kolmandatele isikutele. See on eriti asjakohane seoses tänapäeva digitaalmajandusele iseloomulike tavalisest keerukamate töötlemisahelatega.

(28) *Kolmandale isikule andmete edastamise eest vastutuse põhimõtte* ([28]) kohaselt võib andmete edastamine toimuda ainult i) piiratud ja konkreetsel eesmärgil, ii) lepingu (või sellega võrdväärse kontsernisisese kokkuleppe) ([29]) alusel ja iii) juhul kui nimetatud lepingust tuleneb samal tasemel kaitse, kui on tagatud põhimõtetega, mis hõlmab ka nõuet, et põhimõtete kohaldamist on võimalik piirata ainult ulatuses, mis on vajalik riikliku julgeoleku, õiguskaitse ja muu avaliku huvi tagamise eesmärgil ([30]). Seda tuleks lugeda koostoimes *teate põhimõtte* ja kolmandast isikust vastutavale töötlejale edasisaatmise korral ([31]) *valiku põhimõttega*, mille kohaselt andmesubjektidele tuleb teada anda (muu hulgas) kolmandast isikust andmete vastuvõtja liik/isik, andmete edastamise eesmärk ja pakutud valik; ka tuleb neid teavitada võimalusest edasisaatmisest keelduda (*opt out*) või tundlike andmete korral sellest, et nad peavad selleks andma oma konkreetse nõusoleku (*opt in*). *Andmete terviklikkuse ja eesmärgi piiramise põhimõtet* arvestades eeldatakse kohustusega anda samal tasemel kaitse, kui on tagatud põhimõtetega, et kolmas isik tohib talle edastatud isikuandmeid töödelda ainult eesmärkidel, mis ei ole vastuolus nende eesmärkidega, milleks andmed algselt koguti või milleks isik seejärel loa andis.

(29) Kohustus tagada samal tasemel kaitse nagu põhimõtetes nõutud, kehtib kõigile kolmandatele isikutele, kes on andmete töötlemisega seotud, sõltumata nende asukohast (USA või muu kolmas riik), samuti juhul kui algne kolmandast isikust andmete vastuvõtja ise edastab nimetatud andmed muule kolmandast isikust vastuvõtjale, näiteks edasise töötlemise eesmärgil. Igal juhul tuleb kolmanda isikuga sõlmitud lepingus ette näha, et nimetatud kolmas isik teavitab raamistiku Privacy Shield alusel tegutsevat organisatsiooni, kui ta leiab, et ei suuda enam seda

([25]) Vt ka täienduspõhimõte „Vaidluste lahendamine ja täitmise tagamine“ (II lisa jagu III.11).
([26]) Vt ka täienduspõhimõte „Põhimõtete järgimise kinnitamine“ (II lisa jagu III.6).
([27]) Vt ka täienduspõhimõte „Kontrollimine“ (II lisa jagu III.7).
([28]) Vt ka täienduspõhimõte „Kohustuslikud lepingud andmete edastamiseks kolmandale isikule“ (II lisa jagu III.10).
([29]) Vt ka täienduspõhimõte „Kohustuslikud lepingud andmete edastamiseks kolmandale isikule“ (II lisa jagu III.10.b). Ehkki see põhimõte võimaldab andmete edastamise ka mittelepinguliste vahendite alusel (näiteks grupisisene vastavuse ja kontrolli programm), sätestab tekst selgelt, et need vahendid peavad „taga[ma] jätkuvalt põhimõtete kohase isikuandmete kaitse“. Lisaks sellele, kuna põhimõtete järgimist kinnitanud USA organisatsioonile jääb vastutus põhimõtete järgimise eest, on tal tugev stiimul kasutada ka praktikas tõhusalt toimivaid vahendeid.
([30]) Vt II lisa jagu I.5.
([31]) Isikutel ei ole keeldumisõigust, kui isikuandmed edastatakse kolmandale isikule, kes täidab agendina ülesandeid USA organisatsiooni nimel ja selle juhiseid järgides. Ent selleks peab agendiga olema sõlmitud leping ja põhimõtetega antud kaitse tagamise eest vastutab USA organisatsioon, kasutades oma järelevalve tegemise õigust.

kohustust täita. Kui selline järeldus tehakse, lõpetab kolmas isik andmete töötlemise või tuleb astuda muid mõistlikke ja asjakohaseid samme olukorra parandamiseks ([32]). Juhul kui andmete (edasise) töötlemise ahelas tekivad probleemid nõuetele vastavusega, peab raamistiku Privacy Shield alusel tegutsev organisatsioon, kes tegutseb isikuandmete vastutava töötlejana, tõestama, et ta ei ole vastutav sündmuse eest, mille tagajärjel kahju tekkis, või võtma muul viisil vastutuse vastavalt *kaebuste käsitlemise, täitmise tagamise ja vastutuse põhimõttele*. Andmete edastamisel kolmandast isikust esindajale kehtivad täiendavad kaitsemeetmed ([33]).

2.2. *ELi-USA raamistiku Privacy Shield läbipaistvus, haldamine ja järelvalve*

(30) ELi-USA raamistikuga Privacy Shield on ette nähtud järelevalve- ja nõuete täitmise tagamise mehhanismid, et kontrollida põhimõtete järgimist nende järgimist kinnitanud USA ettevõtetes ning tagada, et iga eiramise suhtes võetakse meetmed. Nimetatud mehhanismid on sätestatud põhimõtetes (II lisa) ja kohustustes, mille on võtnud kaubandusministeerium (I lisa), FTC (IV lisa) ja transpordiministeerium (V lisa).

(31) ELi-USA raamistiku Privacy Shield nõuetekohase rakendamise tagamiseks peab huvitatud osapooltel, nagu andmesubjektid, andmeeksportijad ja riiklikud andmekaitseasutused (edaspidi „DPAd"), olema võimalik kindlaks teha organisatsioonid, kes põhimõtteid järgivad. Sel otstarbel on kaubandusministeerium võtnud kohustuse hoida ja avalikkusele kättesaadavaks teha loetelu organisatsioonidest, kes on kinnitanud põhimõtete järgimist ning kuuluvad vähemalt ühe käesoleva otsuse I ja II lisas loetletud täitevasutuse pädevusse (edaspidi „Privacy Shieldi nimekiri") ([34]). Kaubandusministeerium uuendab seda nimekirja organisatsioonide iga-aastaste korduskinnituste teatiste alusel ja iga kord, kui mõni organisatsioon loobub osalemisest ELi-USA raamistikus Privacy Shield või sellest eemaldatakse. Samuti kogub ja avalikustab ta usaldusväärseid andmeid organisatsioonide kohta, kes on nimekirjast kustutatud, märkides igaühe kohta ära ka kustutamise põhjuse. Lõpuks lisab ta lingi FTC poolt käsitletavate andmekaitseraamistikuga Privacy Shield seotud täitemenetluste loetelule, mis on avaldatud FTC veebisaidil.

(32) Kaubandusministeerium teeb nii Privacy Shieldi nimekirja kui ka korduskinnituste teatised vastava veebisaidi vahendusel avalikult kättesaadavaks. Põhimõtete järgimist kinnitanud organisatsioonid peavad omakorda esitama ministeeriumi veebilehel oleva Privacy Shieldi nimekirja veebiaadressi. Kui organisatsiooni eraelu puutumatuse normid on kättesaadavad veebis, siis peab neis sisalduma hüperlink andmekaitseraamistiku Privacy Shield veebilehele või hüperlink lahendamata kaebuste uurimiseks ettenähtud sõltumatu kaebuste käsitlemise mehhanismi veebilehele või kaebuse esitamise vormile. Kaubandusministeerium kontrollib seoses organisatsiooni poolse esimese ja iga järgneva andmekaitseraamistikuga seotud kinnituse andmisega, et organisatsiooni eraelu puutumatuse normid oleksid põhimõtetega kooskõlas.

(33) Organisatsioonid, kes ei järgi põhimõtteid püsivalt, eemaldatakse Privacy Shieldi nimekirjast ning nad peavad tagastama või kustutama isikuandmed, mille nad ELi-USA raamistiku Privacy Shield raames said. Muudel nimekirjast eemaldamise juhtudel, näiteks vabatahtliku lahkumise või korduvkinnituse andmata jätmise korral, võib organisatsioon sellised andmed säilitada, kui ta kinnitab kaubandusministeeriumile igal aastal põhimõtetest kinnipidamist või tagab isikuandmetele asjakohase kaitse teiste lubatud meetoditega (näiteks kasutades lepingut, mis sisaldab täies ulatuses asjakohaseid standardseid komisjoni poolt heakskiidetud lepingusätteid). Sel juhul peab organisatsioon määrama enda organisatsioonis kontaktpunkti kõigi andmekaitseraamistikuga Privacy Shield seotud küsimuste jaoks.

(34) Kaubandusministeerium jälgib organisatsioone, kes ei osale enam ELi-USA raamistikus Privacy Shield kas sellepärast, et nad on vabatahtlikult sellest loobunud või siis sellepärast, et nende kinnituse kehtivus on lõppenud, et teha kindlaks, kas nad tagastavad, kustutavad või säilitavad ([35]) varem raamistiku alusel saadud isikuandmed.

([32]) Olukord on erinev sõltuvalt sellest, kas kolmas isik on vastutav töötleja või volitatud töötleja (esindaja). Esimesel juhul peab kolmanda isikuga sõlmitud lepinguga olema ette nähtud, et kolmas isik lõpetab andmete töötlemise või astub muid mõistlikke ja asjakohaseid samme olukorra parandamiseks. Teisel juhul peab nimetatud meetmed võtma raamistiku Privacy Shield alusel tegutsev organisatsioon, kes vastutab tema juhiste kohaselt tegutseva esindaja läbiviidud andmetöötluse eest.

([33]) Sellisel juhul peab ka USA organisatsioon astuma mõistlikud ja asjakohased sammud, et i) tagada, et nimetatud esindaja töötleb edastatud isikuandmeid ka tegelikkuses organisatsiooni põhimõtete järgsete kohustustega kooskõlas oleval viisil ja ii) vastava teate saamisel loata töötlemine peatada ja heastada.

([34]) Teave Privacy Shieldi nimekirja haldamise kohta on esitatud I ja II lisas (jaod I.3, I.4, III.6.d ja III.11.g).

([35]) Vt näiteks II lisa jaod I.3, III.6.f. ja III.11.g.i.

Juhul kui organisatsioonid andmed säilitavad, on neil kohustus jätkata nende andmete suhtes põhimõtete kohaldamist. Juhul kui kaubandusministeerium on organisatsioonid raamistikust kõrvaldanud püsiva põhimõtetele mittevastavuse tõttu, tagab ta, et need organisatsioonid tagastavad või kustutavad raamistiku alusel saadud isikuandmed.

(35) Kui organisatsioon lahkub mingil põhjusel ELi-USA raamistikust Privacy Shield, peab ta kustutama kõik avalikud viited, nagu jätkaks organisatsioon ELi-USA raamistikus Privacy Shield osalemist või omaks sellest tulenevaid õigusi, eelkõige enda avaldatud eraelu puutumatuse normides sisalduvad viited ELi-USA raamistikule Privacy Shield. Kaubandusministeerium otsib osalemise kohta esitatud valeväiteid ja võtab nendega seoses meetmeid, sealhulgas juhul, kui need on esitanud endised liikmed ([36]).Juhul kui organisatsioon on esitanud üldsusele eksitavate väidete või tavade kujul mis tahes valeandmeid põhimõtete järgimise kohta, võtavad FTC, transpordiministeerium või muu asjakohane USA täitevasutus täitemeetmeid; kaubandusministeeriumile valeandmete esitamine on hagetav valeandmete seaduse alusel (False Statements Act, 18 U.S.C. § 1001) ([37]).

(36) Kaubandusministeerium jälgib ametiülesande korras valeväiteid raamistikus Privacy Shield osalemise kohta ja sellele vastavust tõendava tähise väärkasutust ning DPAd võivad esitada ministeeriumi spetsiaalsele kontaktpunktile taotlusi organisatsioonide kontrollimiseks. Kui organisatsioon on ELi-USA andmekaitseraamistikust Privacy Shield lahkunud, ei ole esitanud iga-aastast kinnitust või on Privacy Shieldi nimekirjast kustutatud, kontrollib kaubandusministeerium jooksvalt, et ta oleks kustutanud enda avaldatud eraelu puutumatuse normidest kõik viited, nagu osaleks ta endiselt kõnealuses raamistikus, ning kui ta valeväidete esitamist ei lõpeta, edastab asja menetlemiseks FTC-le, transpordiministeeriumile või muule pädevale asutusele, kes võib võtta täitemeetmeid. Ministeerium saadab välja ka küsimustikud organisatsioonidele, kelle esitatud kinnitused põhimõtete järgimise kohta on aegunud või kes on vabatahtlikult andmekaitseraamistikust Privacy Shield lahkunud, et teha kindlaks, kas organisatsioon tagastab või kustutab isikuandmed, mille ta sai raamistikus osalemise ajal või jätkab ta nende andmete kasutamist ja eraelu puutumatuse põhimõtete rakendamist, ning kui isikuandmed säilitatakse, teeb kindlaks, kellele selles organisatsioonis edaspidi edastada andmekaitseraamistikuga Privacy Shield seotud küsimused.

(37) Kaubandusministeerium viib jooksvalt läbi põhimõtete järgimist kinnitanud organisatsioonide ametikohustuslikke vastavuskontrolle, ([38]) sealhulgas saates üksikasjalikke küsimustikke. Samuti viib ta regulaarselt läbi kontrolle juhul, kui talle on esitatud konkreetne (tõsiseltvõetav) kaebus organisatsiooni vastavuse kohta, kui organisatsioon ei vasta rahuldavalt ministeeriumi järelepärimistele või kui on olemas usutavad tõendid, et organisatsioon võib mitte vastata põhimõtetele. Kui see on asjakohane, konsulteerib kaubandusministeerium nimetatud vastavuskontrollidega seoses DPAdega.

2.3. *Õiguskaitsemehhanismid, kaebuste käsitlemine ja nõuete täitmise tagamine*

(38) ELi-USA raamistiku Privacy Shield *kaebuste käsitlemise, täitmise tagamise ja vastutuse põhimõtte* kohaselt peavad organisatsioonid nägema ette kaebuste käsitlemise mehhanismi isikutele, keda põhimõtete järgimata jätmine mõjutab, ja seega võimaluse ELi andmesubjektidele esitada kaebusi seoses põhimõtete järgimist kinnitatud USA ettevõte nõuetele mittevastavusega ning et saada neile kaebustele lahendus, vajaduse korral tõhusat õiguskaitset pakkuva otsusega.

(39) Osana põhimõtete järgimise kinnitamisest peavad organisatsioonid vastama kaebuste käsitlemise, nõuete täitmise tagamise ja vastutuse põhimõtte nõuetele, nähes ette kergesti kättesaadavad sõltumatud kaebuste käsitlemise mehhanismid, mille abil iga üksikisiku kaebusi ja vaidlusi uuritakse ja need lahendatakse tulemuslikult, selle eest üksikisikult tasu küsimata.

(40) Organisatsioonid võivad valida kas liidus või Ameerika Ühendriikides paiknevad sõltumatud kaebuste käsitlemise mehhanismid. Sealhulgas on võimalus võtta vabatahtlikult kohustus teha koostööd ELi DPAdega. Ent juhul kui

([36]) Vt I lisa jagu „Osalemise kohta esitatud valeväidete otsimine ja nendega tegelemine".
([37]) Vt II lisa jaod III.6.h. ja III.11.f.
([38]) Vt I lisa.

organisatsioon töötleb personaliandmeid, nimetatud valik puudub ja koostöö DPAdega on sel juhul kohustuslik. Muud võimalused on sõltumatu alternatiivne vaidluste lahendamine või erasektori poolt välja töötatud *eraelu puutumatuse programmid*, mille eeskirjadesse on lisatud eraelu puutumatuse põhimõtted. Programmid peavad kooskõlas kaebuste käsitlemise, nõuete täitmise tagamise ja vastutuse põhimõtte nõuetega hõlmama tõhusaid nõuete täitmise tagamise mehhanisme. Organisatsioonidel on kohustus hüvitada kõik nõuete eiramise probleemid. Samuti peavad nad täpsustama, et nad tunnustavad FTC, transpordiministeeriumi või muu Ameerika Ühendriikide täitevasutuse uurimis- ja nõuete täitmise tagamise õigusi.

(41) Sellest tulenevalt annab raamistik Privacy Shield andmesubjektidele mitu võimalust oma õiguste kasutamiseks, kaebuste esitamiseks seoses põhimõtete järgimist kinnitanud USA ettevõte nõuetele mittevastavusega ning neile kaebustele lahenduse saamiseks, vajaduse korral tõhusat õiguskaitset pakkuva otsusega. Üksikisikud võivad esitada oma kaebuse otse organisatsioonile, organisatsiooni poolt viidatud sõltumatule vaidluste lahendamise organile, riiklikele DPAdele või FTC-le.

(42) Juhul kui ühegi sellise kaebuste käsitlemise või nõuete täitmise tagamise mehhanismi abil kaebusele lahendust ei leita, on üksikisikutel samuti õigus algatada Privacy Shieldi paneelis siduv vahekohtumenetlus (käesoleva otsuse II lisa 1. lisa). Üksikisikud võivad vabal valikul kasutada ükskõik millist õiguskaitsemehhanismi või neid kõiki ning neil ei ole kohustust eelistada üht mehhanismi teisele ega järgida konkreetset järjekorda; erandiks on vahekohus, kus menetluse algatamise eeltingimuseks on teatud õiguskaitsevahendite ammendumine. Sellest hoolimata on soovitatav järgida teatud loogikat, mis on esitatud järgnevalt.

(43) Esiteks võivad ELi andmesubjektid esitada kaebused põhimõtete järgimata jätmise kohta otse *põhimõtete järgimist kinnitanud USA ettevõttele*. Selliste kaebuste lahendamise soodustamiseks peab organisatsioon nende menetlemiseks kehtestama tõhusa õiguskaitsemehhanismi. Organisatsiooni eraelu puutumatuse normides tuleb seega esitada üksikisikutele selge teave, mis käsitleb kas organisatsioonisisest või -välist kontaktpunkti, mille kaudu kaebusi käsitletakse (selleks võib olla ka ükskõik milline asjakohane asutus liidus, kes on pädev järelepärimistele või kaebustele vastama), ja sõltumatuid kaebuste käsitlemise mehhanisme.

(44) Üksikisiku esildise saamisel kas otse üksikisikult või kaubandusministeeriumilt, kellele selle on edastanud DPA, peab organisatsioon 45 päeva jooksul ELi andmesubjektile vastama. Vastus peab hõlmama hinnangut kaebuse põhjendatuse kohta ning teavet selle kohta, kuidas organisatsioon probleemi heastab. Samuti peavad organisatsioonid kiiresti reageerima päringutele, mille on esitanud kaubandusministeerium või DPA ([39]) (juhul kui organisatsioon on kohustunud DPAga koostööd tegema) ja mis käsitlevad nendepoolset põhimõtete järgimist. Organisatsioonid peavad säilitama dokumendid oma eraelu puutumatuse normide rakendamise kohta ja tegema need mittevastavuse uurimise või sellekohase kaebuse korral nõudmisel kättesaadavaks sõltumatule kaebuste käsitlemise mehhanismile või FTC-le (või mis tahes muule USA ametiasutusele, kellel on pädevus kõlvatute tavade või pettuse uurimiseks).

(45) Teiseks võivad üksikisikud esitada kaebuse otse *sõltumatule vaidluste lahendamise organile* (kas Ameerika Ühendriikides või liidus), kelle organisatsioon on määranud ning kes uurib ja lahendab üksikkaebusi (välja arvatud juhul, kui need on selgelt alusetud või tõsiseltvõetamatud) ja osutab üksikisikutele tasuta vajalikku abi. Sellise organi poolt kohaldatavad karistused ja heastamismeetmed peavad olema piisavalt ranged, et tagada organisatsioonide vastavus põhimõtetele, ja nendega tuleks ette näha mittevastavuse mõju heastamine organisatsiooni poolt ning sõltuvalt olukorrast asjaomaste andmete töötlemise lõpetamine ja/või nende kustutamine, samuti avastatud põhimõtete järgimata jätmise avalikustamine. Organisatsiooni määratud sõltumatud vaidluste lahendamise organid peavad oma veebisaidil esitama asjakohase teabe seoses ELi-USA andmekaitseraamistikuga Privacy Shield ning teenustega, mida nad selle raames osutavad. Igal aastal peavad nad avaldama nende vaidluste lahendamise teenuse kohta koondstatistikat sisaldava aruande ([40]).

([39]) Selle menetleva asutuse määrab DPAde paneel, mis on ette nähtud täienduspõhimõttega „Andmekaitseasutuste roll“ (II lisa jagu III.5).

([40]) Aastaaruanne peab sisaldama: 1) andmekaitseraamistikuga Privacy Shield seotud kaebuste arvu aruandeaastal; 2) laekunud kaebuste liike; 3) vaidluste lahendamise kvaliteedinäitajaid, näiteks kaebuste lahendamiseks kulunud aega; ja 4) laekunud kaebuste tagajärgi, eriti kehtestatud heastamismeetmete või sanktsioonide arvu ja liiki.

(46) Osana oma vastavuskontrollimeetmetest kontrollib kaubandusministeerium, et põhimõtete järgimist kinnitanud USA ettevõtted on ka tegelikkuses registreerinud end sõltumatute kaebuste käsitlemise mehhanismide juures, kelle juures registreerumist nad kinnitavad. Nii organisatsioonid kui ka vastutavad sõltumatud kaebuste käsitlemise mehhanismid peavad kiiresti reageerima kaubandusministeeriumi päringutele ja taotlustele esitada raamistikuga Privacy Shield seotud teavet.

(47) Juhul kui organisatsioon ei täida kaebuste käsitlemise või iseregulatsiooniorgani otsust, peab nimetatud organ teavitama sellest kaubandusministeeriumit ja FTC-d (või mis tahes muud USA ametiasutust, kellel on pädevus kõlvatute tavade või pettuse uurimiseks) või pädevat kohust ([41]). Kui organisatsioon keeldub järgimast mis tahes eraelu puutumatuse iseregulatsiooni-, sõltumatu vaidluste lahendamise või valitsusorgani lõppotsust või kui selline organ otsustab, et organisatsioon ei ole korduvalt põhimõtteid järginud, loetakse see püsivaks mittevastavuseks ning kaubandusministeerium kustutab põhimõtteid mittejärginud organisatsiooni pärast 30 päevast etteteatamist, millele organisatsioonil on võimalus vastata, nimekirjast ([42]). Kui organisatsioon pärast nimekirjast kustutamist jätkuvalt väidab, et ta tegutseb kooskõlas andmekaitseraamistiku Privacy Shield põhimõtetega, pöördub ministeerium sellega seoses FTC või muu täitevasutuse poole ([43]).

(48) Kolmandaks võivad üksikisikud esitada oma kaebused ka riiklikule *andmekaitseasutusele*. Organisatsioonidel on kohustus DPA poolt läbiviidaval uurimisel ja kaebuse lahendamisel koostööd teha, kui kaebus on seotud töösuhte raames kogutud personaliandmete töötlemisega või kui nad on vabatahtlikult nõustunud DPAde järelevalvele alluma. Eelkõige peavad nad vastama päringutele, täitma DPA soovitusi, sealhulgas heastamis- ja hüvitamismeetmete kohta, ning DPA-le kirjalikult kinnitama, et nimetatud meetmed on võetud.

(49) DPAde nõuanded edastatakse liidu tasemel moodustatud mitteametliku DPAde paneeli kaudu, ([44]) mis aitab tagada ühtlustatud ja sidusa lähenemise konkreetsele kaebusele. Nõuanded väljastatakse pärast seda, kui kummalgi vaidluse osapoolel on olnud mõistlik võimalus esitada selgitused ja soovitud tõendid. Paneel saadab nõuande nii kiiresti, kui menetlusnõuded võimaldavad, üldjuhul 60 päeva jooksul pärast kaebuse saamisest. Kui organisatsioon ei järgi nõuannet 25 päeva jooksul pärast selle väljastamist ning ei ole viivitust rahuldavalt põhjendanud, teavitab paneel oma kavatsusest loovutada materjal FTC-le (või muule USA pädevale täitevasutusele) või järeldada, et koostöökohustust on tõsiselt rikutud. Esimesel juhul võib see kaasa tuua täitemeetmete võtmise föderaalse kaubanduskomisjoni seaduse (edaspidi „FTC Act“) paragrahvi 5 (või sarnase normi) alusel. Teisel juhul teavitab paneel kaubandusministeeriumi, kes käsitab organisatsiooni keeldumist DPA paneeli nõuannet järgida püsiva mittevastavusena, mis toob kaasa organisatsiooni kustutamise Privacy Shieldi nimekirjast.

(50) Kui DPA, kellele kaebus on adresseeritud, ei ole kaebuse lahendamisega tegelenud või on seda teinud ebapiisavalt, on üksikisikust kaebajal võimalus vaidlustada nimetatud tegevus või tegevusetus vastava liikmesriigi siseriiklikes kohtutes.

(51) DPAdele võivad kaebusi esitada ka üksikisikud, isegi kui organisatsioon ei ole määranud oma vaidluste lahendamise organiks DPA paneeli. Sellistel juhtudel võib DPA edastada kaebused kas kaubandusministeeriumile või siis FTC-le. Koostöö soodustamiseks ja elavdamiseks seoses üksikisikute kaebuste ja raamistiku Privacy Shield alusel tegutsevate organisatsioonide poolse põhimõtete järgimata jätmisega loob kaubandusministeerium spetsiaalse kontaktpunkti, et pidada sidet ja osutada DPAdele abi organisatsioonide põhimõtetele vastavuse uurimisel ([45]). Ka FTC on võtnud kohustuse luua spetsiaalne kontaktpunkt ([46]) ja osutada DPAdele uurimisabi vastavalt USA turvalise võrgu seadusele (SAFE WEB Act) ([47]).

([41]) Vt II lisa jagu III.11.e.
([42]) Vt II lisa jagu III.11.g, eriti punktid ii ja iii.
([43]) Vt I lisa jagu „Osalemise kohta esitatud valeväidete otsimine ja nendega tegelemine“.
([44]) Mitteametliku DPAde paneeli töökorra peaksid kehtestama DPAd vastavalt oma pädevusele oma töö korraldamisel ja omavahelisel koostööl.
([45]) Vt I lisa jaod „Tugevdab koostööd andmekaitseasutustega“ ja „Hõlbustab põhimõtete järgimata jätmise kohta esitatud kaebuste menetlemist“ ning II lisa jagu II.7.e.
([46]) Vt IV lisa, lk 6.
([47]) *Samas*.

(52) Neljandaks on *kaubandusministeerium* kohustunud võtma vastu, vaatama läbi ja püüdma parimal võimalikul viisil lahendada kaebusi põhimõtete järgimata jätmise kohta organisatsioonides. Selleks näeb kaubandusministeerium DPAdele ette erikorra kaebuste edastamiseks spetsiaalsesse kontaktpunkti, nende jälgimiseks ja ettevõtetega suhtlemiseks, et lahendamisele kaasa aidata. Et üksikisikute kaebuste menetlemist kiirendada, teeb kontaktpunkt vastavusküsimustes koostööd otse vastava DPAga ning eelkõige hoiab teda kursis kaebuste seisuga kuni 90 päeva jooksul nende esitamisest. See võimaldab andmesubjektidel esitada kaebusi põhimõtete järgimata jätmise kohta põhimõtete järgimist kinnitanud USA ettevõtete poolt otse oma riiklikule DPA-le ning lasta need suunata kaubandusministeeriumile, kes on ELi-USA andmekaitseraamistikku Privacy Shield haldaja USA-s. Kaubandusministeerium on kohustunud esitama ELi-USA andmekaitseraamistiku Privacy Shield toimimise aastaülevaates ka kokkuvõtliku aruande igal aastal laekunud kaebustest ([48]).

(53) Kui kaubandusministeerium oma ametikohaste kontrollide, kaebuste või muu teabe alusel leiab, et organisatsioon on eraelu puutumatuse põhimõtetele püsivalt mittevastav, kustutab ta selle organisatsiooni Privacy Shieldi nimekirjast. Püsivaks mittevastavuseks loetakse ka eraelu puutumatuse iseregulatsiooni organi, sõltumatu vaidluste lahendamise organi või valitsusasutuse, sealhulgas DPA lõpliku otsuse täitmisest keeldumine.

(54) Viiendaks peab raamistiku Privacy Shield alusel tegutsev organisatsioon tunnustama USA ametiasutuste, eriti *föderaalse kaubanduskomisjoni* ([49]) (kes tagab praktikas põhimõtete järgimise) volitusi uurimise ja täitemeetmete läbiviimiseks. FTC vaatab eelisjärjekorras läbi esildised, mille on eraelu puutumatuse põhimõtetele mittevastavuse kohta edastanud sõltumatud kaebuste lahendamise organid või iseregulatsiooniorganid, kaubandusministeerium ja DPAd (omal algatusel või kaebuste põhjal), et teha kindlaks, kas on rikutud FTC Acti paragrahvi 5 ([50]). FTC on võtnud kohustuse luua standardiseeritud menetlus esildiste käsitlemiseks, luua DPAde edastatud esildiste jaoks asutusesisene kontaktpunkt ning vahetada tehtud esildistega seotud teavet. Lisaks võtab ta kaebusi vastu ka otse üksikisikutelt ning kohustub omal algatusel läbi viima andmekaitseraamistikuga Privacy Shield seotud uurimisi, eelkõige eraelu puutumatuse kaitse küsimustega seotud laiemate uurimiste raames.

(55) FTC võib teha vastavusse viimiseks ettekirjutusi (nn *consent orders*) ning jälgib süsteemselt nimetatud ettekirjutuste täitmist. Kui organisatsioon neid ei täida, võib FTC saata juhtumi edasi pädevale kohtule, et rakendada tsiviilõiguslikke sanktsioone ja muid õiguskaitsevahendeid, sealhulgas ebaseadusliku tegevusega põhjustatud kahju suhtes. Alternatiivina võib FTC otse taotleda föderaalkohtult esialgset või püsivat õiguskaitset või muude õiguskaitsevahendite kasutamist. Iga raamistiku Privacy Shield alusel tegutsevale organisatsioonile tehtav ettekirjutus peab sisaldama aruandlussätteid ([51]) ja organisatsioonid peavad avalikustama FTC-le esitatavate vastavus- või hindamisaruannete asjakohased osad, mis on seotud raamistikuga Privacy Shield. Peale selle peab FTC Internetis loendit ettevõtetest, kellele FTC või kohtud on teinud raamistikuga Privacy Shield seotud asjades ettekirjutusi või määrusi.

(56) Kuuendaks võib ELi andmesubjekt viimase võimalusena, juhul kui ükski muu ettenähtud õiguskaitsevahend ei ole üksikisiku kaebusele rahuldavat lahendust toonud, algatada siduva vahekohtumenetluse nn Privacy Shieldi paneelis. Organisatsioonid peavad teavitama üksikisikuid võimalusest algatada teatud tingimusel vahekohtumenetlus ning neil on vastamiskohustus, kui üksikisik on nimetatud võimalust kasutanud ja esitanud asjaomasele organisatsioonile sellekohase teate ([52]).

([48]) Vt I lisa jagu „Hõlbustab põhimõtete järgimata jätmise kohta esitatud kaebuste menetlemist".

([49]) Raamistiku Privacy Shield alusel tegutsev organisatsioon peab avalikult deklareerima võetud kohustust põhimõtteid järgida, tegema kooskõlas kõnealuste põhimõtetega avalikuks oma eraelu puutumatuse kaitse normid ja rakendama neid täielikult. Mittevastavus on hagetav FTC Acti paragrahvi 5 alusel, mis keelab äritegevuses või äritegevust mõjutavad kõlvatud tavad ja pettuse.

([50]) FTC-lt saadud teabe alusel pole tal seoses eraelu puutumatuse kaitsega õigust viia läbi kohapealset kontrolli. Ent tal on õigus nõuda organisatsioonidelt dokumentide esitamist ja tunnistuste andmist (vt FTC Act, paragrahv 20) ning kasutada otsuste eiramise korral nende täitmise tagamiseks kohtusüsteemi.

([51]) FTC ettekirjutuse või kohtu määrusega võidakse kohustada ettevõtteid rakendama eraelu puutumatuse programme ja tegema FTC-le korrapäraselt kättesaadavaks vastavusaruanded või sõltumatud hinnangud neile programmidele.

([52]) Vt II lisa jaod II.1.xi ja III.7.c.

(57) Vahekohus koosneb vähemalt 20 vahekohtunikust, kelle määravad kaubandusministeerium ja Euroopa Komisjon lähtuvalt nende sõltumatusest, aususest ja kogemustest USA eraelu puutumatuse kaitse õiguse ja liidu andmekaitseõiguse alal. Iga konkreetse vaidluse jaoks valivad pooled nimetatud koosseisust ühe kuni kolm ([53]) vahekohtunikku. Menetlusi reguleeritakse kaubandusministeeriumi ja komisjoni vahel kokku lepitavate vahekohtu standardeeskirjadega. Need eeskirjad lisanduvad juba sõlmitud raamkokkuleppele, mis hõlmab mitmeid sätteid nimetatud mehhanismi kättesaadavuse suurendamiseks ELi andmesubjektide jaoks: i) paneelile esitatava kaebuse koostamise juures võib andmesubjekt saada abi oma riiklikult DPA-lt; ii) vahekohtumenetlus toimub küll Ameerika Ühendriikides, kuid ELi andmesubjektid võivad soovi korral osaleda videokonverentsi või konverentskõne kaudu, mida võimaldatakse üksikisikule tasuta; iii) ehkki vahekohtumenetluses kasutatakse üldjuhul inglise keelt, võimaldatakse andmesubjektile harilikult põhjendatud taotluse alusel ja tasuta ([54]) istungi suuline ja dokumentide kirjalik tõlge; iv) kõik pooled, keda esindab paneelis advokaat, peavad enda õigusabikulud küll ise tasuma, kuid kaubandusministeerium moodustab andmekaitseraamistikus Privacy Shield osalevate organisatsioonide iga-aastastest sissemaksetest rahastatava fondi, mis katab vahekohtumenetluse toetuskõlblikud kulud vastavalt maksimummääradele, mille USA ametiasutused kehtestavad pärast Euroopa Komisjoniga nõupidamist.

(58) Privacy Shieldi paneelil on õigus kehtestada „konkreetsele isikule sobivad asjakohased mitterahalised kaitsemeetmed“, ([55]) mis on vajalikud põhimõte järgimata jätmise heastamiseks. Kuigi paneel võtab otsustamisel arvesse ka teisi heastamismeetmeid, mis on andmekaitseraamistiku Privacy Shield muude mehhanismide raames juba määratud, võivad üksikisikud siiski pöörduda vahekohtusse, kui nad peavad kõnealuseid muid heastamismeetmeid ebapiisavaks. See võimaldab ELi andmesubjektidel pöörduda vahekohtusse kõigil juhtudel, kus USA pädevate asutuste (näiteks FTC) tegevus või tegevusetus ei ole toonud nende kaebustele rahuldavat lahendust. Vahekohtumenetlust ei või algatada, kui DPA ise on põhimõtete järgimist kinnitanud USA ettevõtte suhtes õiguslikult pädev kõnealust küsimust lahendama, kuna organisatsioon on kohustatud tegema DPAdega koostööd ja järgima nende nõuandeid seoses töösuhte raames kogutud personaliandmete töötlemisega või on vabatahtlikult võtnud kohustuse seda teha. Üksikisikud saavad vahekohtu otsuse täitmisele pöörata USA kohtute kaudu föderaalse vahekohtu seaduse (Federal Arbitration Act) alusel, mis tagab õiguskaitse juhuks, kui ettevõte otsust ei täida.

(59) Seitsmendaks, kui organisatsioon ei täida oma kohustust järgida põhimõtteid ja eraelu puutumatuse avaldatud norme, võib USA osariikide õigus pakkuda täiendavaid õiguskaitsevahendeid näiteks lepinguvälise kahju hüvitamiseks ning teadliku valeandmete esitamise, kõlvatute tavade või pettuse ja lepingurikkumiste puhuks.

(60) Lisaks sellele, kui ELi andmesubjektilt nõude saanud DPA leiab, et selle üksikisiku isikuandmete edastamisel Ameerika Ühendriikide organisatsioonile rikutakse ELi andmekaitseseadust, sealhulgas juhul kui ELi andmeeksportijal on põhjust arvata, et organisatsioon ei vasta põhimõtetele, võib ta ka teostada enda volitusi andmeeksportija suhtes ning anda vajaduse korral käsu andmete edastamine peatada.

(61) Käesolevas jaos esitatud teavet arvestades leiab komisjon, et USA kaubandusministeeriumi avaldatud põhimõtted tervikuna tagavad isikuandmete kaitse sisuliselt samaväärsel tasemel, nagu on tagatud direktiiviga 95/46/EÜ kehtestatud oluliste aluspõhimõtetega.

(62) Põhimõtete tõhus rakendamine on tagatud ka läbipaistvuskohustustega ning raamistiku Privacy Shield haldamise ja vastavuskontrolliga kaubandusministeeriumi poolt.

(63) Lisaks leiab komisjon, et andmekaitseraamistiku Privacy Shield jaoks ette nähtud seire-, õiguskaitse- ja nõuete tagamise täitmise mehhanismid tervikuna võimaldavad praktikas tuvastada põhimõtete rikkumisi raamistiku Privacy Shield alusel tegutsevates organisatsioonides ja nende eest karistada ning pakuvad andmesubjektile õiguskaitsevahendeid temaga seotud isikuandmetele juurdepääsu tagamiseks ning vajadusel nimetatud andmete parandamiseks või kustutamiseks.

([53]) Pooled peavad kokku leppima vahekohtunike arvu.

([54]) Paneel võib siiski otsustada, et konkreetses vahekohtuvaidluses võib kulude katmine kaasa tuua põhjendamatuid või ebaproportsionaalseid kulusid.

([55]) Üksikisikud ei saa vahekohtus kahjunõudeid esitada, ent vahekohtusse pöördumine ei mõjuta samas võimalust nõuda kahju hüvitamist USA tavakohtute kaudu.

## 3. USA AVALIKU SEKTORI ASUTUSTE JUURDEPÄÄS ELI-USA ANDMEKAITSERAAMISTIKU PRIVACY SHIELD ALUSEL EDASTATUD ISIKUANDMETELE JA NENDE KASUTAMINE SELLISTE ASUTUSTE POOLT

(64) Nagu on sätestatud II lisa jaos I.5, on põhimõtete järgimine piiratud ulatusega, mis on vajalik riikliku julgeoleku, avaliku huvi või õiguskaitseliste vajaduste täitmiseks.

(65) Euroopa Komisjon on hinnanud piiranguid ja kaitsemeetmeid, mis on sätestatud USA õiguses seoses ELi-USA andmekaitseraamistiku Privacy Shield alusel edastatud isikuandmetele juurdepääsu ja nende kasutamisega USA avaliku sektori asutuste poolt riikliku julgeoleku, õiguskaitse ja muu avaliku huvi eesmärgil. Lisaks on USA valitsus esitanud riigi luuredirektori büroo (Office of the Director of National Intelligence, edaspidi „ODNI") ([56]) kaudu Euroopa Komisjonile üksikasjalikud kinnitused ja kohustused, mis on ära toodud käesoleva otsuse VI lisas. USA välisministri allkirjaga kirjas, mis on esitatud otsuse III lisas, on USA valitsus võtnud ka kohustuse luua uus riikliku julgeolekuga seotud sekkumiste järelevalve mehhanism, nimelt andmekaitseraamistiku Privacy Shield ombudsman, kes on USA luureühendusest sõltumatu. Lõpuks on USA justiitsministeeriumi kinnituses, mis on esitatud käesoleva otsuse VII lisas, kirjeldatud piiranguid ja kaitsemeetmeid seoses isikuandmetele juurdepääsu ja nende kasutamisega avaliku sektori asutuste poolt õiguskaitse ja muudel avaliku huvi eesmärkidel. Läbipaistvuse suurendamiseks ja nimetatud kohustuste õigusliku siduvuse väljendamiseks avaldatakse kõik need eespool loetletud ja käesolevale otsusele lisatud dokumendid USA ametlikus teatajas *Federal Register*.

(66) Komisjoni järeldusi seoses piirangutega Euroopa Liidust Ameerika Ühendriikidesse edastatud isikuandmetele juurdepääsule ja nende kasutamisele USA avaliku sektori asutuste poolt ning tõhusa õiguskaitse olemasolu kohta kirjeldatakse üksikasjalikumalt allpool.

### 3.1. *Juurdepääs ja kasutamine USA avaliku sektori asutuste poolt riikliku julgeoleku huvides*

(67) Komisjoni analüüs näitab, et USA õiguses on sätestatud mitmed piirangud ELi-USA andmekaitseraamistiku Privacy Shield alusel edastatud isikuandmetele juurdepääsule ja nende kasutamisele riikliku julgeoleku huvides ning ka järelevalve- ja õiguskaitsemehhanismid, mis piisaval määral tagavad nende andmete tõhusa kaitse ebaseadusliku sekkumise ja kuritarvitamise riski eest ([57]). Alates 2013. aastast, mil komisjon avaldas oma kaks teatist (vt põhjendus 7), on seda õigusraamistikku järgnevalt kirjeldatud viisil oluliselt tugevdatud.

#### 3.1.1. Piirangud

(68) Vastavalt USA konstitutsioonile kuulub riikliku julgeoleku tagamine presidendi pädevusse, kes on relvajõudude ülemjuhataja, täitevvõimu juht ja kes korraldab USA välissuhtlust välisluure valdkonnas ([58]). Kuigi kongressi pädevuses on kehtestada piiranguid ja ta on seda mitmes aspektis ka teinud, saab president nimetatud piires juhtida USA luureühenduse tööd, kasutades selleks eelkõige korraldusi või presidendi suuniseid. Mõistagi kehtib sama ka neis valdkondades, kus kongress suuniseid ei anna. Selle valdkonna kaks keskset õigusakti on praegu korraldus (Executive Order) 12333 (edaspidi „E.O. 12333") ([59]) ja presidendi poliitikasuunis (Presidential Policy Directive) nr 28.

([56]) Riiklik luuredirektor (edaspidi „DNI") tegutseb USA luureühenduse juhatajana ning presidendi ja riikliku julgeoleku nõukogu peamine nõuandjana. Vt luure reformi ja terrorismi ennetamise seadus (Intelligence Reform and Terrorism Prevention Act of 2004), Pub. ICL. 108–458, 17.12.2004. Muu hulgas kehtestab ODNI nõuded riigi luureülesannete andmisele ning luureandmete kogumisele, analüüsile, esitamisele ja jagamisele USA luureühenduse poolt ning korraldab ja juhib nimetatud tegevusi, töötades muu hulgas välja teabele või luureandmetele juurdepääsu ja nende kasutamise ja jagamise suunised. Vt E.O. 12333 paragrahv 1.3 a), b).

([57]) Schrems, punkt 91.

([58]) USA konstitutsiooni II artikkel. Vt ka PPD-28 sissejuhatav osa.

([59]) E.O. 12333: United States Intelligence Activities, Federal Register Vol. 40, No. 235 (8. detsember 1981). Korralduse avalikult kättesaadava osa põhjal määratletakse USA luuretegevuse eesmärgid, suunad, ülesanded ja vastutusalad (sealhulgas luureühenduse eri liikmete rollid) ning sätestatakse luuretegevuse korraldamise üldtingimused (eelkõige vajadus kehtestada üksikasjalikud menetlusnormid). E.O. 12333 paragrahvi 3.2 kohaselt kehtestavad president, keda toetab riikliku julgeoleku nõukogu, ja riigi luuredirektor korralduse rakendamiseks vajalikud direktiivid, menetlused ja suunised.

(69) Presidendi 17. jaanuari 2014. aasta poliitikasuunisega nr 28 (edaspidi „PPD-28“) on kehtestatud mitmed nn signaaliluurega seotud piirangud ([60]). See presidendi suunis on USA luureasutustele ([61]) siduv ja jääb kehtima kuni USA valitsuse vahetumiseni ([62]). PPD-28 on eriti oluline USA-välist päritolu isikutele, sealhulgas ELi andmesubjektidele. Selles on muu hulgas sätestatud, et:

a) signaaliluure andmete kogumine peab põhinema õigusaktil või presidendi loal ning toimuma kooskõlas USA konstitutsiooni (eriti selle neljanda muudatuse) ja USA õigusega;

b) iga isikut tuleb kohelda väärikalt ja austusega, olenemata tema kodakondsusest või elukohast;

c) igal isikul on tema isikuandmete töötlemise suhtes seaduslikud eraelu puutumatuse kaitsega seotud huvid;

d) USA signaaliluuretegevuse kavandamise lahutamatuks osaks on eraelu puutumatuse ja kodanikuvabadustega seotud kaalutlused;

e) seetõttu tuleb USA signaaliluuretegevuses tagada nõuetekohased kaitsemeetmed kõikide isikute isikuandmetele olenemata nende kodakondsusest või elukohast.

(70) Vastavalt suunisele PPD-28 võib signaaliluureandmeid koguda üksnes juhul, kui selleks on riigi või riigiasutuste tegevust toetav välis- või vastuluurega seotud põhjus, aga mitte mis tahes muudel eesmärkidel (nt USA ettevõtetele konkurentsieelise loomiseks). Sellega seoses selgitab ODNI, et luureühenduse liikmed „peaksid nõudma, et võimaluse korral peab kogumine olema suunatud konkreetsetele välisluure sihtmärkidele või teemadele, kasutades diskriminante (nt konkreetsed vahendid, valikutingimused ja identifikaatorid)“ ([63]). Lisaks tagatakse kinnitustes, et luureandmete kogumise kohta ei hakka kaalutlusotsuseid tegema üksikud luureagendid, vaid rakendatakse põhimõtteid ja menetlusi, mille USA luureühenduse eri liikmed (asutused) peavad PPD-28 ellurakendamiseks kehtestama ([64]). Sellega seoses toimub sobivate tunnuste uurimine ja valik üldise riikliku luureprioriteetide raamistiku (General Intelligence Priorities Framework, NIPF) raames, mis tagab, et luureprioriteete kehtestavad kõrge taseme poliitikakujundajad ning need vaadatakse korrapäraselt läbi, et reageerida üksnes riigi julgeolekut ähvardavatele tegelikele ohtudele ning võtta arvesse võimalikke riske, sealhulgas eraelu puutumatusega seotud riske ([65]). Sellest lähtudes uurivad asutuse töötajad läbi ja määravad kindlaks konkreetsed valikutingimused, mis peaksid võimaldama koguda välisluureandmeid vastavalt prioriteetidele ([66]). Valikutingimused või nn tunnused tuleb korrapäraselt läbi vaadata, et veenduda, kas neil on säilinud prioriteetidele vastav luureväärtus ([67]).

([60]) E.O. 12333 kohaselt on Riikliku Julgeoleku Ameti (National Security Agency, edaspidi „NSA“) direktor signaaliluure valdkonna juht, kes juhib ühtset signaaliluuretegevuse organisatsiooni.

([61]) Mõiste „luureühendus“ määratluse kohta vt E.O. 12333 paragrahv 3.5 (h) ja PPD-28 märkus 1.

([62]) Vt justiitsministeeriumi (Department of Justice) õigusbüroo seisukoht president Clintonile, 29. jaanuar 2000. Selle juriidilise arvamuse kohaselt on presidendi suunistel „sisuliselt sama õigusmõju, mis korraldusel“.

([63]) ODNI kinnitused (VI lisa), lk 3.

([64]) Vt PPD-28 paragrahvid 4(b) ja (c). Avaliku teabe kohaselt kinnitas 2015. aasta läbivaatamine olemasolevat kuut eesmärki. Vt ODNI, Signals Intelligence Reform, 2016 Progress Report.

([65]) ODNI kinnitused (VI lisa), lk 6 (viitega direktiivile Intelligence Community Directive 204). Vt ka PPD-28 paragrahv 3.

([66]) ODNI kinnitused (VI lisa), lk 6. Vt nt NSA kodanikuvabaduste ja eraelu puutumatuse kaitse büroo (edaspidi „NSA CLPO“), NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333, 7. oktoober 2014. Vt ka ODNI seisundiaruanne 2014. Välisluure jälitustegevuse seaduse (FISA) paragrahvi 702 kohaste juurdepääsutaotluste puhul reguleerivad päringuid välisluure järelevalvekohtu (Foreign Intelligence Surveillance Court, FISC) kinnitatud minimeerimisprotseduurid. Vt NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16. aprill 2014.

([67]) Vt Signals Intelligence Reform, 2015 Anniversary Report. Vt ka ODNI kinnitused (VI lisa), lk 6, 8–9, 11.

(71) PPD-28 nõuete sätted, nagu see, et andmete kogumine peab alati ([68]) olema „võimalikult täpselt suunatud“ ning luureühendus peab püüdma esmajärjekorras kasutada muud saadaolevat teavet ning sobivaid ja teostatavaid alternatiive, ([69]) peegeldavad lisaks üldreeglit eelistada sihipärast andmete kogumist massiandmekogumisele. ODNI antud kinnituse kohaselt tagavad nad ennekõike, et massiandmekogumine ei ole ei massiline ega ka valimatu ja et erandit ei hakata kasutama rohkem kui reeglit ([70]).

(72) Kuigi suunises PPD-28 on selgitatud, et luureühenduse liikmetel on vahel tarvis luuresignaale masskoguda, näiteks uute või arengujärgus ohtude tuvastamiseks ja hindamiseks, antakse selles neile juhis kasutada esmajärjekorras alternatiive, mis võimaldavad signaaliluureandmete suunatud kogumist ([71]). Sellest tulenevalt toimub massiandmekogumine ainult juhul, kui sihipärane andmete kogumine diskriminante, st konkreetse sihtmärgiga seotud identifikaatorit (nt meiliaadressi või telefoninumbrit) kasutades ei ole võimalik „tehnilistel või operatiivsetel kaalutlustel“ ([72]). See kehtib nii signaaliluureandmete kogumise viisi kui ka selle suhtes, mida reaalselt kogutakse ([72]).

(73) ODNI kinnituste kohaselt üritab ta ka sel juhul, kui luureühendus ei saa andmete kogumise sihipärastamiseks kasutada konkreetseid identifikaatoreid, kitsendada andmete kogumise ulatust „nii palju kui võimalik“. Selleks kasutab ta „filtreid ja muid tehnilisi abivahendeid, et andmeid kogutaks nende vahendite põhjal, mis sisaldavad tõenäoliselt välisluure seisukohast väärtuslikke andmeid“ (ja on seega kooskõlas USA poliitikakujundajate poolt vastavalt põhjenduses 70 kirjeldatud menetlusele sätestatud nõuetega). Sellest tulenevalt sihipärastatakse massiandmekogumine vähemalt kahel viisil: esiteks seondub see alati konkreetse välisluure eesmärgiga (näiteks saada signaaliluureandmeid konkreetses piirkonnas tegutseva terrorirühmituse kohta) ja keskendub andmete kogumisel sellega seonduvale sidele. ODNI esitatud avalduse kohaselt annab sellest tunnistust asjaolu, et„Ameerika Ühendriikide signaaliluuretegevus puudutab ainult murdosa kogu internetis toimuvast suhtlusest“ ([73]). Teiseks on ODNI kinnitustes selgitatud, et kasutatavad filtrid ja muud tehnilised vahendid töötatakse välja andmete kogumiseks „nii täpselt kui võimalik“, et viia kogutud „asjassepuutumatu teabe“ hulk miinimumini.

(74) Lõpetuseks, isegi kui Ameerika Ühendriigid otsustavad signaaliluureandmeid põhjendustes 70–73 kirjeldatud tingimuste kohaselt masskoguda, piirab PPD-28 kogutud andmete kasutamist kuut riikliku julgeolekuga seotud eesmärki sisaldava konkreetse loendiga, et kaitsta kõigi isikute eraelu puutumatust ja kodanikuvabadusi nende olenemata kodakondsusest ja elukohast ([74]). Need lubatavad eesmärgid on meetmed spionaažist, terrorismist ja

([68]) Vt joonealune märkus 63.

([69]) Tuleb ka märkida, et E.O. 12333 paragrahvi 2.4 kohaselt peavad luureühenduse liikmed „kasutama Ameerika Ühendriikides kogumislahendusi, millega kaasneb võimalikult vähe sekkumist“. Kitsenduste kohta seoses massiandmekogumise asendamisega sihipärase andmete kogumisega vt USA riikliku teadustöönõukogu poolt läbi viidud hindamise tulemused, mis on ära toodud Euroopa Liidu Põhiõiguste Ameti väljaandes „Surveillance by intelligence services: fundamental rights, safeguards and remedies in the EU“ (2015), lk 18.

([70]) ODNI kinnitused (VI lisa), lk 4.

([71]) Vt ka PPD-28 paragrahv 5(d), mille kohaselt riigi luurejuht peab luureühenduse asjaomaste liikmete ning teadus- ja tehnoloogiapoliitika bürooga kooskõlastatult esitama presidendile „aruande, milles hinnatakse võimalusi luua tarkvara, mis võimaldaks luureühendusel masskogumise asemel hõlpsamini suunatult teavet koguda“. Avaliku teabe kohaselt järeldati selles aruandes, et „puudub tarkvaraline alternatiiv, mis teatavat liiki riiklikku julgeolekut ähvardavate ohtude tuvastamisel täielikult asendaks masskogumist“. Vt Signals Intelligence Reform, 2015 Anniversary Report.

([72]) Vt joonealune märkus 63.

([73]) ODNI kinnitused (VI lisa). Sellega vastatakse riiklike andmekaitseasutuste poolt piisavusotsuse eelnõu kohta esitatud arvamuses väljendatud kõhklustele. Vt artikli 29 alusel asutatud andmekaitse töörühm, arvamus 01/2016 ELi-USA andmekaitseraamistiku Privacy Shield piisavusotsuse eelnõu kohta (vastu võetud 13. aprillil 2016), lk 38, nr 47.

([74]) Vt ka PPD-28 paragrahv 2.

massihävitusrelvadest tulenevate ohtude ning küberjulgeoleku, relvajõudude ja sõjaväelaste vastu suunatud ohtude tuvastamiseks ja nende vastu võitlemiseks ning viie muu ohuga seotud rahvusvahelise kuritegevuse tuvastamiseks ja selle vastu võitlemiseks, ning need vaadatakse läbi vähemalt üks kord aastas. Vastavalt USA valitsuse kinnitustele on luureühenduse liikmed tugevdanud analüüsisüsteeme ja -standardeid, et filtreerida määratlemata signaaliluureandmeid vastavalt nimetatud nõuetele; suunatud päringute kasutamine „tagab, et analüütikutele antakse uurida üksnes selliseid andmeid, millel eeldatakse olevat potentsiaalne luurealane väärtus“ ([75]).

(75) Need piirangud on ELi-USA andmekaitseraamistiku Privacy Shield alusel edastatavate isikuandmete seisukohalt eriti olulised, eelkõige juhul, kui isikuandmete kogumise koht on väljaspool Ameerika Ühendriike, sh teel läbi transatlantiliste kaablite liidust Ameerika Ühendriikidesse. Nagu USA ametiasutused ODNI kinnitustes märkisid, kohaldatakse neis sätestatud piiranguid ja kaitsemeetmeid – sealhulgas PPD-28 sätteid – ka seda liiki kogumisele ([76]).

(76) Kuigi kasutatavad juriidilised mõisted on erinevad, vastavad need põhimõtted sisuliselt vajalikkuse ja proportsionaalsuse põhimõtetele. Suunatud kogumine toimub selgete prioriteetide alusel ning masskogumine piirdub (erandlike) olukordadega, kus suunatud kogumine ei ole tehnilistel või operatiivtööga seotud põhjustel võimalik. Isegi kui *masskogumist* pole võimalik vältida, on kogutud andmete edasine „kasutamine“ ehk juurdepääs neile *rangelt piiratud* konkreetsete õiguspäraste riikliku julgeoleku eesmärkidega ([77]).

(77) Kuna suunise on välja andnud president kui täitevvõimu juht, on need nõuded siduvad kogu luureühendusele ning neid on hiljem rakendatud asutusesiseste eeskirjade ja menetlustega, millega on üldpõhimõtted teisendatud konkreetseteks igapäevatöö juhisteks. Lisaks on kongress, ehkki PPD-28 pole talle siduv, astunud samme tagamaks, et isikuandmete kogumine ja neile juurdepääs oleks Ameerika Ühendriikides suunatud ega toimuks „üldistatud alustel“.

(78) Olemasolevast teabest, sealhulgas USA valitsuse kinnitustest tuleneb, et pärast andmete edastamist Ameerika Ühendriikide organisatsioonidele, kes on kinnitanud põhimõtete järgimist ELi-USA andmekaitseraamistiku Privacy Shield raames, võivad USA luureasutused neid isikuandmeid nõuda üksnes ([78]) juhul, kui nõue vastab välisluure ja jälitustegevuse seadusele (Foreign Intelligence Surveillance Act, edaspidi „FISA“) või selle esitab Föderaalne Juurdlusbüroo (Federeal Bureau of Investigation, edaspidi „FBI“) nn julgeoleku-teabenõude (National Security Letter, edaspidi „NSL“) alusel ([79]). FISA sisaldab mitmeid õiguslikke aluseid, millele tuginedes võib koguda (ja

([75]) ODNI kinnitused (VI lisa), lk 4. Vt ka Intelligence Community Directive 203.
([76]) ODNI kinnitused (VI lisa), lk 2. Kohaldatakse ka E.O. 12333-s sätestatud piiranguid (nt et kogutav teave peab vastama presidendi kehtestatud luureprioriteetidele).
([77]) Vt Schrems, punkt 93.
([78]) FBI võib lisaks andmeid koguda ka õiguskaitselubade alusel (vt käesoleva otsuse jagu 3.2).
([79]) NSL-ide kasutamist on üksikasjalikumalt selgitatud ODNI kinnitustes (VI lisa), lk 13–14 ja nr 38. Nagu selles märgitud, võib FBI kasutada NSL-e üksnes muude kui sisuandmete väljanõudmiseks sanktsioneeritud riikliku julgeolekuga seotud uurimise huvides, mida viiakse läbi kaitseks rahvusvahelise terrorismi või salaluuretegevuse vastu. ELi-USA andmekaitseraamistiku Privacy Shield alusel edastatavate andmetega seoses on kõige asjakohasem volitusnorm arvatavasti elektroonilise side seadus (Electronic Communications Privacy Act) (18 U.S.C. § 2709), mis nõuab, et kasutajaandmete või tegevuslogide väljanõudmisel tuleb kasutada „tingimust, mis identifitseerib konkreetse isiku, grupi, telefoninumbri või konto“.

seejärel töödelda) ELi andmesubjektide isikuandmeid, mis on edastatud ELi-USA andmekaitseraamistiku Privacy Shield alusel. Lisaks FISA paragrahvile 104, ([80]) millega on hõlmatud tavapärane individualiseeritud elektrooniline jälgimine, ja FISA paragrahvile 402 ([81]) pealtkuulamisseadmete paigaldamise kohta, on kaks peamist alust FISA paragrahv 501 (endine seaduse U.S. PATRIOT ACT paragrahv 215) ja FISA paragrahv 702 ([82]).

(79) Sellega seoses keelab 2. juunil 2015 vastu võetud seadus USA FREEDOM Act FISA paragrahvi 402 (väljamineva ja sissetuleva side jälgimise seadmeid lubav norm) ja FISA paragrahvi 501 (varem seaduse U.S. PATRIOT ACT paragrahv 215) ([83]) alusel ning NSL-ide alusel andmete masskogumise ning nõuab, et selle asemel kasutataks konkreetseid „valikutingimusi“ ([84]).

(80) Ehkki FISA sisaldab veel õiguslikke aluseid riikliku julgeolekuga seotud tegevuseks, sealhulgas signaaliluureks, näitab komisjoni hinnang, et ELi-USA andmekaitseraamistiku Privacy Shield alusel edastatavate isikuandmete puhul piiravad nimetatud volitused avaliku sektori asutuste sekkumist suunatud kogumisse ja juurdepääsu samaväärselt.

(81) FISA paragrahvi 104 alusel toimuva tavapärase individualiseeritud elektroonilise jälgimise puhul on see selge ([85]). FISA paragrahvi 702 puhul, mis on aluseks kahele USA luureasutuste olulisele luureprogrammile (PRISM, UPSTREAM), tehakse otsinguid suunatult, kasutades individuaalseid tunnuseid vastavalt konkreetsetele sidevahenditele, näiteks sihtmärgi e-posti aadress või telefoninumber, mitte aga võtmesõnade ega isegi mitte sihtmärgiks olevate üksikisikute nimede järgi ([86]). Seega, nagu on märkinud eraelu puutumatuse ja

([80]) 50 U.S.C. § 1804. Kuigi selle volitusnormi kohaselt tuleb „esitada ülevaade faktidest ja asjaoludest, millele tuginedes taotleja arvab, et A) elektroonilise luure sihtmärk on võõrvõim või võõrvõimu agent“, võivad selle alla kuuluda ka USA-välised isikud, kes tegelevad rahvusvahelise terrorismi või massihävitusrelvade rahvusvahelise levitamisega (sealhulgas ettevalmistustega selleks) (50 U.S.C. § 1801 (b)(1)). Seos ELi-USA andmekaitseraamistiku Privacy Shield alusel edastatavate isikuandmetega on siiski üksnes teoreetiline, kuna ülevaade faktidest peab põhjendama arvamust, et „kõik sidevahendid või kohad, mille suhtes elektroonilist jälgimist rakendatakse, on kasutusel või plaanitakse kasutusele võtta võõrvõimu või võõrvõimu agendi poolt“. Igal juhul tuleb selle normi kohaldamiseks esitada taotlus FISC-ile, kes hindab muu hulgas, kas esitatud faktidest lähtudes on olemas põhjendatud kahtlus, et see tõepoolest nii on.

([81]) 50 U.S.C. § 1842 ja § 1841 lg 2 ning 18. peatüki paragrahv 3127. See norm ei puuduta side sisu, vaid on suunatud pigem teenust kasutava kliendi või kasutaja andmetele (sh nimi, aadress, kasutajakood, kasutatud teenuse kestus/liik, maksete tegija/makseviis). See eeldab loataotluse esitamist FISC-ile (või USA föderaalkohtu magistraadile) ning konkreetse valikutingimise kasutamist § 1841 lg 4 tähenduses, st tingimust, mis identifitseerib konkreetse isiku, konto vms, ning seda kasutatakse tagamaks, et taotletava teabe maht oleks nii väike kui mõistlikult võimalik.

([82]) Ehkki FISA paragrahv 501 (endine seaduse U.S. PATRIOT ACT paragrahv 215) lubab FBI-l taotleda kohtu korraldust „käegakatsutavate asjade“ (eelkõige telefonside metaandmete, kuid ka äridokumentide) väljanõudmiseks välisluure otstarbel, lubab FISA paragrahv 702 US luureühenduse liikmetele juurdepääsu teabele, sealhulgas Interneti-side sisule, mille allikas on Ameerika Ühendriikides, ent mis on suunatud teatavatele väljaspool Ameerika Ühendriike asuvatele USA-välistele isikutele.

([83]) Selle sätte alusel võib FBI nõuda välja „käegakatsutavaid asju“ (st logisid, materjale, dokumente), kui ta tõendab välisluure järelevalvekohtule (FISC), et on piisavalt alust pidada neid konkreetse FBI uurimise huvides vajalikuks. Otsingu teostamisel peab FBI kasutama FISC-i heakskiidetud valikutingimusi, mille puhul on olemas „mõistlik konkreetselt väljendatav kahtlus“, et vastav tingimus on seotud ühe või mitme võõrvõimu või nende agentidega, kes tegelevad rahvusvahelise terrorismi või selle ettevalmistamisega. Vt PCLOB, Section 215 Report, lk 59; NSA CLPO, Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15. jaanuar 2016, lk 4–6.

([84]) ODNI kinnitused (VI lisa), lk 13 (nr 38).

([85]) Vt joonealune märkus 81.

([86]) PCLOB, Sec. 702 Report, lk 32–33 koos edasiviidetega. Eraelu puutumatuse büroo andmetel peab NSA kontrollima, et sihtmärgi ja valikutingimuse vahel on seos, dokumenteerima välisluureandmed, mida loodetakse saada, selle teabe peavad läbi vaatama ja kinnitama kaks NSA vanemanalüütikut ning kogu protsessi jälgitakse edaspidi ODNI ja justiitsministeeriumi vastavuskontrolli abil. Vt NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16. aprill 2014.

kodanikuvabaduste järelevalve komisjon (Privacy and Civil Liberties Oversight Board, edaspidi „PCLOB"), on paragrahvi 702 alusel toimuv luure „suunatud üksnes konkreetsetele [USA-välistele] isikutele, kelle kohta on antud individuaalne korraldus" ([87]). Aegumisklauslist tulenevalt vaadatakse FISA paragrahv 702 läbi 2017. aastal, mil komisjon peab uuesti hindama ka ELi andmesubjektidele pakutavaid kaitsemeetmeid.

(82) Peale selle on USA valitsus oma kinnitustes Euroopa Komisjonile selgesõnaliselt taganud, et USA luureühendus „ei tegele mis tahes isikute, ka mitte Euroopa tavakodanike valimatu jälgimisega" ([88]). Ameerika Ühendriikides kogutud isikuandmete puhul kinnitavad seda avaldust empiirilised tõendid, mis näitavad, et *juurdepääsutaotlused* NSLide ja FISA alusel hõlmavad nii eraldi kui ka koos arvestatuna võrreldes Interneti andmevoogude üldise mahuga üksnes suhteliselt väikest arvu sihtmärke ([89]).

(83) Kogutud andmetele *juurdepääsu* ja *andmekaitsega* seoses on suunisega PPD-28 nõutud, et juurdepääs „peab olema piiratud volitatud töötajatega, kellel on vastavaid andmeid tarvis oma tööülesande täitmiseks" ning isikuandmeid „tuleb töödelda ja hoida tingimustes, mis tagavad nende piisava kaitse ja välistavad volitamata isikute juurdepääsu kooskõlas tundliku teabe suhtes kohaldatavate kaitsemeetmetega". Luuretöötajad saavad asjakohase ja piisava väljaõppe suunises PPD-28 sätestatud põhimõtete alal ([90]).

(84) Peale selle on suunises PPD-28 USA luureasutuste kogutavate ELi andmesubjektide isikuandmete *säilitamise* ja *edasijagamise* kohta märgitud, et iga isikut (sh USA-väliseid isikuid) tuleb kohelda väärikalt ja austusega, igal isikul on tema isikuandmete töötlemise suhtes seaduslikud eraelu puutumatuse kaitsega seotud huvid ning luureühenduse liikmed peavad seetõttu kehtestama normid nõuetekohaste andmekaitsemeetmete tagamiseks, mis on „mõistlikult kujundatud edasilevitamist ja säilitamist minimeerival viisil" ([91]).

([87]) PCLOB, Sec. 702 Report, lk 111. Vt ka ODNI kinnitused (VI lisa), lk 9 („[FISA] paragrahvi 702 alusel toimuv kogumine ei ole valimatu masskogumine, vaid suunatud kitsalt välisluureandmete kogumisele individuaalselt kindlaks määratud seaduslike sihtmärkide kohta") ja lk 13, nr 36 (viitega FISC 2014. aasta arvamusele); NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16. aprill 2014. Isegi UPSTREAMi puhul võib NSA taotleda elektroonilise side pealtkuulamist või -vaatamist üksnes valikutingimustele vastavate subjektide sissetuleva ja väljamineva ning nende subjektidega seotud side puhul.

([88]) ODNI kinnitused (VI lisa), lk 18. Vt ka lk 6, mille kohaselt kohaldatavad menetlused „näitavad kindlat soovi vältida signaaliluureandmete meelevaldset ja valimatut kogumist ning rakendada – alates valitsuse kõrgeimast tasandist – mõistlikkuse põhimõtet".

([89]) Vt „Statistical Transparency Report Regarding Use of National Security Authorities", 22. aprill 2015. Interneti andmevoogude kohta üldiselt vt nt Euroopa Liidu Põhiõiguste Amet, Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU (2015), lk 15–16. Mis puutub programmi UPSTREAM, siis vastavalt kustutatud salastatusega FISC arvamusele aastast 2011 päreneb üle 90 % FISA paragrahvi 702 kohaselt kogutud sidest programmist PRISM ja vähem kui 10 % programmist UPSTREAM. Vt FISC, Memorandum Opinion, 2011 WL 10945618 (FISA Ct., 3.10.2011), märkus 21 (kättesaadav aadressil: http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf).

([90]) Vt PPD-28 paragrahv 4(a)(ii). Vt ka ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive, 28. juuli 2014, lk 5, mille kohaselt „peaksid luureühenduse liikmete tegevuspõhimõtted toetama olemasolevaid analüüsitavasid ja -standardeid ning analüütikud peavad püüdma päringuid või muid otsingutingimusi ja -meetodeid struktureerida, et määratleda õiguspärase luure- või õiguskaitseülesandega seonduvad luureandmed; päringud isikute kohta peaksid kuuluma luure- või õiguskaitsevajadusele vastavate luureandmete kategooriasse; luure- või õiguskaitsevajadustega mitteseotud isikuandmete läbivaatamine tuleks viia miinimumini". Vt nt CIA, Signals Intelligence Activities, lk 5; FBI, Presidential Policy Directive 28 Policies and Procedures, lk 3. Vastavalt aruandele „2016 Progress Report on the Signals Intelligence Reform" on luureühenduse liikmed (sh FBI, CIA ja NSA) astunud samme, et suurendada oma töötajate teadlikkust PPD-28 nõuetest, luues uusi või muutes olemasolevaid koolituskavu.

([91]) ODNI kinnituste kohaselt kehtivad need piirangud sõltumata sellest, kas kogumine oli massiline või sihipärane, ja isiku kodakondsusest.

(85) USA valitsuse selgituse kohaselt tähendab kõnealune mõistlikkuse nõue, et luureühenduse liikmed ei pea mitte võtma „kõiki teoreetiliselt võimalikke meetmeid“, vaid et neil tuleb „tasakaalustada oma püüded kaitsta seaduslikke eraelu puutumatuse ja kodanikuvabaduste huve signaaliluuretegevuse praktiliste vajadustega“ ([92]). Seejuures koheldakse USA-väliseid isikuid samamoodi kui USA isikuid, võttes aluseks justiitsministri kinnitatud menetlused ([93]).

(86) Nende normide kohaselt ei või säilitamistähtaeg üldjuhul ületada viit aastat, kui seadusega pole ette nähtud teisiti ja puudub selgesõnaline vastupidine korraldus, mille annab riigi luuredirektor pärast eraelu puutumatuse kaitse kaalutluste hoolikat hindamist – võttes arvesse ODNI kodanikuvabaduste kaitse ametniku arvamust ning asutuste eraelu puutumatuse ja kodanikuvabaduste kaitse ametnike arvamusi, mille kohaselt on säilitamise jätkamine riikliku julgeoleku huvides ([94]). Jagamine piirdub juhtudega, kus teave on kogumise põhjuseks olnud eesmärgil vajalik ja vastab seega välisluure või õiguskaitsega seotud vajadusele ja loale ([95]).

(87) USA valitsus on kinnitanud, et isikuandmeid ei või jagada üksnes põhjusel, et asjaomane isik ei ole USA isik ning „signaaliluureandmeid välismaise isiku igapäevase tegevuse kohta ei loeta välisluureandmeteks, mida võib ainuüksi selle asjaolu alusel jagada või alaliselt säilitada, välja arvatud juhul, kui see vastab muul viisil välisluure või õiguskaitsega seotud vajadusele ja loale“ ([96]).

(88) Eeltoodu põhjal järeldab komisjon, 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.

(89) Nagu eelnevast analüüsist nähtub, on USA seadustega tagatud, et jälgimismeetmeid rakendatakse ainult välisluureandmete saamiseks (mis kujutab endast õigustatud poliitilist eesmärki) ([97]) ja need on nii juhtumipõhised kui

([92]) Vt ODNI kinnitused (VI lisa).
([93]) Vt PPD-28 paragrahv 4(a)(i) ja E.O. 12333 paragrahv 2.3.
([94]) Vt PPD-28 paragrahv 4(a)(i). ODNI kinnitused (VI lisa), lk 7. Näiteks FISA paragrahvi 702 alusel kogutavate isikuandmete puhul näevad FISC kinnitatud NSA minimeerimismenetlused reeglina ette, et programmis PRISM säilitatakse liigitamata sisu metaandmeid kuni viis aastat ja programmis UPSTREAM kuni kaks aastat. NSA järgib neid säilitamispiiranguid automatiseeritud protsessi abil, mis säilitamistähtaja lõppemisel kustutab kogutud andmed. Vt NSA paragrahvi 702 FISA minimeerimismenetlused, paragrahv 7 koos paragrahviga 6(a)(1); NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16. aprill 2014. Ka FISA paragrahvi 501 (endine seaduse U.S. PATRIOT ACT paragrahv 215) puhul on säilitamistähtaeg viis aastat, välja arvatud juhul, kui isikuandmed moodustavad osa nõuetekohase loa alusel jagatavatest välisluureandmetest või justiitsministeerium teatab NSA-le kirjalikult, et andmeid tuleb säilitada seoses käimasoleva või kavandatava kohtumenetlusega. Vt NSA, CLPO, Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15. jaanuar 2016.
([95]) Eriti just FISA paragrahvi 501 (endine seaduse U.S. PATRIOT ACT paragrahv 215) puhul võib isikuandmeid jagada üksnes terrorismivastasel otstarbel või kuriteo tõendina ning FISA paragrahvi 702 puhul üksnes juhul, kui selleks on õiguspärane välisluure või õiguskaitsega seotud vajadus. Vt NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16. aprill 2014. Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15. jaanuar 2016. Vt ka NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333, 7. oktoober 2014.
([96]) ODNI kinnitused (VI lisa), lk 7 (viitega direktiivile Intelligence Community Directive (ICD) 203).
([97]) Euroopa Kohus on selgitanud, et riiklik julgeolek kujutab endast õigustatud poliitilist eesmärki. Schrems, punkt 88. Vt ka Digital Rights Ireland ja teised, punktid 42–44 ja 51, milles Euroopa Kohus leidis, et võitlus raske kuritegevuse, eeskätt organiseeritud kuritegevuse ja terrorismi vastu võib suures ulatuses sõltuda nüüdisaegse uurimistehnika kasutamisest. Lisaks sellele, vastupidiselt kriminaaluurimisele, mille eesmärgiks on üldjuhul tagasiulatuv vastutuse ja süü tõendamine seoses minevikus toimunud käitumisega, keskendub luuretegevus sageli riiklikku julgeolekut ohustavate asjaolude ennetamisele enne kahju tekkimist. Seega on võimalik, et sellised juurdlused peavad hõlmama suuremat hulka võimalikke objekte (nn sihtmärke) ja laiemat geograafilist ala. Vt EIK, 29. juuni 2006, Weber ja Saravia *vs.* Saksamaa, toimik nr 54934/00, punktid 105–118 (nn strateegilise järelevalve kohta).

võimalik. Ennekõike on massiandmekogumine lubatud ainult erandjuhul, kui sihipärane kogumine ei ole võimalik, ja sellega koos rakendatakse täiendavaid meetmeid, et viia miinimumini kogutavate andmete hulk ja neile hilisem juurdepääs (mis peab olema sihipärane ja lubatud ainult konkreetsel eesmärgil).

(90) Komisjoni hinnangul vastab see Euroopa Kohtu poolt kohtuasjas Schrems antud otsusega väljendatud seisukohale, mille kohaselt õigusaktiga, millega kaasneb sekkumine harta artiklitega 7 ja 8 tagatud põhiõigustesse, peavad olema kehtestatud „miinimumnõuded [kaitsenõuded]“ ([98]) ja „[r]angelt vajalikuga ei piirdu õigusakt, mis annab üldise loa säilitada kõikide selliste isikute kõik isikuandmed, kelle andmed on edastatud liidust Ameerika Ühendriikidesse, ilma et olenevalt taotletavast eesmärgist esineks eristamist, piiranguid või erandeid ning ilma, et oleks ette nähtud objektiivset kriteeriumi, mis võimaldaks piiritleda ametiasutuste juurdepääsu andmetele ja nende hilisemat kasutamist konkreetsetel rangelt piiritletud eesmärkidel, millega nii andmete tutvumise kui ka kasutamisega kaasnev sekkumine võib olla põhjendatud“ ([99]). Ka ei ole lubatud piiramatu andmete kogumine ja säilitamine kõigi inimeste kohta igasuguste piiranguteta, samuti piiramatu juurdepääs neile. Lisaks sellele välistavad komisjonile antud kinnitused, mis hõlmavad lubadust, et Ameerika Ühendriikide signaaliluuretegevus puudutab ainult murdosa kogu internetis toimuvast suhtlusest, võimaluse „üldiseks“ ([100]) juurdepääsuks elektroonilise side sisule.

### 3.1.2. Tõhus õiguskaitse

(91) Komisjon on hinnanud nii Ameerika Ühendriikides olemasolevaid järelevalvemehhanisme, et uurida USA luureasutuste sekkumist Ameerika Ühendriikidesse isikuandmete edastamisse, kui ka ELi andmesubjektide võimalusi taotleda üksikisiku õiguskaitset.

*Järelevalve*

(92) USA luureühenduse suhtes kohaldatakse erinevaid läbivaatamis- ja järelevalvemehhanisme, mis kuuluvad riigivõimu kolme haru alla. Need hõlmavad täidesaatva võimu raames tegutsevaid sise- ja välisorganeid, mitut USA Kongressi komiteed, samuti spetsiaalselt välisluure jälitustegevuse seadusega reguleeritud tegevusega seonduvat kohtulikku järelevalvet.

(93) Esiteks teeb USA asutuste luuretegevuse üle ulatuslikku järelevalvet täidesaatev võim.

(94) Vastavalt PPD-28 paragrahvile 4(a)(iv) peavad luureühenduse liikmete normid ja menetlused „sisaldama sobivaid meetmeid isikuandmete kaitse abinõude rakendamise järelevalve soodustamiseks“; üks neist meetmetest peaks olema korrapärane auditeerimine ([101]).

([98]) Schrems, punkt 91 koos edasiviidetega.
([99]) Schrems, punkt 93.
([100]) Schrems, punkt 94.
([101]) ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, lk 7. Vt nt CIA, Signals Intelligence Activities, lk 6 (Compliance); FBI, Presidential Policy Directive 28 Policies and Procedures, paragrahv III (A)(4), (B)(4); NSA, PPD-28 Section 4 Procedures, 12. jaanuar 2015, paragrahv 8.1, 8.6(c).

(95) Selleks on loodud mitu järelevalvetasandit, sealhulgas kodanikuvabaduste või eraelu kaitse ametnikud, peainspektorid, ODNI eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon, PCLOB ning luuretegevuse järelevalve nõukogu presidendi juures. Neid järelevalvefunktsioone toetavad kõikides asutustes töötavad vastavuskontrolliametnikud ([102]).

(96) Nagu USA valitsus on selgitanud, ([103]) on luuretegevusega seotud ministeeriumites ja luureasutustes olemas järelevalvekohustusi täitvad *kodanikuvabaduste või eraelu kaitse ametnikud* ([104]). Ehkki nende ametnike konkreetsed volitused on volitusnormidest sõltuvalt erinevad, on üldjuhul nende pädevuses teha järelevalvet menetluste üle, millega tagatakse ministeeriumis/asutuses eraelu puutumatuse ja kodanikuvabaduste kaitsega seotud küsimuste nõuetekohane käsitlemine ning et asutus on kehtestatud nõuetekohased menetlused enda eraelu puutumatuse või kodanikuvabaduste rikkumise üle kaevanud üksikisikute kaebuste läbivaatamiseks (ning mõningatel asutustel, näiteks ODNI-l, on ka õigus kaebusi iseseisvalt uurida) ([105]). Ministeeriumi/asutuse juht peab omakorda tagama, et ametnik saaks kogu teabe ja juurdepääsu materjalidele, mida ta oma tööks vajab. Kodanikuvabaduste ja eraelu puutumatuse kaitse ametnikud esitavad kongressile ja PCLOB-le korrapäraselt aruandeid, mis sisaldavad ka laekunud kaebuste arvu ja liiki ministeeriumite/asutuste kaupa ning kokkuvõtet kaebuste lahendamisest, tehtud järelevalvest ja uuringutest ning ametniku tegevuse mõjust ([106]). Riiklike andmekaitseasutuste hinnangu kohaselt võib kodanikuvabaduste või eraelu kaitse ametnike tehtavat sisekontrolli pidada „küllaltki tõhusaks“, ehkki nende arvates ei ole need ametnikud vajalikul määral sõltumatud ([107]).

(97) Lisaks on igal luureühenduse liikmel oma *peainspektor*, kelle üheks tööülesandeks on jälgida välisluuretegevust ([108]). Nende hulka kuulub ODNI peainspektori amet, millel on ulatuslik pädevus kogu luureühenduse suhtes ning õigus uurida kaebusi või teavet väidetava ebaseadusliku tegevuse või võimu kuritarvitamise kohta ODNI ja/või luureühenduse programmides ja tegevustes ([109]). Peainspektorid on seaduse järgi sõltumatud ([110]) üksused, kes vastutavad vastava asutuse riikliku julgeolekuga seotud programmide ja tegevuste auditeerimise ja uurimise eest, sealhulgas kuritarvituste ja seaduserikkumiste puhul ([111]). Neil on juurdepääsuõigus kõikidele andmetele,

([102]) Näiteks NSA vastavusosakonnas on üle 300 vastavusküsimustega tegeleva töötaja. Vt ODNI kinnitused (VI lisa), lk 7.

([103]) Vt Ombudsmani mehhanism (III lisa), jao 6(b) punktid (i)–(iii).

([104]) Vt 42 U.S.C. § 2000ee-1. Nende hulgas on näiteks välisministeerium, justiitsministeerium (sh FBI), sisejulgeoleku ministeerium, kaitseministeerium, NSA, CIA ja ODNI.

([105]) USA valitsus on selgitanud, et kui ODNI kodanikuvabaduste ja eraelu puutumatuse büroo saab kaebuse, koordineerib ta kaebuse edasise menetlemise võimalikku käiku luureühenduses selle teiste liikmetega. Vt Ombudsmani mehhanism (III lisa), jagu 6(b) (ii).

([106]) Vt 42 U.S.C. § 2000ee-1 (f)(1),(2).

([107]) Artikli 29 alusel asutatud andmekaitse töörühm, arvamus 01/2016 ELi-USA andmekaitseraamistiku Privacy Shield piisavusotsuse eelnõu kohta (vastu võetud 13. aprill 2016), lk 41.

([108]) ODNI kinnitused (VI lisa), lk 7. Vt nt NSA, PPD-28 Section 4 Procedures, 12. jaanuar 2015, paragrahv 8.1; CIA, Signals Intelligence Activities, lk 7 (Responsibilities).

([109]) Peainspektori ametikoht loodi oktoobris 2010. Peainspektori nimetab ametisse president ja kinnitab senat ning teda saab ametist vabastada ainult president, mitte riigi luuredirektor.

([110]) Need peainspektorid määratakse ametisse tähtajatult ning neid võib ametist vabastada üksnes president, kes peab ametist vabastamist USA Kongressile kirjalikult põhjendama. See ei tähenda, et nad on oma tegevuses täiesti vabad. Teatavatel juhtudel võib organisatsiooni juht keelata peainspektoril auditi või uurimise algatamise, teostamise või lõpuleviimise, kui seda peetakse vajalikuks oluliste riiklike (julgeolekuga seotud) huvide kaitsmiseks. Ent selle õiguse kasutamisest tuleb teatada USA Kongressile, kes võib asjaomase juhi sel alusel vastutusele võtta. Vt nt 1978. aasta peainspektori seadus (Inspector General Act of 1978), § 8 (kaitseministeeriumi peainspektor); § 8E (justiitsministeeriumi peainspektor), § 8G (d)(2)(A),(B) (NSA peainspektor); 50. U.S.C. § 403q (b) (CIA peainspektor); Intelligence Authorization Act For Fiscal Year 2010, paragrahv 405(f) (luureühenduse peainspektor). Riiklike andmekaitseasutuste hinnangu kohaselt vastavad peainspektorid „tõenäoliselt korralduslikku sõltumatuse kriteeriumitele, nagu need on määratlenud Euroopa Liidu Kohus ja Euroopa Inimõiguste Kohus, vähemalt alates sellest, kui uut ametisse nimetamise korda kohaldatakse kõigi suhtes“. Vt artikli 29 alusel asutatud andmekaitse töörühm, arvamus 01/2016 ELi-USA andmekaitseraamistiku Privacy Shield piisavusotsuse eelnõu kohta (vastu võetud 13. aprill 2016), lk 40.

([111]) Vt ODNI kinnitused (VI lisa), lk 7. Vt ka Inspector General Act of 1978 (muudetud), Pub. L. 113–126, 7. juuli 2014.

aruannetele, audititele, protokollidele, dokumentidele, poliitikamaterjalidele, soovitustele ja muudele materjalidele, vajaduse korral kohtuliku teabenõude alusel, ning nad võivad võtta tunnistajatelt ütlusi ([112]). Ehkki peainspektorid võivad anda üksnes mittesiduvaid soovitusi parandusmeetmeteks, avalikustatakse nende aruanded ja teave aruannete alusel võetud meetmete (või nende puudumise) kohta ning saadetakse lisaks USA Kongressile, kes võib nende alusel ise järelevalvet teha ([113]).

(98) Peale selle täidab *eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon* (Privacy and Civil Liberties Oversight Board, edaspidi „PCLOB"), täitevvõimu osaks olev sõltumatu organ, ([114]) mille kaheparteilise ja viieliikmelise juhatuse ([115]) määrab ametisse president Senati heakskiidul, terrorismivastaste normide ja nende rakendamisega seotud ülesandeid, et kaitsta eraelu puutumatust ja kodanikuvabadusi. Luureühenduse tegevuse läbivaatamisel on tal juurdepääsuõigus kõikidele asjaomaste asutuste andmetele, aruannetele, audititele, protokollidele, dokumentidele, poliitikamaterjalidele ja soovitustele, sealhulgas salastatud teabele, ning õigus küsitleda isikuid ja võtta tunnistajatelt ütlusi. Ta saab aruandeid mitmete föderaalministeeriumite/asutuste ([116]) kodanikuvabaduste ja eraelu puutumatuse kaitse ametnikelt, võib anda neile soovitusi ning annab korrapäraselt aru USA Kongressi komisjonidele ja presidendile ([117]). PCLOB ülesandeks on koostada oma volituste ulatuses ka hindamisaruanne PPD-28 rakendamise kohta.

(99) Lisaks täiendab eespool nimetatud järelevalvemehhanisme presidendi luuretegevuse nõuandekogu juurde loodud *luuretegevuse järelevalve nõukogu*, mis jälgib USA luureorganite tegevuse vastavust konstitutsioonile ja kõigile kehtivatele eeskirjadele.

(100) Järelevalve hõlbustamiseks soovitatakse luureühenduse liikmetel kujundada infosüsteeme selliselt, et oleks võimalik jälgida, salvestada ja läbi vaadata isikuandmetega seotud päringuid ja muid otsinguid ([118]). Järelevalve- ja vastavuskontrolliorganid kontrollivad korrapäraselt luureühenduse liikmete tavasid signaaliluureandmetes sisalduvate isikuandmete kaitsmisel ja nimetatud menetluste järgimist ([119]).

(101) Neid järelevalvefunktsioone toetavad ka ulatuslikud vastavuskontrolliga seotud aruandlusnõuded. Asutuste menetlused peavad eelkõige tagama, et kui esineb oluline nõuetele vastavuse probleem seoses mis tahes kodakondsusega isiku signaaliluure raames kogutud isikuandmetega, teavitatakse probleemist viivitamata luureühenduse asjaomase liikme juhti, kes omakorda teavitab riigi luuredirektorit, kes otsustab vastavalt suunisele PPD-28 parandusmeetmete vajalikkuse üle ([120]). Lisaks peavad kõik luureühenduse liikmed vastavalt korraldusele E.O. 12333 andma mittevastavuse juhtumitest aru luuretegevuse järelevalve nõukogule ([121]). Need mehhanismid

([112]) Vt 1978. aasta peainspektori seadus (Inspector General Act of 1978), § 6.
([113]) Vt ODNI kinnitused (VI lisa), lk 7. Vt ka 1978. aasta peainspektori seadus (Inspector General Act of 1978), § 4 lg 5 ja § 5. Vastavalt Intelligence Authorization Act For Fiscal Year 2010, Pub. L. 111–259, 7. oktoober 2010, paragrahvi 405(b) lõigetele 3 ja 4 hoiab luureühenduse peainspektor riigi luuredirektorit ja kongressi kursis parandusmeetmete vajaduse ja rakendamise edusammudega.
([114]) Riiklike andmekaitseasutuste hinnangu kohaselt on PCLOB minevikus „tõestanud oma autonoomset pädevust". Vt artikli 29 alusel asutatud andmekaitse töörühm, arvamus 01/2016 ELi-USA andmekaitseraamistiku Privacy Shield piisavusotsuse eelnõu kohta (vastu võetud 13. aprill 2016), lk 42.
([115]) Lisaks on PCLOB-l umbes 20 tavatöötajat. Vt https://www.pclob.gov/about-us/staff.html.
([116]) Need on vähemalt justiitsministeerium, kaitseministeerium, sisejulgeoleku ministeerium, riigi luuredirektor ja Luure Keskagentuur ning lisaks muud ministeeriumid, asutused või täitevvõimu organid, kelle puhul PCLOB seda vajalikuks peab.
([117]) Vt 42 U.S.C. § 2000ee. Vt Ombudsmani mehhanism (III lisa), jagu 6(b) (iv). Muu hulgas on PCLOB-l teavitamiskohustus juhul, kui mõni täitevvõimuorgan keeldub selle nõuandeid järgmast.
([118]) ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, lk 7–8.
([119]) Samas, lk 8. Vt ka ODNI kinnitused (VI lisa), lk 9.
([120]) ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, lk 7. Vt nt NSA, PPD-28 Section 4 Procedures, 12. jaanuar 2015, paragrahvid 7.3, 8.7(c), (d). FBI, Presidential Policy Directive 28 Policies and Procedures, paragrahvid III (A)(4), (B)(4); CIA, Signals Intelligence Activities, lk 6 (Compliance) ja lk 8 (Responsibilities).
([121]) Vt E.O. 12333, paragrahv 1.6(c).

tagavad, et probleemiga tegeletakse luureühenduse kõrgeimal tasandil. Kui tegemist on USA-välise isikuga, otsustab riigi luuredirektor pärast välisministri ja mittevastavusest teatanud ministeeriumi või asutuse juhiga nõupidamist, kas tuleks astuda samme vastava välisriigi valitsuse teavitamiseks, tagades seejuures allikate ja meetodite ning USA teenistuses olevate isikute kaitse ([122]).

(102) Teiseks on lisaks neile täitevvõimu järelevalvemehhanismidele USA kongressil, täpsemalt *esindajatekoja ja senati luure- ja kohtukomiteel* järelevalvekohustused kogu USA välisluuretegevuse suhtes, kaasa arvatud USA signaaliluure. Vastavalt riikliku julgeoleku seadusele (National Security Act) peab president „tagama, et kongressi luurekomiteedel oleks täielik ja ajakohane teave Ameerika Ühendriikide luuretegevuse kohta, sealhulgas oluliste tulevikus kavandatavate luuretegevuste kohta vastavalt käesoleva alapeatüki nõuetele“ ([123]). Samuti peab president „tagama, et kongressi luurekomiteesid teavitatakse viivitamata mis tahes ebaseaduslikust luuretegevusest ja ebaseadusliku tegevusega seoses võetud või kavandatavatest parandusmeetmetest“ ([124]). Nimetatud komiteede liikmetel on juurdepääs salastatud teabele ning luuremeetoditele ja -programmidele ([125]).

(103) Hilisemate õigusaktidega on nii luureühenduse liikmete, asjaomaste peainspektorite kui ka justiitsministri aruandlusnõudeid laiendatud ja täpsustatud. Näiteks nõuab FISA, et justiitsminister peab senati ja esindajatekoja luure- ja kohtukomiteesid „täielikult teavitama“ mõningate FISA paragrahvide alla kuuluvatest valitsuse tegevustest ([126]). Samuti nõuab see, et valitsus esitaks kongressi komiteedele „koopiad kõikidest vastuluurekohtu või vastuluure apellatsioonikohtu otsustest, korraldustest ja arvamustest, millega olulisel määral sisustatakse või tõlgendatakse“ FISA sätteid. Eelkõige tehakse FISA paragrahvi 702 kohase jälgimisega seoses järelevalvet luure- ja kohtukomiteedele seaduse alusel esitatavate aruannete ning sagedase teavitamise ja kuulamiste kaudu. Nende hulgas on kaks korda aastas esitatav justiitsministri aruanne FISA paragrahvi 702 kasutamise kohta koos tõendavate dokumentidega, eelkõige justiitsministeeriumi ja ODNI vastavuskontrolli aruannetega ning mittevastavusjuhtumite kirjeldusega, ([127]) ning samuti kaks korda aastas esitatav justiitsministri ja DNI hinnang, milles kirjeldatakse suunamis- ja minimeerimismenetluste, sealhulgas selliste menetluste järgimist, mille ülesanne on tagada, et kogumine toimub õiguspärasel välisluure-eesmärgil ([128]). Samuti saab kongress aruandeid peainspektoritelt, kes on volitatud hindama suunamis- ja minimeerimismenetluste ning justiitsministri suuniste järgimist asutustes.

(104) Vastavalt 2015. aasta seadusele USA FREEDOM Act peab USA valitsus igal aastal kongressile (ja üldsusele) muu hulgas avaldama taotletud ja saadud FISA korralduste ja direktiivide arvu ning luuretegevuse objektiks olnud USA isikute ja USA-väliste isikute hinnangulise arvu ([129]). Kõnealune seadus nõuab ka välja antud NSL-ide arvu

([122]) PPD-28, paragrahv 4(a)(iv).
([123]) Vt paragrahv 501(a)(1) (50 U.S.C. § 413(a)(1)). See säte sisaldab üldnõudeid seoses kongressi järelevalvega riikliku julgeoleku valdkonnas.
([124]) Vt paragrahv 501(b) (50 U.S.C. § 413(b)).
([125]) Vt paragrahv 501(d) (50 U.S.C. § 413(d)).
([126]) Vt 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.
([127]) Vt 50 U.S.C. § 1881f.
([128]) Vt 50 U.S.C. § 1881a(l)(1).
([129]) Vt seadus USA FREEDOM Act of 2015, Pub. L. No. 114–23, paragrahv 602(a). Lisaks on paragrahvis 402 sätestatud, et „riigi luuredirektor korraldab justiitsministriga kooskõlastatult salastatusest vabastamise läbivaatamise kõikidele välisluure järelevalvekohtu või (paragrahvis 601(e) sätestatud) välisluure järelevalve apellatsioonikohtu otsustele, määrustele ja arvamustele, milles on oluliselt sisustatud või tõlgendatud õigusnorme, sealhulgas uudsel või olulisel viisil sisustatud või tõlgendatud mõistet „konkreetne valikutingimus”, ning avalikustab selle läbivaatamise tulemustest lähtuvalt need otsused, määrused või arvamused võimalikult suures ulatuses“.

avalikustamist eraldi USA isikute ja USA-väliste isikute kohta (lubades samas FISA korralduste ja kinnituste ning NSL-ide saajatel avaldada teatavatel tingimustel läbipaistvusaruandeid) ([130]).

(105) Kolmandaks peab USA riigiasutuste luuretegevus olema kontrollitav ning eeldab teatavatel juhtudel ka meetmete eelnevat heakskiitu *FISA kohtu* (FISC) ([131]) poolt, mis on sõltumatu kohus, ([132]) kelle otsuseid saab vaidlustada välisluure apellatsioonikohus (FISCR) ([133]) ning lõpuks Ameerika Ühendriikide ülemkohtus ([134]). Kui on nõutav eelnev heakskiit, peavad taotlevad asutused (FBI, NSA, CIA jne) esitama taotluse projekti justiitsministeeriumi riikliku julgeoleku osakonna juristidele, kes vaatavad selle läbi ning küsivad vajaduse korral täiendavat teavet ([135]). Kui taotlus on lõplikult valmis, peab selle heaks kiitma justiitsminister, asejustiitsminister või asejustiitsminister riikliku julgeoleku küsimustes ([136]). Seejärel esitab justiitsministeerium taotluse FISC-le, kes hindab taotlust ja teeb esialgse otsuse, kuidas edasi tegutseda ([137]). Istungi toimumise korral on FISC-l õigus küsitleda tunnistajaid ja küsida nõu ekspertidelt ([138]).

(106) FISCd (ja FISCRi) abistab viieliikmeline alaline komitee, millesse kuuluvad riikliku julgeoleku küsimuste ja kodanikuvabaduste eksperdid ([139]). Kohus määrab nende seast ühe isiku täitma *amicus curiae* ülesandeid, et aidata läbi vaadata taotlusi või muudatusi, mis kohtu hinnangul sisaldavad õigusnormide uudset või olulist tõlgendust, välja arvatud juhul, kui kohus peab sellise ülesande määramist mittevajalikuks ([140]). See peab eelkõige tagama, et kohtu hinnangus võetakse nõuetekohaselt arvesse eraelu puutumatuse kaalutlusi. Kohus võib määrata mõne üksikisiku või organisatsiooni *amicus curiae* ülesannetesse ja tehniliseks eksperdiks ka juhul, kui ta seda vajalikuks peab, või anda seda taotlevale üksikisikule või organisatsioonile loa esitada *amicus curiae* memorandum ([141]).

---

([130]) USA FREEDOM Act, paragrahvid 602(a), 603(a).

([131]) Teatavat liiki jälgimise puhul võib alternatiivina taotlusi läbi vaadata ja määrusi anda Ameerika Ühendriikide ülemkohtu esimehe poolt avalikult määratud USA föderaalkohtu magistraat.

([132]) FISC koosneb üheteistkümnest kohtunikust, kelle nimetab ametisse Ameerika Ühendriikide ülemkohtu esimees USA ringkonnakohtu kohtunike hulgast, kelle on eelnevalt ametisse nimetanud president ja kinnitanud senat. Kohtunikud nimetatakse ametisse määramata ajaks, neid saab ametist vabastada üksnes mõjuvatel põhjustel ning nende ametiaeg FISCs kestab seitse aastat ega kattu teiste kohtunike ametiajaga. FISA kohaselt tuleb kohtunikud määrata vähemalt seitsmest erinevast USA kohturingkonnast. Vt FISA paragrahv 103 (50 U.S.C. § 1803 (a)); PCLOB, Sec. 215 Report, lk 174–187. Kohtunikke abistavad kogenud kohtunikuabid, kes moodustavad kohtu juriidilise personali ning valmistavad ette kogumistaotluste õiguslikud analüüsid. Vt PCLOB, Sec. 215 Report, lk 178; Letter from the Honourable Reggie B. Walton, Presiding Judge, U.S. Foreign Intelligence Surveillance Court, to the Honourable Patrick J. Leahy, Chairman, Committee on the Judiciary, U.S. Senate (29. juuli 2013) (edaspidi „Waltoni kiri"), lk 2–3.

([133]) FISCR koosneb kolmest kohtunikust, kelle nimetab ametisse Ameerika Ühendriikide ülemkohtu esimees USA ringkonna- või apellatsioonikohtute kohtunike hulgast ja nende ametiaeg kestab seitse aastat ega kattu teiste kohtunike ametiajaga. Vt FISA paragrahv 103 (50 U.S.C. § 1803 (b)).

([134]) Vt 50 U.S.C. §§ 1803 (b), 1861 a (f), 1881 a (h), 1881 a (i)(4).

([135]) Näiteks täiendavad faktilised andmed jälgitava sihtmärgi kohta, jälgimismeetodite tehnilised andmed ja kinnitused selle kohta, kuidas saadud andmeid kasutatakse ja jagatakse. Vt PCLOB, Sec. 215 Report, lk 177.

([136]) 50 U.S.C. § 1804 (a), § 1801 (g).

([137]) FISC võib taotluse heaks kiita, küsida lisateavet, määrata vajaduse korral istungi või teatada, et taotlus võidakse jätta rahuldamata. Vastavalt sellele eelotsusele esitab valitsus lõpliku taotluse. See võib algsest taotlusest oluliselt erineda, arvestades kohtuniku esialgset vastust. Kuigi FISC kiidab suurema osa lõplikest taotlustest heaks, sisaldab märkimisväärne osa neist algse taotlusega võrreldes olulisi muudatusi – näiteks juulist septembrini 2013 heaks kiidetud taotlustest muudeti 24 %. Vt PCLOB, Sec. 215 Report, lk 179; Waltoni kiri, lk 3.

([138]) PCLOB, Sec. 215 Report, lk 179, märkus 619.

([139]) 50 U.S.C. § 1803 (i)(1),(3)(A). Nende uute sätetega rakendati ellu PCLOBi soovitused luua eraelu puutumatuse ja kodanikuvabaduste kaitse ekspertide kogu, mille liikmed saaksid täita *amicus curiae* ülesandeid, et anda kohtule õiguslikke argumente eraelu puutumatuse ja kodanikuvabaduste edendamiseks. Vt PCLOB, Sec. 215 Report, lk 183–187.

([140]) 50 U.S.C. § 1803 (i)(2)(A). ODNI andmetel on määramisi juba toimunud. Vt Signals Intelligence Reform, 2016 Progress Report.

([141]) 50 U.S.C. § 1803 (i)(2)(B).

(107) ELi-USA andmekaitseraamistiku Privacy Shield alusel toimuva andmete edastamisega seotud kahe tähtsaima juriidilise jälgimisloa järelevalve toimub FISCs erinevalt.

(108) Vastavalt FISA paragrahvile 501, ([142]) mis lubab koguda „mis tahes materiaalseid esemeid (sealhulgas raamatuid, andmekandjaid, pabereid, dokumente ja muid esemeid)“, peab FISC-le esitatav taotlus sisaldama asjaolude kirjeldust, millest nähtub, et on piisavalt alust pidada soovitavaid materiaalseid esemeid vajalikuks sellise sanktsioneeritud uurimise (muu kui ohuhindamise) huvides, mida viiakse läbi USA-välise isikuga seotud välisluureinfo kogumiseks või kaitseks rahvusvahelise terrorismi või salaluuretegevuse eest. Taotlus peab sisaldama ka kogutud luureandmete säilitamise ja jagamise minimeerimiseks justiitsministri poolt kehtestatud menetluste nimekirja ([143]).

(109) Seevastu FISA paragrahvi 702 puhul ([144]) ei anna FISC luba üksikuteks jälgimismeetmeteks; selle asemel annab ta load jälgimisprogrammide jaoks (nt PRISM, UPSTREAM) vastavalt iga-aastastele vastavuskinnitustele, mille koostavad justiitsminister ja riigi luuredirektor. FISA paragrahv 702 lubab võtta välisluureinfo kogumise sihtmärgiks isikuid, kelle puhul on piisavalt alust arvata, et nad asuvad väljaspool Ameerika Ühendriike ([145]). Sihipärastamist korraldab NSA kahes etapis: esiteks teevad NSA analüütikud kindlaks välismaal asuvad USA-välised isikud, kelle jälgimine võimaldab analüütikute hinnangul saada vastavuskinnituses sätestatud vajalikke välisluureandmeid. Teiseks, pärast nende üksikisikute kindlakstegemist ja nende sihtmärgiks võtmise kinnitamist NSA-sisese põhjaliku kontrollimehhanismi abil, ([146]) võetakse sihtmärkide kasutatavate sidevahendite (nt e-posti aadressid) identimistunnused „ülesandeks“ (st neid arendatakse ja kasutatakse) ([147]). Nagu märgitud, ei sisalda FISC heakskiidetavad kinnitused teavet sihtmärgiks võetavate konkreetsete isikute kohta, vaid neis määratletakse pigem välisluureinfo kategooriad ([148]). Kuigi FISC ei hinda (ei eeldatava põhjuse järgi ega mõnel muul alusel) seda, kas isikud on välisluureinfo kogumise sihtmärgiks valitud õigesti, ([149]) on tal õigus kontrollida tingimust, et „kogumise oluliseks eesmärgiks on saada välisluureinfot“ ([150]). Nimelt on vastavalt FISA paragrahvile 702 NSA-l lubatud jälgida USA-st väljaspool asuvate USA-väliste isikute sidet üksnes juhul, kui on piisavalt alust arvata, et konkreetset sidevahendit kasutatakse välisluureinfo edastamiseks (nt rahvusvahelise terrorismi, tuumarelvade leviku või vaenuliku kübertegevusega seoses). Vastavate diskretsiooniotsuste järelevalvet teevad kohtud ([151]). Kinnitustes tuleb sätestada ka suunamis- ja minimeerimismenetlused ([152]). Justiitsminister ja riigi luuredirektor

([142]) 50 U.S.C. § 1861.
([143]) 50 U.S.C. § 1861 (b).
([144]) 50 U.S.C. § 1881.
([145]) 50 U.S.C. § 1881a (a).
([146]) Vt PCLOB, Sec. 702 Report, lk 46.
([147]) 50 U.S.C. § 1881a (h).
([148]) 50 U.S.C. § 1881a (g). PCLOB andmetel on need kategooriad seni seondunud peamiselt rahvusvahelise terrorismi ning massihävitusrelvade hankimise sarnaste teemadega. Vt PCLOB, Sec. 702 Report, lk 25.
([149]) Vt PCLOB, Sec. 702 Report, lk 27.
([150]) 50 U.S.C. § 1881a.
([151]) „Liberty and Security in a Changing World“, Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies, 12. detsember 2013, lk 152.
([152]) 50 U.S.C.1881a (i).

kontrollivad vastavust ja asutused on kohustatud teatama kõikidest mittevastavuse juhtudest FISC-le ([153]) (samuti kongressile ja presidendi luuretegevuse järelevalve nõukogule), kes võib selle alusel luba muuta ([154]).

(110) Lisaks on USA valitsus FISC järelevalve efektiivsuse suurendamiseks nõustunud rakendama PCLOBi soovitust, mille kohaselt tuleb FISC-ile esitada dokumendid paragrahvi 702 kohaste sihitamisotsuste kohta, sealhulgas juhuvalik ülesandelehtedest, et FISC saaks hinnata välisluure-eesmärgi nõude järgimist praktikas ([155]). Samas on USA valitsus nõustunud muutma NSA sihitamismenetlusi ja astunud selleks samme, et sihitamisotsuste välisluurega seotud põhjuseid paremini dokumenteerida ([156]).

*Üksikisiku õiguskaitse*

(111) USA õigus pakub erinevaid võimalusi ELi andmesubjektidele, kes muretsevad, et nende isikuandmeid võib olla töödeldud (kogutud, vaadatud jm) USA luureühenduse liikmete poolt ja soovivad teada, kas seejuures on järgitud USA õigusest tulenevaid piiranguid. Need hõlmavad põhimõtteliselt kolme valdkonda: sekkumine FISA alusel, riigiametnike tahtlik ebaseaduslik juurdepääs isikuandmetele ja juurdepääs andmetele teabevahetuse seaduse (Freedom of Information Act, FOIA) alusel ([157]).

(112) Esiteks pakub välisluure jälitustegevuse seadus (Foreign Intelligence Surveillance Act) mitmeid USA-välistele isikutele kättesaadavaid õiguskaitsevahendeid ebaseadusliku elektroonilise jälgimise vaidlustamiseks ([158]). Muu hulgas on üksikisikutel võimalik esitada Ameerika Ühendriikide vastu tsiviilhagi, kui nende kohta käivaid andmeid on ebaseaduslikult ja tahtlikult kasutatud või avaldatud, ([159]) esitada (ametivolituste ületamise sätete alusel) rahalisi kahjunõudeid otse USA riigiametnike vastu ([160]) ja vaidlustada jälgimise õiguspärasus (ning otsida võimalusi andmeid mitte avalikustada), kui USA valitsus kavatseb isiku elektroonilise jälgimise käigus kogutud andmeid või neist tuletatud teavet kasutada või avaldada USA kohtu- või haldusmenetluses ([161]).

(113) Teiseks andis USA valitsus komisjonile viited mitmele muule võimalusele, mida ELi andmesubjektid saavad kasutada õiguskaitse hankimiseks riigiametnike vastu, juhul kui valitsusel on tema isikuandmetele juurdepääs või

([153]) FISC töökorra punktis 13(b) on nõutud, et valitsus esitaks kohtule viivitamata kirjaliku teate, kui ta avastab, et mõnd kohtu luba või heakskiitu on rakendatud sellele loale või heakskiidule mittevastaval viisil või ebaseaduslikult. Samuti on sellega nõutud, et valitsus teataks kohtule kirjalikult sellise rikkumise asjaoludest. Üldjuhul esitab valitsus punkti 13(a) kohase lõpliku teate pärast seda, kui kõik faktid on teada ning loata kogutu on hävitatud. Vt Waltoni kiri, lk 10.

([154]) 50 U.S.C. § 1881 (l). Vt ka PCLOB, Sec. 702 Report, lk 66–76. NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16. aprill 2014. Isikuandmete kogumine luure-eesmärkidel vastavalt FISA paragrahvile 702 allub nii täitevvõimu sise- kui välisjärelevalvele. Sisejärelevalve hõlmab muu hulgas asutusesiseseid vastavusprogramme, mille alusel hinnatakse suunamis- ja minimeerimismenetluste nõuetele vastavust; mittevastavuse juhtumitest teatamist nii asutuse sees kui väljapoole – ODNI-le, justiitsministeeriumile, kongressile ja FISC-le; ja neile saadetavaid aastaaruandeid. Väline järelevalve koosneb peamiselt suunamis- ja minimeerimiskontrollidest, mida teevad ODNI, justiitsministeerium ja peainspektorid, kes annavad omakorda aru kongressile ja FISC-ile, sealhulgas mittevastavuse juhtumitest. Olulistest mittevastavuse juhtumitest tuleb FISC-ile teatada viivitamata ja muudest juhtumitest kvartaliaruandes. Vt PCLOB, Sec. 702 Report, lk 66–77.

([155]) PCLOB, Recommendations Assessment Report, 29. jaanuar 2015, lk 20.

([156]) PCLOB, Recommendations Assessment Report, 29. jaanuar 2015, lk 16.

([157]) Lisaks on salastatud teabe menetluste seaduse (Classified Information Procedures Act) paragrahvis 10 sätestatud, et kriminaalasjades, kus Ameerika Ühendriigid soovivad tõendada, et osa materjale on salastatud (nt kuna selle loata avaldamine on keelatud riikliku julgeoleku kaalutlustel), peavad Ameerika Ühendriigid süüalusele teatama, millistele osadele materjalist nad soovivad salastatud teabega seotud süüteo tõendamisel tugineda.

([158]) Vt järgnevad ODNI kinnitused (VI lisa), lk 16.

([159]) 18 U.S.C. § 2712.

([160]) 50 U.S.C. § 1810.

([161]) 50 U.S.C. § 1806.

neid kavatsetakse kasutada ebaseaduslikult, sealhulgas väidetavalt riikliku julgeoleku huvides (näiteks arvutipettuste ja sellealase kuritarvitamise seadus (Computer Fraud and Abuse Act), ([162]) elektroonilise side seadus ([163]) ja finantsandmetega seotud eraelu puutumatuse seadus (Right to Financial Privacy Act)) ([164]). Kõik need kaebeõiguse alused on seotud konkreetsete andmete, sihtmärkide ja/või juurdepääsu liikidega (nt kaugjuurdepääs arvutile Interneti kaudu) ning neile saab tugineda teatavatel tingimustel (nt tahtlik/teadlik tegevus, ametivolituste ületamine, tekitatud kahju) ([165]). Üldisem õiguskaitsevõimalus on olemas haldusmenetluse seaduse (Administrative Procedure Act, 5 U.S.C. § 702) näol, mille kohaselt on „igal isikul, kelle õigusi on rikutud ametkonna tegevusega või keda on negatiivselt mõjutanud või kahjustanud ametkonna tegevus“ õigus pöörduda kohtusse. See hõlmab võimalust taotleda kohtult, et „tunnistatakse ebaseaduslikuks ja jäetakse arvesse võtmata organi tegevus, uurimistulemused ja järeldused, mis leitakse olevat [—] meelevaldsed, suvalised või põhinevat kaalutusõiguse kuritarvitamisel või mis pole muul viisil seadusega kooskõlas“ ([166]).

(114) Peale selle on USA valitsus osutanud, et USA-välised isikud saavad FOIA alusel taotleda juurdepääsu föderaalasutuste registritele, sealhulgas konkreetse isiku isikuandmeid sisaldavatele registritele ([167]). FOIA eesmärki arvestades ei paku see võimalust saada individuaalset õiguskaitset isikuandmete käsitlemise kui sellise vastu, ent võimaldab üksikisikutel põhimõtteliselt saada juurdepääsu riiklikes luureasutustes hoitavale asjakohasele teabele. Isegi sel juhul näivad võimalused olevat piiratud, kuna asutused võivad keelduda teatavate loetletud erandite alla kuuluva teabe avaldamisest, sealhulgas juurdepääsust riikliku julgeoleku huvides salastatud teabele ja õiguskaitseorganite uurimisinfole ([168]). Samas saavad üksikisikud riiklike luureasutuste poolt neile eranditele tuginemise vaidlustada nii haldusmenetluse korras kui ka kohtus.

(115) Kuigi isikutele, sealhulgas ELi andmesubjektidele, keda on riikliku julgeoleku huvides ebaseaduslikult (elektrooniliselt) jälgitud, on saadaval erinevaid õiguskaitsevõimalusi, on samas selge, et vähemalt mõnesid USA luureametkondade kasutatavaid õiguslikke aluseid (nt korraldust E.O. 12333) need ei hõlma. Isegi kui kohtuliku kaitse võimalused USA-välistele isikutele on põhimõtteliselt olemas, näiteks FISA alusel toimuva jälgimise puhul, on õiguskaitsevahendite kasutamine piiratud ([169]) ning üksikisikute (sh USA isikute) esitatavaid nõudeid ei võeta menetlusse, kui nad ei suuda tõendada „õigustatud huvi“, ([170]) mistõttu tavakohtutele juurdepääs on piiratud ([171]).

(116) Et luua veel üks kõikidele ELi andmesubjektidele kättesaadav õiguskaitsevõimalus, on USA valitsus otsustanud luua uue, ombudsmani mehhanismi, nagu on märgitud USA välisministri kirjas komisjonile, mis sisaldub käesoleva otsuse III lisas. See mehhanism põhineb PPD-28 kohasel välisministeeriumi juhtivkoordinaatori (asekantsleri tase) määramisel, kes on välisriikide valitsustele kontaktpunktiks USA signaaliluuretegevusega seotud probleemide tõstatamisel, kuid mehhanism pakub algsest kavandist tunduvalt rohkem lisavõimalusi.

([162]) 18 U.S.C. § 1030.
([163]) 18 U.S.C. §§ 2701–2712.
([164]) 12 U.S.C. § 3417.
([165]) ODNI kinnitused (VI lisa), lk 17.
([166]) 5 U.S.C. § 706 (2)(A).
([167]) 5 U.S.C. § 552. Sarnased seadused on olemas osariikide tasandil.
([168]) Sel juhul saab isik harilikult üksnes standardvastuse, milles asutus keeldub andmete olemasolu kinnitamast või ümber lükkamast. Vt ACLU *vs.* CIA, 710 F.3d 422 (D.C. Cir. 2014).
([169]) Vt ODNI kinnitused (VI lisa), lk 16. Esitatud selgituste kohaselt on õiguskatsevahendite kasutamine võimalik tingimusel, et olemas on kas *kahju* (18 U.S.C. § 2712; 50 U.S.C. § 1810) või tõendid selle kohta, et *valitsus kavatseb kasutada või avaldada* isiku elektroonilise jälgimise käigus kogutud andmeid või neist tuletatud teavet *USA kohtu- või haldusmenetluses selle isiku vastu* (50 U.S.C. § 1806). Nagu Euroopa Kohus on aga korduvalt rõhutanud, ei ole eraelu puutumatuse kui põhiõiguse riive tuvastamise seisukohalt oluline, kas asjaomane isik on riive tõttu kahju kandnud või mitte. Vt Schrems, punkt 89 koos edasiviidetega.
([170]) See menetlussevõtmisse kriteerium tuleneb USA konstitutsiooni III artiklis sätestatud põhjendatusnõudest.
([171]) Vt Clapper *vs.* Amnesty Int'l USA, 133 S.Ct. 1138, 1144 (2013). NSLide kasutamisega seoses sätestab seadus USA FREEDOM Act (paragrahvid 502(f)–503), et avaldamisest keeldumise nõuded tuleb korrapäraselt läbi vaadata ning teavitada NSL-ide *saajaid*, kui avaldamisest keeldumise nõue pole enam faktiliselt põhjendatud (vt ODNI kinnitused (VI lisa), lk 13). See ei taga siiski, et ELi andmesubjekti teavitataks uurimise objektiks olekust.

(117) Eelkõige on USA valitsus võtnud kohustused, et ombudsmani mehhanism tagab üksikisikute kaebuste uurimise ja menetlemise ning et üksikisikud saavad sõltumatu kinnituse, et USA seadusi on järgitud, või kui neid on rikutud, kinnituse rikkumise kõrvaldamise kohta ([172]). Mehhanismi alla kuulub „raamistiku Privacy Shield ombudsman“, see tähendab asekantsler ja muud töötajad, samuti muud järelevalveorganid, kellel on pädevus teha järelevalvet erinevate luureühenduse liikmente üle, kellega koostöös raamistiku ombudsman kaebusi käsitleb. Eelkõige juhul, kui üksikisiku taotlus käsitleb jälgimise kooskõla USA seadustega, saab raamistiku Privacy Shield ombudsman tugineda sõltumatutele uurimisvolitusi omavatele järelevalveorganitele (näiteks peainspektorid või PCLOB). Iga üksiku juhtumi korral tagab riigisekretär ombudsmanile vahendid, mis võimaldavad tagada, et vastused isikute taotlustele põhinevad kogu vajalikul teabel.

(118) Selle „liitstruktuuri“ kaudu tagab ombudsmani mehhanism sõltumatu järelevalve ja üksikisiku õiguskaitse. Lisaks sellele tagab koostöö muude järelevalveorganitega vajalikud eksperditeadmised. Lõpuks, kehtestades raamistiku Privacy Shield ombudsmanile kohustuse kinnitada vastavust või heastada mis tahes mittevastavus, peegeldab mehhanism USA valitsuse kui terviku kindlat soovi ELi üksikisikute kaebuste menetlemiseks ja lahendamiseks.

(119) Esiteks, erinevalt puhtalt valitsustevahelistest mehhanismidest võtab raamistiku Privacy Shield ombudsman vastu kaebusi üksikisikutelt ja menetleb neid. Kaebused on võimalik esitada sellistele liikmesriikide järelevalveasutustele, kelle pädevusse kuulub järelevalve riiklike julgeolekuteenistuste üle ja/või avaliku sektori asutuste poolne isikuandmete töötlemine, ning kes esitavad need kesksele ELi organile, kust nad suunatakse raamistiku Privacy Shield ombudsmanile ([173]). ELi üksikisikutele on see kasulik, kuna nad saavad pöörduda riikliku ametiasutuse poole nii-öelda kodu lähedal ja oma keeles. Nimetatud asutuse ülesandeks on üksikisikuid abistada, et raamistiku Privacy Shield ombudsmanile esitatud taotlused sisaldaksid peamisi andmeid ja et neid saaks seega lugeda „täielikeks“. Üksikisik ei pea tõendama, et USA valitsus on signaaliluuretegevuse kaudu ka tegelikult tema isikuandmetele juurde pääsenud.

(120) Teiseks kohustub USA valitsus tagama, et oma ametiülesannete täitmisel on raamistik Privacy Shield ombudsmanil võimalik toetuda koostööle muude USA seadusega ette nähtud järelevalve- ja nõuetele vastavuse mehhanismidele. See võib mõnikord hõlmata riiklikke luureasutusi, eriti juhul, kui taotlust võib tõlgendada juurdepääsu taotlemisena teabevabaduse seaduse raames. Muudel juhtudel ja eriti, kui taotlused käsitlevad jälgimise kooskõla USA seadustega, hõlmab nimetatud koostöö sõltumatuid järelevalveorganeid (st peainspektoreid), kellel on kohustus ja volitused põhjalikku juurdlust läbi viia (eriti seoses ligipääsuga kõigile asjaomastele dokumentidele ning volitused järelepärimiste esitamiseks ja ütluste taotlemiseks) ja nõuetele mittevastavust menetleda ([174]). Privacy Shieldi ombudsman saab õiguse saata asju arutamiseks ka PCLOBile ([175]). Kui mõni neist järelevalveorganitest tuvastab nõuetele mittevastavuse, peab asjaomane luureühenduse liige (st

([172]) Juhul kui kaebaja taotleb ligipääsu USA avaliku sektori asutuste valduses olevatele dokumentidele, kohaldatakse teabevabaduse seaduses sätestatud eeskirju ja korda. See hõlmab võimalust kasutada taotluse tagasilükkamise korral FOIA-ga sätestatud tingimustel kohtulikke õiguskaitsevahendeid (sõltumatu järelevalve asemel).

([173]) Vastavalt ombudsmani mehhanismi (III lisa) punktile 4(f) suhtleb andmekaitseraamistiku Privacy Shield ombudsman otse ELi üksikisikute kaebusi menetleva organiga, kes omakorda vastutab taotluse esitanud üksikisikuga suhtlemise eest. Kui otsesuhtlus moodustab osa alusprotsessidest, mis võivad pakkuda taotletavat õiguskaitset (nt FOIA juurdepääsutaotlus, vt jagu 5), toimub see suhtlus vastavalt kohaldatavatele menetlustele.

([174]) Vt Ombudsmani mehhanism (III lisa), jagu 2(a). Vt ka põhjendused 0–0.

([175]) Vt Ombudsmani mehhanism (III lisa), jagu 2(c). USA valitsuse selgituste kohaselt jälgib PCLOB pidevalt terrorismivastase võitlusega tegelevate USA asutuste põhimõtteid ja menetlusi, sealhulgas nende rakendamist, et teha kindlaks, kas nad oma tegevuses „kaitsevad nõuetekohaselt piisavalt eraelu puutumatust ja kodanikuvabadusi ning tegutsevad kooskõlas kehtivate eraelu puutumatust ja kodanikuvabadusi käsitlevate õigusaktide ja põhimõtetega.“ Samuti „saab ja vaatab ta läbi eraelu puutumatuse ja kodanikuvabaduste kaitse ametnike aruanded ja muu teabe ning annab neile vajaduse korral soovitusi seoses nende tegevusega.“

luureasutus) mittevastavuse heastama, kuna ainult sellisel juhul on ombudsmanil võimalik anda üksikisikule „positiivne“ vastus (st mittevastavus on kõrvaldatud), milleks USA valitsus on kohustuse võtnud. Samuti teavitatakse raamistiku Privacy Shield ombudsmani koostöö raames juurdluse tulemustest ja ombudsmani käsitusse antakse vahendid, tagamaks, et talle edastatakse kogu vastuse ettevalmistamiseks vajalik teave.

(121) Kõigele lisaks on Privacy Shieldi ombudsman USA luureühendusest sõltumatu ega allu seega selle juhistele ([176]). See on väga oluline, kuna ombudsmani ülesandeks on „kinnitada“, et i) kaebust on nõuetekohaselt uuritud ja ii) kohaldatavat USA õigust, sealhulgas eelkõige VI lisas esitatud piiranguid ja kaitsemeetmeid ei ole rikutud või juhul kui on toimunud rikkumine, on see heastatud. Selle sõltumatu kinnituse andmiseks peab raamistiku Privacy Shield ombudsman saama vajaliku uurimisega seonduva teabe, et hinnata kaebuse vastuse paikapidavust. Lisaks on riigisekretär kohustunud tagama, et asekantsler tegutseb raamistiku Privacy Shield ombudsmani ametis objektiivselt ja vabana mis tahes väärmõjust, mis võib antavat vastust mõjutada.

(122) Üldiselt tagab see mehhanism, et üksikisikute kaebuste suhtes viiakse läbi üksikasjalik uurimine ja et need lahendatakse ning et vähemalt jälgimise valdkonnas on kaasatud sõltumatud järelevalveorganid, kellel on vajalikud eksperditeadmised ja uurimisvolitused, ja ombudsman, kes saab oma ülesandeid täita vabana kahjulikust, eriti poliitiliselt mõjust. Lisaks sellele on üksikisikutel võimalik esitada kaebusi, tõestamata selleks oma jälgimise all olemist, või esitada lihtsalt vihjed jälgimise all olemise kohta ([177]). Nende sätete valgusel leiab komisjon, et olemas on asjakohased ja tõhusad tagatised väärkasutamise vastu.

(123) Eeltoodu põhjal järeldab komisjon, et Ameerika Ühendriigid tagavad tõhusa õiguskaitse, mis ei lase tema luureasutustel riivata nende isikute põhiõigusi, kelle isikuandmeid ELi-USA andmekaitseraamistiku Privacy Shield alusel liidust Ameerika Ühendriikidesse edastatakse.

(124) Sellega seoses võtab komisjon teadmiseks Euroopa Kohtu otsuse kohtuasjas Schrems, mille kohaselt „[s]amuti ei järgi õigusakt, milles ei ole andmesubjektile ette nähtud mingit võimalust kasutada õiguskaitsevahendeid, et tutvuda teda puudutavate isikuandmetega või lasta neisse parandusi teha või neid kustutada, harta artiklis 47 sätestatud põhiõiguse tõhusale kohtulikule kaitsele põhisisu“ ([178]). Komisjoni hinnangu tulemusel on leidnud kinnitust, et seesugused õiguskaitsevahendid on Ameerika Ühendriikides olemas, sealhulgas ombudsmani mehhanismi loomise kaudu. Ombudsmani mehhanismiga nähakse ette sõltumatu uurimisvolitustega järelevalvesüsteem. Komisjoni jälgib raamistikku Privacy Shield jooksvalt, sealhulgas iga-aastase ühise läbivaatamise kaudu, milles osaleb ka ombudsman, ja selle raames antakse uus hinnang nimetatud mehhanismi tõhususele.

3.2. *Juurdepääs ja kasutamine USA avaliku sektori asutuste poolt õiguskaitse ja avalikes huvides*

(125) Seoses ELi-USA andmekaitseraamistiku Privacy Shield alusel edastatud isikuandmete riivega õiguskaitse huvides on USA valitsus (justiitsministeeriumi kaudu) kinnitanud, et kohaldatakse piiranguid ja kaitsemeetmeid, mis komisjoni hinnangul tagavad piisava kaitsetaseme.

([176]) Vt Roman Zakharov *vs* Venemaa, 4. detsembri 2015. aasta otsus (suurkoda) kohtuasjas nr 47143/06, punkt 275 („ehkki põhimõtteliselt on soovitatav, et teenistuslikku järelevalvet teeb kohtunik, võidakse kohtuväliste organite tehtavat järelvalvet lugeda konventsiooniga kooskõlas olevaks tingimusel, et järelevalveorgan ei sõltu jälgimist teostavatest asutustest ja et ta omab piisavaid ja tõhusaid järelevalvevolitusi“).

([177]) Vt Kennedy *vs*. Ühendkuningriik, 18. mai 2010. aasta otsus kohtuasjas nr 26839/05, punkt 167.

([178]) Schrems, punkt 95. Nagu kohtuotsuse punktidest 91 ja 96 selgelt nähtub, käsitleb punkt 95 liidu õiguskorraga tagatud kaitsetaset, millega kolmanda riigi kaitsetase peab olema „sisuliselt võrdväärne“. Vastavalt kohtuotsuse punktidele 73 ja 74 ei pea kolmanda riigi kaitsetase ja tema poolt rakendatavad vahendid olema identsed, ehkki kasutatavad vahendid peavad praktikas tõhusaks osutuma.

(126) Esitatud teabe kohaselt eeldab õiguskaitseorganite poolne läbiotsimine ja konfiskeerimine USA põhiseaduse neljanda muudatuse kohaselt ([179]) põhimõtteliselt ([180]) kohtu määrust, mille saamiseks tuleb tõendada „põhjendatud kahtlust". Üksikutel selgelt sätestatud erandjuhtudel, mille puhul määrust ei nõuta, ([181]) peavad õiguskaitseorganid juhinduma „mõistlikkuse põhimõttest" ([182]). Läbiotsimise või konfiskeerimise mõistlikkuse kindlakstegemiseks tuleb „ühelt poolt hinnata, mil määral see riivab üksikisiku eraelu puutumatust, ja teiselt poolt, kui vajalik on see riigi õiguspäraste huvide teostamiseks" ([183]). Üldisemalt tagab neljas muudatus eraelu puutumatuse, väärikuse ning kaitse valitsusesindajate meelevaldsete ja sekkuvate tegude eest ([184]). Sisuliselt kannavad need põhimõtted liidu õiguse vajalikkuse ja proportsionaalsuse ideed. Kui õiguskaitseorganid konfiskeeritud esemeid enam tõenditena ei vaja, tuleks need tagastada ([185]).

(127) Kuigi põhiseaduse neljanda parandusega antavad õigused ei laiene USA-välistele isikutele, kes ei ela Ameerika Ühendriikides, on neil sellegipoolest kaudselt kasu sellest tulenevast kaitsest, kuna isikuandmed on USA ettevõtete valduses ja sellest tulenevalt peavad õiguskaitseorganid igal juhul taotlema õigusasutuse luba (või vähemalt järgima mõistlikkuse nõuet) ([186]). Täiendava kaitse tagavad spetsiaalsed seaduse alusel tegutsevad ametiasutused ning justiitsministeeriumi suunised, mis piiravad õiguskaitseorganite juurdepääsu andmetele vajalikkus- ja proportsionaalsusnõudega sarnastel alustel (nt kohustades FBI-d kasutama uurimismeetodeid, millega kaasneb võimalikult väike eraelu puutumatuse ja kodanikuõiguste riive) ([187]). USA valitsuse kinnituste kohaselt kohaldatakse samaväärset või tugevamat kaitset ka (osariikide seaduste alusel toimuvatele) osariikide õiguskaitseorganite uurimistele ([188]).

(128) Ehkki kohtu või juurdluskogu (*grand jury* ehk kohtuniku või kohtu-uurija koostatud uurimisorgan) luba ei ole kõikidel juhtudel nõutav, ([189]) on haldusorganitel lubatud teabenõudeid kasutada vaid konkreetsetel juhtudel ning neile rakendatakse ka sõltumatut kohtulikku kontrolli, vähemalt juhul, kui valitsus taotleb kohtult nende jõustamist ([190]).

---

([179]) Neljandas muudatuses on sätestatud, et „[i]nimeste õigust turvalisusele oma isiku, maja, dokumentide ja mõju suhtes ebamõistlike läbiotsimiste ja haarangute vastu ei tohi rikkuda ning läbiotsimismääruseid ei väljastata, välja arvatud tõenäolise põhjuse korral, mis tugineb vandele või kinnitusele ning milles kirjeldatakse konkreetselt läbiotsitavat asukohta ja läbiotsitavaid isikuid või esemeid". Ainult (magistraadid) kohtunikud võivad läbiotsimismääruseid väljastada. Föderaalkohtu määrused elektrooniliselt salvestatud teabe kopeerimiseks on täiendavalt reguleeritud kriminaalmenetluse föderaaleeskirjade (Federal Rules of Criminal Procedure) eeskirjaga 41.

([180]) Ülemkohus on korduvalt viidanud määruseta läbiotsimisele kui „erakorralisele". Vt näiteks Johnson *vs.* Ameerika Ühendriigid, 333 U.S. 10, 14 (1948); McDonald *vs.* Ameerika Ühendriigid, 335 U.S. 451, 453 (1948); Camara *vs* munitsipaalkohus, 387 U.S. 523, 528–29 (1967); *G.M.* Leasing Corp. *vs* Ühendriigid, 429 U.S. 338, 352–53, 355 (1977). Samuti on Ülemkohus korduvalt rõhutanud, et „selle valdkonna peamine riigiõiguslik norm on see, et väljaspool kohtumenetlust, kohtuniku või magistraadi eelneva heakskiiduta läbiviidud läbiotsimine on põhiseaduse neljanda muudatuse – kohaselt iseenesest ebamõistlik ja ses suhtes on kohaldatavaid ainult üksikud spetsiaalselt ette nähtud ja täpselt piiritletud erandid". Vt näiteks Coolidge *vs.* New Hampshire, 403 U.S. 443, 454–55 (1971); *G.M.* Leasing Corp. *vs.* Ühendriigid, 429 U.S. 338, 352–53, 358 (1977).

([181]) City of Ontario, Cal. *vs.* Quon, 130 S. Ct. 2619, 2630 (2010).

([182]) PCLOB, Sec. 215 Report, lk 107, viide kohtulahendile Maryland *vs.* King, 133 S. Ct. 1958, 1970 (2013).

([183]) PCLOB, Sec. 215 Report, lk 107, viide kohtulahendile Samson *vs.* California, 547 U.S. 843, 848 (2006).

([184]) City of Ontario, Cal. *vs.* Quon, 130 S. Ct. 2619, 2630 (2010), 2627.

([185]) Vt näiteks Ühendriigid *vs* Wilson, 540 F.2d 1100 (D.C. Cir. 1976).

([186]) Vt Roman Zakharov *vs* Venemaa, 4. detsembri 2015. aasta otsus (suurkoda) kohtuasjas nr 47143/06, punkt 269, mille kohaselt „nõue näidata sideteenuse pakkujale sidevahendite pealtkuulamise luba, et saada ligipääs isiku teabevahetusele, on üks olulistest kaitsemehhanismidest õiguskaitseasutuste kuritarvituste eest, mis tagab, et kõigil pealtkuulamisjuhtudel on olemas nõuetekohane luba."

([187]) Justiitsministeeriumi kinnitused (VII lisa), lk 4 koos edasiviidetega.

([188]) Justiitsministeeriumi kinnitused (VII lisa), märkus 2.

([189]) Komisjonile laekunud teabe kohaselt ja jättes kõrvale ELi-USA andmekaitseraamistiku Privacy Shield alusel toimuva andmeedastuse seisukohalt tõenäoliselt ebaolulised erivaldkonnad (nt tervisekindlustuspettuse, laste kuritarvitamise ja keelatud ainetega seotud juhtumite uurimine), seondub see eelkõige teatavate seaduse Electronic Communications Privacy Act (ECPA) volitusnormidega, täpsemalt kasutajainfo (18 U.S.C. § 2703(c)(1), (2)) ja üle 180 päeva vanuste e-kirjade sisu väljanõudmisega (18 U.S.C. § 2703(b)). Viimasel juhul tuleb asjaomast isikut siiski teavitada ning tal tekib seega võimalus taotlus kohtus vaidlustada. Vt ka justiitsministeeriumi ülevaade *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Ch. 3: The Stored Communications Act*, lk 115–138.

([190]) USA valitsuse kinnituste kohaselt võivad haldusorganite teabenõuete saajad need kohtus vaidlustada ebamõistlikkuse, st ülemäärasuse, ahistavuse või koormavuse alusel. Vt justiitsministeeriumi kinnitused (VII lisa), lk 2.

(129) Sama kehtib haldusorganite teabenõuetele, mis esitatakse avalikes huvides. Lisaks on USA valitsuse kinnitustes märgitud, et kehtivad ka sarnased sisulised piirangud, mille kohaselt asutused võivad taotleda juurdepääsu üksnes teabele, mis on seotud nende võimkonda kuuluvate küsimustega, ning peavad järgima seejuures mõistlikkuse põhimõtet.

(130) Lisaks on USA õigusega nähtud üksikisikutele ette mitu õiguskaitsevahendit kaitseks avaliku sektori asutuse või selle ametniku eest juhul, kui sellised asutused töötlevad isikuandmeid. Nimetatud vahendid, mille hulka kuulub haldusmenetluse seadus (Administrative Procedure Act, APA), teabevabaduse seadus (Freedom of Information Act, FOIA) ja elektroonilise side seadus (Electronic Communications Privacy Act, ECPA), on kättesaadavad kõigile isikutele hoolimata nende kodakondsusest ja sõltuvalt kohaldatavatest tingimustest.

(131) Üldiselt, vastavalt haldusmenetluse seaduse ([191]) sätetele kohtuliku läbivaatamise kohta, on „igal isikul, kelle õigusi on rikutud ametkonna tegevusega või keda on negatiivselt mõjutanud või kahjustanud ametkonna tegevus“ õigus pöörduda kohtusse ([192]). See hõlmab võimalust taotleda kohtult, et „tunnistatakse ebaseaduslikuks ja jäetakse arvesse võtmata organi tegevus, uurimistulemused ja järeldused, mis leitakse olevat [—] meelevaldsed, suvalised või põhinevat kaalutusõiguse kuritarvitamisel või mis pole muul viisil seadusega kooskõlas“ ([193]).

(132) Täpsemalt on elektroonilise side seaduse II jaotisega ([194]) kehtestatud eraelu puutumatuse õiguste süsteem, mis reguleerib õiguskaitse juurdepääsu kolmandatest isikutest teenusepakkujate poolt säilitavate telefonikõnede, vestluste või elektroonilise teabevahetuse sisule ([195]). See kriminaliseerib ebaseadusliku (st ilma kohtu loata või muul viisil lubatud) juurdepääsu sellisele teabevahetusele ja annab puudutatud isikule võimaluse esitada tsiviilhagi USA föderaalkohtule tegeliku ja karistusliku iseloomuga kahju eest, samuti õiglase hüvitise või tuvastushagi nimetatud ebaseaduslikud teod tahtlikult toime pannud valitsusametniku vastu või Ameerika Ühendriikide vastu.

(133) Samuti on vastavalt teabevahetuse seaduse (5 U.S.C. § 552) sätetele igal isikul õigus saada juurdepääs föderaalasutuste registritele ja kui halduslikud õiguskaitsevahendid on ammendunud, selle õiguse kasutamiseks kohtu kaudu, välja arvatud juhul, kui nimetatud registrid on kaitstud avalikustamise eest erandiga või õiguskorra tagamisega seonduva keeluga ([196]).

---

([191]) 5 U.S.C. § 702.

([192]) Üldiselt kohaldatakse kohtulikku läbivaatamist ainult asutuse „lõplikule“ tegevusele ja mitte selle „ettevalmistavale, menetluslikule ega vahepealsele“ tegevusele. Vt 5 U.S.C. § 704.

([193]) 5 U.S.C. § 706 (2)(A).

([194]) 18 U.S.C. §§ 2701–2712.

([195]) Elektroonilise side seadus kaitseb teabevahetust, mille sisu säilitavad kahte selgelt määratletud liiki võrguteenuse osutajad ja täpsemalt teenuseosutajad, kes pakuvad: i) elektroonilise side teenuseid, näiteks telefoni- või meiliside, ii) kaugandmetöötlusteenuseid nagu andmesalvestus või -töötlus.

([196]) Need erandid on aga piiratud. Näiteks on 5 U.S.C. § 552 (b)(7) kohaselt teabevahetuse seadusest tulenevad õigused välistatud „õiguskaitsega seonduvate andmete või teabe korral, ent ainult selles ulatuses, milles nimetatud õiguskaitsega seonduvate andmete või teabe esitamine A) võib põhjendatud eelduse kohaselt õiguskaitset häirida, B) jätaks isiku ilma õigusest õiglasele kohtumenetlusele või sõltumatule kohtumõistmisele, C) võib põhjendatud eelduse kohaselt kujutada endast põhjendamatut eraellu sekkumist, D) võib põhjendatud eelduse kohaselt avalikustada konfidentsiaalse allika, sealhulgas riikliku, kohaliku või välismaise organi või ametiasutuse või eraõigusliku asutuse, kes on andnud konfidentsiaalset teavet, ja juhul kui andmed või teabe on kogunud kriminaalõigust jõustav asutus kriminaalmenetluse raames või amet, mis viib seadusega kooskõlas läbi juurdlust seoses riikliku julgeolekuga, konfidentsiaalsest allikast saadud teabe, E) avalikustaks õiguskaitseasutuste uurimise või süüdistuste esitamise tehnikad ja menetlused või õiguskaitseasutuste uurimise või süüdistuste esitamise juhised, kui selline avalikustamine võiks põhjendatud eelduse kohaselt tuua kaasa seaduse täimisest kõrvalehoidmise, või F) võib põhjendatud eelduse kohaselt seada ohtu mis tahes üksikisiku elu või füüsilise turvalisuse.“ Samuti „[k]ui esitatakse taotlus juurdepääsuks andmetele [mille esitamine võib põhjendatud eelduse kohaselt õiguskaitset häirida] ja – A) uurimine või süüdistuse esitamine hõlmab võimalikku kriminaalõiguse rikkumist ning B) on alust arvata, et i) uurimise või süüdistuse esitamise objekt ei ole menetlusest teadlik ja ii) andmete avalikustamine võib põhjendatud eelduse kohaselt õiguskaitset häirida, võib amet ainult selle aja kestel, kui antud asjaolu eksisteerib, andmetele selle jao nõudeid mitte kohaldada.“ (5 U.S.C. § 552 (c)(1)).

(134) Lisaks sellele võimaldavad veel mitu õigusakti üksikisikutel esitada hagi USA avaliku sektori asutuse või ametniku vastu, näiteks pealtkuulamisseadus (Wiretap Act), ([197]) arvutipettuste ja sellealase kuritarvitamise seadus (Computer Fraud and Abuse Act), ([198]) föderaalne õigusvastaselt tekitatud kahju hüvitamise seadus (Federal Torts Claim Act), ([199]) finantsandmetega seotud eraelu puutumatuse seadus (Right to Financial Privacy Act) ([200]) ja õiglase krediidiinfo seadus (Fair Credit Reporting Act) ([201]).

(135) Seetõttu järeldab komisjon, et Ameerika Ühendriikides on olemas eeskirjad, mille ülesandeks on piirata selliste isikute põhiõiguste riivamist õiguskaitse ([202]) või avaliku huvi eesmärgil, kelle isikuandmeid edastatakse liidust Ameerika Ühendriikidesse, piiratakse rangelt sellega, mis on vajalik asjaomase seadusliku eesmärgi saavutamiseks, ning millega tagatakse tõhus õiguskaitse selliste riive vastu.

## 4. KAITSETASEME PIISAVUS ELI-USA ANDMEKAITSERAAMISTIKU PRIVACY SHIELD RAAMES

(136) Neid järeldusi arvestades leiab komisjon, et Ameerika Ühendriigid tagavad ELi-USA andmekaitseraamistiku Privacy Shield alusel piisava kaitsetaseme isikuandmetele, mis edastatakse liidust põhimõtete järgimist kinnitanud organisatsioonidele Ameerika Ühendriikides.

(137) Eelkõige leiab komisjon, et USA kaubandusministeeriumi avaldatud põhimõtted tervikuna tagavad isikuandmete kaitse sisuliselt samaväärsel tasemel, nagu on tagatud direktiiviga 95/46/EÜ kehtestatud aluspõhimõtetega.

(138) Põhimõtete tõhus rakendamine on tagatud ka läbipaistvuskohustustega ning andmekaitseraamistiku Privacy Shield haldamisega kaubandusministeeriumi poolt.

(139) Lisaks leiab komisjon, et andmekaitseraamistiku Privacy Shield jaoks ette nähtud seire- ja kaebuste käsitlemise mehhanismid tervikuna võimaldavad praktikas tuvastada põhimõtete rikkumisi raamistiku Privacy Shield alusel tegutsevates organisatsioonides ja nende eest karistada ning pakuvad andmesubjektile õiguskaitsevahendeid temaga seotud isikuandmetele juurdepääsu tagamiseks ning lõpuks nimetatud andmete parandamiseks või kustutamiseks.

(140) Lisaks leiab komisjon USA õigussüsteemi kohta saada oleva teabe, sealhulgas USA valitsuse kinnituste ja kohustuste põhjal, et selliste isikute põhiõiguste riivamine Ameerika Ühendriikides riikliku julgeoleku, õiguskaitse või muu avaliku huvi eesmärgil, kelle isikuandmeid edastatakse liidust Ameerika Ühendriikidesse, ja põhimõtete järgimist kinnitanud organisatsioonidele sellest tulenevalt kehtivad piirangud eraelu puutumatuse põhimõtete järgimisel, piirduvad asjaomase seadusliku eesmärgi saavutamiseks rangelt vajalikuga ning tagatud on tõhus õiguskaitse selliste riive vastu.

---

([197]) 18 U.S.C. §§ 2510 et seq. Pealtkuulamisseaduse (18 U.S.C. § 2520) kohaselt võib isik, kelle telefonikõnesid, vestlusi või elektroonilist teabevahetust jälgitakse, avalikustatakse või tahtlikult kasutatakse, esitada tsiviilhagi seoses pealtkuulamisseaduse rikkumisega, sealhulgas teatud asjaoludel ühe konkreetse valitsusametniku või Ameerika Ühendriikide vastu. Seoses suunamis- ja muude kui sisuandmete kogumise (näiteks IP aadress, meilide saaja ja saatja aadress) kohta vt ka väljamineva ja sissetuleva side jälgimisseadmete kohta käivaid peatükke peatükis 18 (18 U.S.C. §§ 3121-3127 ja tsiviilmenetlus § 2707).

([198]) 18 U.S.C. § 1030. Arvutipettuste ja sellealase kuritarvitamise seaduse kohaselt võib isik esitada hagi ükskõik millise isiku vastu seoses tahtliku volitamata juurdepääsuga (või volitusi ületava juurdepääsuga) andmete saamiseks finantsasutuselt, USA valitsuse arvutisüsteemist või muust konkreetsest arvutist, sealhulgas teatud asjaoludel ühe konkreetse valitsusametniku vastu.

([199]) 28 U.S.C. §§ 2671 et seq. Föderaalse õigusvastaselt tekitatud kahju hüvitamise seaduse kohaselt võib isik esitada teatud tingimustel hagi Ameerika Ühendriikide vastu seoses „mis tahes valitsusametniku hoolimatu või süülise teo või tegevusetuse tõttu, kui ta tegutseb oma tööülesannete või ametikohustuste raames".

([200]) 12 U.S.C. §§ 3401 et seq. Finantsandmetega seotud eraelu puutumatuse seaduse kohaselt võib isik esitada teatud tingimustel hagi Ameerika Ühendriikide vastu seoses kaitstud finantsandmete saamise või avalikustamisega nimetatud seadusega vastuolus. Valitsuse juurdepääs kaitstud finantsandmetele on üldiselt keelatud, välja arvatud juhul, kui valitsus kohaldab taotluse suhtes seaduslikku ettekirjutust või läbiotsimismäärust või piiratud juhtudel ametlikku kirjalikku taotlust ning isikut, kelle kohta käivat teavet taotletakse, teavitatakse sellisest taotlusest.

([201]) 15 U.S.C. §§ 1681-1681x. Õiglase krediidiinfo seaduse kohaselt võib isik esitada hagi mis tahes isiku vastu, kes ei ole täitnud tarbijakrediidi aruannete kogumisele, edasijagamisele ja kasutamisele kehtivaid nõudeid (eriti seoses seadusliku loa nõudega), või teatud asjaoludel valitsusasutuse vastu.

([202]) Euroopa Kohus on tunnistanud, et õiguskaitse kujutab endast õigustatud poliitilist eesmärki. Vt liidetud kohtuasjad C-293/12 ja C-594/12: Digital Rights Ireland ja teised, EU:C:2014:238, punkt 42; Vt ka Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 8 lõige 2 ja Euroopa Inimõiguste Kohtu otsus kohtuasjas Weber ja Saravia *vs* Saksamaa, 54934/00, punkt 104.

(141) Komisjon järeldab, et see on kooskõlas direktiivi 95/46/EÜ artikli 25 nõuetega, mida tõlgendatakse koostoimes Euroopa Liidu põhiõiguste hartaga, nagu Euroopa Kohus on selgitanud eelkõige kohtuasja Schrems otsuses.

## 5. **ANDMEKAITSEASUTUSTE (DPADE) TEGEVUS JA TEABE EDASTAMINE KOMISJONILE**

(142) Kohtuasjas Schrems tehtud otsuses selgitas Euroopa Kohus, et komisjonil puudub pädevus piirata liikmesriigi DPAde volitusi, mis neil on tulenevalt direktiivi 95/46/EÜ artiklist 28 (sealhulgas õigus peatada andmeedastus), kui isik selle sätte alusel esitatud avalduses seab kahtluse alla selle, kas komisjoni piisavusotsus on kooskõlas eraelu puutumatuse ja andmekaitse põhiõigustega ([203]).

(143) Andmekaitseraamistiku Privacy Shield toimimise tõhusa järelevalve huvides peaksid liikmesriigid teavitama komisjoni DPAde sellealastest meetmetest.

(144) Euroopa Kohus leidis lisaks sellele, et vastavalt direktiivi 95/46/EÜ artikli 25 lõike 6 teisele lõigule peavad liikmesriigid ja nende organid võtma liidu institutsioonide aktid järgimiseks vajalikud meetmed, kuna üldjuhul eeldatakse nende õiguspärasust ja need tekitavad seega õiguslikke tagajärgi seni, kuni neid ei ole tagasi võetud, tühistamishagi menetlemise tulemusena tühistatud ega eelotsusemenetluse tulemusel või õigusvastasuse väite alusel kehtetuks tunnistatud. Seega on direktiivi 95/46/EÜ artikli 25 lõike 6 alusel vastu võetud komisjoni piisavusotsus siduv kõikide otsuse adressaadiks olevate liikmesriikide organitele, sealhulgas sõltumatutele järelevalveasutustele ([204]). Kui selline asutus on saanud kaebuse, milles seatakse kahtluse alla komisjoni piisavusotsuse kooskõla eraelu puutumatuse ja andmekaitse põhiõigustega ning ta leiab esitatud vastuväited olevat hästi põhjendatud, peab liikmesriigi õigusega olema ette nähtud õiguskaitsevahend, mis võimaldab tal edastada need vastuväited siseriiklikule kohtule, kes kahtluste korral peab menetluse peatama ja esitama eelotsusetaotluse Euroopa Kohtule ([205]).

## 6. **PIISAVUSOTSUSE KORRAPÄRANE LÄBIVAATAMINE**

(145) Kuna USA õiguskorrast tulenev kaitsetase võib muutuda, kontrollib komisjon pärast käesoleva otsuse vastuvõtmist korrapäraselt, kas järeldused ELi-USA andmekaitseraamistiku Privacy Shield raames Ameerika Ühendriikide poolt tagatava kaitse piisava taseme kohta on endiselt faktiliselt ja õiguslikult põhjendatud. Niisugune kontrollimine on igal juhul nõutav, kui komisjonile laekunud teave tekitab kõnealuse küsimuse suhtes põhjendatud kahtluse ([206]).

(146) Seepärast jälgib komisjon pidevalt ELi-USA andmekaitseraamistikuga Privacy Shield loodud isikuandmete edastamise üldraamistikku ning käesolevale otsusele lisatud dokumentides sisalduvate kinnituste ja kohustuste täitmist USA ametiasutuste poolt. Selle protsessi hõlbustamiseks on USA andnud lubaduse teavitada komisjoni olulistest raamistiku Privacy Shield suhtes asjakohastest arengusuundadest USA õiguses seoses andmekaitsega ning piirangute ja kaitsemehhanismidega, mida kohaldatakse avaliku sektori asutuste poolse isikuandmetele juurdepääsu suhtes. Lisaks vaadatakse käesolev otsus igal aastal ühiselt läbi ning see läbivaatamine hõlmab ELi-USA andmekaitseraamistiku Privacy Shield toimimise kõiki aspekte, sealhulgas riikliku julgeoleku ja õiguskaitsega seotud erandite tegemist põhimõtetest. Peale selle, kuna piisavusotsust võivad mõjutada ka õiguslikud arengusuunad liidu seadusandluses, hindab komisjon raamistikuga Privacy Shield antava kaitse taset pärast seda, kui on hakatud kohaldama isikuandmete kaitse üldmäärust.

(147) I, II ja VI lisas osutatud iga-aastase ühise läbivaatamise tegemiseks kohtub komisjon kaubandusministeeriumi ja FTC-ga, kellega on vajaduse korral kaasas teiste andmekaitseraamistiku Privacy Shield rakendamises osalevate ministeeriumite ja asutuste esindajad ning riikliku julgeolekuga seotud küsimuste puhul ODNI, luureühenduse teiste liikmete ja ombudsmani esindajad. See kohtumine on osalemiseks avatud ka ELi andmekaitseasutustele ja artikli 29 kohase töörühma esindajatele.

([203]) Schrems, punktid 40 jj, 101–103.
([204]) Schrems, punktid 51, 52 ja 62.
([205]) Schrems, punkt 65.
([206]) Schrems, punkt 76.

(148) Iga-aastase ühise läbivaatamise käigus palub komisjon kaubandusministeeriumil esitada igakülgse teabe ELi-USA andmekaitseraamistiku Privacy Shield toimimise kõikide asjakohaste aspektide kohta, sealhulgas andmekaitseasutustest kaubandusministeeriumile edastatud esildiste ja ametikohaste vastavuskontrollide tulemuste kohta. Lisaks palub komisjon selgitusi ELi-USA andmekaitseraamistikuga Privacy Shield ja selle toimimisega seotud selliste küsimuste ja teemade kohta, mis tulenevad olemasolevast teabest, sealhulgas seaduse USA FREEDOM Act alusel lubatud läbipaistvusaruannetest, USA riiklike luureasutuste avalikest teadetest, DPAdelt, eraelu puutumatusega tegelevatelt rühmadelt, meediast ja mis tahes muudest allikatest. Peale selle peaksid liikmesriigid komisjoni sellealasele tööle kaasaaitamiseks teavitama komisjoni juhtumitest, kus Ameerika Ühendriikides põhimõtete järgimise tagamise eest vastutavate asutuste tegevus ei taga vastavust või kui on mis tahes andmeid, et riikliku julgeoleku või kuritegevuse ennetamise, uurimise, tuvastamise või kriminaalasjade menetlemisega tegelevate USA avaliku sektori asutuste tegevus ei taga nõutavat kaitsetaset.

(149) Iga-aastase ühise läbivaatamise alusel koostab komisjon avaliku aruande Euroopa Parlamendile ja nõukogule.

## 7. **PIISAVUSOTSUSE KEHTIVUSE PEATAMINE**

(150) Kui komisjon järeldab kontrollide või muu saadaoleva teabe alusel, et raamistikuga Privacy Shield tagatud kaitse taset ei saa enam pidada sisuliselt samaväärseks liidus oleva kaitse tasemega või kui on selgeid märke võimalikest probleemidest Ameerika Ühendriikides eraelu puutumatuse põhimõtete järgimisel või kui riikliku julgeoleku või kuritegevuse ennetamise, uurimise, tuvastamise või kriminaalasjade menetlemisega tegelevate USA avaliku sektori asutuste tegevus ei taga nõutavat kaitsetaset, teavitab ta sellest kaubandusministeeriumi ja palub kiiresti võtta sobivad meetmed võimaliku eraelu puutumatuse põhimõtetele mittevastavuse kõrvaldamiseks kindlaksmääratud mõistliku tähtaja jooksul. Kui USA ametiasutused ei ole kindlaksmääratud aja möödumisel rahuldavalt tõendanud, et ELi-USA andmekaitseraamistik Privacy Shield tagab endiselt tõhusa nõuete täitmise ja piisava kaitsetaseme, algatab komisjon menetluse käesoleva otsuse osaliseks või täielikuks peatamiseks või kehtetuks tunnistamiseks ([207]). Alternatiivina võib komisjon teha ettepaneku otsust muuta, piirates piisavusotsuse kohaldamisala ainult sellise andmeedastusega, millele kehtivad lisatingimused.

(151) Komisjon algatab peatamise või kehtetuks tunnistamise eelkõige juhul, kui:

a) on märke, et USA avaliku sektori asutused ei täida käesolevale otsusele lisatud dokumentides sisalduvaid kinnitusi ega kohustusi, sealhulgas seoses tingimuste ja piirangutega, mille alusel pääsevad USA avaliku sektori asutused juurde ELi-USA andmekaitseraamistiku Privacy Shield alusel edastatud isikuandmetele ja kasutavad neid riikliku julgeoleku, õiguskaitse ja muu avaliku huvi eesmärgil;

b) ELi andmesubjektide kaebusi ei lahendata tõhusalt; sellega seoses võtab komisjon arvesse kõiki asjaolusid, mis mõjutavad ELi andmesubjektide võimalust oma õigusi kasutada, sealhulgas eelkõige põhimõtete järgimist kinnitanud USA ettevõtete vabatahtlikku kohustust teha koostööd DPAdega ja järgida nende nõuandeid; või

c) Privacy Shieldi ombudsman ei vasta õigeaegselt ega nõuetekohaselt ELi andmesubjektide taotlustele.

(152) Komisjon kaalub käesoleva otsuse muutmise, kehtivuse peatamise või kehtetuks tunnistamise menetluse algatamist ka juhul, kui ELi-USA raamistiku Privacy Shield toimimise iga-aastase ühise läbivaatamise puhul või muudes olukordades ei anna kaubandusministeerium, teised raamistiku Privacy Shield rakendamisega tegelevad ministeeriumid või asutused või siis riikliku julgeolekuga seonduvates küsimustes USA luureühenduse esindajad

([207]) Alates isikuandmete kaitse üldmääruse kohaldamise alguskuupäevast kasutab komisjon enda õigust võtta nõuetekohaselt põhjendatud ja kiireloomulistel juhtudel vastu rakendusakt, millega peatatakse käesoleva otsuse kehtivus ning mida kohaldatakse viivitamata ilma selle eelnevat esitamist asjakohasele komiteemenetluse komiteele ja mis on jõus kuni kuus kuud.

või ombudsman teavet või selgitusi, mis on vajalikud, hindamaks eraelu puutumatuse põhimõtetele vastavust, kaebuste menetlemise tulemuslikkust või nõutava kaitsetaseme vähenemist USA riiklike luureasutuste tegevuse tagajärjel, eelkõige tulenevalt isikuandmete kogumisest ja neile juurdepääsust, mis ei ole rangelt vajalik ega proportsionaalne. Sellega seoses võtab komisjon arvesse võimalusi saada asjakohast teavet muudest allikatest, sealhulgas põhimõtete järgimist kinnitanud USA ettevõtete aruannetest, mida lubab seadus USA FREEDOM Act.

(153) Direktiivi 95/46/EÜ artikli 29 kohaselt moodustatud töörühm üksikisikute kaitseks seoses isikuandmete töötlemisega avaldas oma arvamuse ELi-USA andmekaitseraamistiku Privacy Shield kohta ([208]) ning seda arvamust on arvesse võetud käesoleva otsuse koostamisel.

(154) Euroopa Parlament võttis vastu resolutsiooni Atlandi-üleste andmevoogude kohta ([209]).

(155) Käesoleva otsusega ettenähtud meetmed on kooskõlas direktiivi 95/46/EÜ artikli 31 lõike 1 alusel loodud komitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

*Artikkel 1*

1. Ameerika Ühendriigid tagavad ELi-USA andmekaitseraamistiku Privacy Shield alusel direktiivi 95/46/EÜ artikli 25 lõike 2 tähenduses piisava kaitsetaseme isikuandmetele, mis edastatakse liidust Ameerika Ühendriikides asuvatele organisatsioonidele.

2. ELi-USA andmekaitseraamistik Privacy Shield koosneb 7. juulil 2016 Ameerika Ühendriikide kaubandusministeeriumi poolt välja antud põhimõtetest, mis on esitatud II lisas, ning ametlikest kinnitustest ja kohustustest, mis on esitatud I ja III–VII lisas loetletud dokumentides.

3. Lõike 1 kohaldamisel edastatakse isikuandmed ELi-USA andmekaitseraamistiku Privacy Shield raames juhul, kui need edastatakse liidust Ameerika Ühendriikides asuvatele organisatsioonidele, mis kuuluvad Privacy Shieldi nimekirja, mida haldab ja mille teeb avalikkusele kättesaadavaks Ameerika Ühendriikide kaubandusministeerium kooskõlas II lisas esitatud põhimõtete I ja II jaoga.

*Artikkel 2*

Käesolev otsus ei mõjuta direktiivi 95/46/EÜ muude sätete kui artikli 25 lõike 1 (millega reguleeritakse isikuandmete töötlemist liikmesriikides), eriti artikli 4 kohaldamist.

*Artikkel 3*

Kui tulenevalt sellest, et liikmesriikide pädevad ametiasutused kasutavad direktiivi 95/46/EÜ artikli 28 lõike 3 kohaseid volitusi, katkestatakse kooskõlas II lisas esitatud põhimõtete I ja III jaoga ajutiselt või alaliselt andmevoogude edastamine Privacy Shieldi nimekirja kuuluvale Ameerika Ühendriikide organisatsioonile, et tagada üksikisikute kaitse seoses nende isikuandmete töötlemisega, teavitab asjaomane liikmesriik sellest viivitamatult komisjoni.

*Artikkel 4*

1. Komisjon jälgib pidevalt ELi-USA andmekaitseraamistiku Privacy Shield toimimist, et hinnata, kas Ameerika Ühendriigid tagavad jätkuvalt piisava kaitsetaseme isikuandmetele, mis edastatakse selle alusel liidust Ameerika Ühendriikides asuvatele organisatsioonidele.

([208]) Arvamus 01/2016 ELi-USA andmekaitseraamistiku Privacy Shield piisavusotsuse eelnõu kohta, vastu võetud 13. aprill 2016.
([209]) Euroopa Parlamendi 26. mai 2016. aasta resolutsioon Atlandi-üleste andmevoogude kohta ((2016/2727(RSP)).

2. Liikmesriigid ja komisjon teavitavad üksteist juhul, kui selgub, et II lisas esitatud põhimõtete täitmise tagamiseks seaduslikku volitust omavad Ameerika Ühendriikide ametiasutused ei taga tõhusaid avastamis- ja kontrollimehhanisme, mis võimaldavad põhimõtete rikkumisi praktikas tuvastada ja nende eest karistada.

3. Liikmesriigid ja komisjon teavitavad üksteist kõikidest märkidest, et riikliku julgeoleku, õiguskaitse või muude avalike huvide eest vastutavate USA ametiasutuste poolsed üksikisikute isikuandmete kaitse õiguse riived ületavad rangelt vajalikku ja/või selliste riivete vastu puudub tõhus õiguskaitse.

4. Komisjon hindab ühe aasta jooksul alates käesoleva otsuse liikmesriikidele teatavakstegemisest ning edaspidi igal aastal artikli 1 lõikes 1 sätestatud järeldust kogu olemasoleva teabe, sealhulgas I, II ja VI lisas osutatud iga-aastase ühise läbivaatamise käigus saadud teabe alusel.

5. Komisjoni teavitab kõikidest olulistest järeldustest direktiivi 95/46/EÜ artikliga 31 asutatud komiteed.

6. Komisjon esitab direktiivi 95/46/EÜ artikli 31 lõikes 2 osutatud korras meetmete eelnõu käesoleva otsuse kehtivuse peatamiseks, muutmiseks või kehtetuks tunnistamiseks või selle kohaldamisala piiramiseks muu hulgas juhul, kui on märke, et:

— USA avaliku sektori asutused ei täida käesolevale otsusele lisatud dokumentides sisalduvaid kinnitusi ja kohustusi, sealhulgas seoses tingimuste ja piirangutega, mille alusel pääsevad USA avaliku sektori asutused juurde ELi-USA andmekaitseraamistiku Privacy Shield alusel edastatud isikuandmetele ja kasutavad neid õiguskaitse, riikliku julgeoleku ja muu avaliku huvi eesmärgil;

— ELi andmesubjektide kaebusi ei lahendata tõhusalt ja probleem on süsteemne; või

— Privacy Shieldi ombudsman jätab süstemaatiliselt andmata õigeaegsed ja nõuetekohased vastused ELi andmesubjektide taotlustele, nagu on nõutud III lisa jaos 4(e).

Komisjon esitab nimetatud meetmete eelnõu ka juhul, kui Ameerika Ühendriikides ELi-USA andmekaitseraamistiku Privacy Shield toimimise eest vastutavad organid ei tee koostööd, mis on komisjonile vajalik artikli 1 lõikes 1 sätestatud järelduse kehtivuse kindlakstegemiseks.

*Artikkel 5*

Liikmesriigid võtavad kõik käesoleva otsuse järgimiseks vajalikud meetmed.

*Artikkel 6*

Käesolev otsus on adresseeritud liikmesriikidele.

Brüssel, 12. juuli 2016

*Komisjoni nimel*
*komisjoni liige*
Věra JOUROVÁ

*I LISA*

**USA kaubandusministri Penny Pritzkeri kiri**

7. juuli 2016

Pr Věra Jourová
Õigus- ja tarbijaküsimuste ning soolise võrdõiguslikkuse volinik
European Commission
Rue de la Loi/Westraat 200
1049 Brussels
Belgium

Lugupeetud volinik Jourová

Ameerika Ühendriikide nimel on mul hea meel käesolevaga edastada ELi-USA andmekaitseraamistiku Privacy Shield materjalide pakett, mis on valminud kahe aasta jooksul meie meeskondade viljakate arutelude tulemusena. Kõnealune pakett koos muude, komisjonile avalikest allikatest kättesaadavate materjalidega, on väga tugev alus komisjoni uue piisavustagatise jaoks ([1]).

Peame mõlemad olema uhked raamistiku täiustumise üle. Andmekaitseraamistik Privacy Shield lähtub mõlemal pool Atlandi ookeani tugeva üksmeelse toetuse saanud põhimõtetest, mille rakendamist oleme nüüd tõhustanud. Oma ühise töö läbi on meil reaalne võimalus parandada eraelu puutumatust kogu maailmas.

Andmekaitseraamistiku Privacy Shield pakett sisaldab Privacy Shield põhimõtteid ja 1. lisana ka kirja kõnealust programmi administreerivalt kaubandusministeeriumi väliskaubandusametilt (ITA), milles kirjeldatakse kohustusi, mille meie ministeerium on võtnud tagamaks, et andmekaitseraamistik Privacy Shield toimiks tõhusalt. Pakett sisaldab ka 2. lisa, milles on esitatud muud kaubandusministeeriumi kohustused seoses uue vahekohtumudeliga, mis on kasutatav andmekaitseraamistiku Privacy Shield raames.

Olen teinud oma töötajatele ülesandeks rakendada kõik vajalikud ressursid andmekaitseraamistiku Privacy Shield viivitamatult ja täielikuks elluviimiseks ning 1. ja 2. lisas esitatud kohustuste õigeaegse täitmise tagamiseks.

Andmekaitseraamistiku Privacy Shield pakett sisaldab ka muid USA asutuste koostatud dokumente, nimelt:

— Föderaalse kaubanduskomisjoni (Federal Trade Commission – FTC) kiri, milles kirjeldatakse tema tegevust andmekaitseraamistiku Privacy Shield täitmise tagamisel;

— transpordiministeeriumi kiri, milles kirjeldatakse tema tegevust andmekaitseraamistiku Privacy Shield täitmise tagamisel;

— USA riikliku luurejuhi ameti (Office of the Director of National Intelligence, ODNI) kaks kirja kaitsemeetmete ja piirangute kohta, mida kohaldatakse USA riiklike julgeolekuasutuste suhtes;

— välisministeeriumi kiri koos memorandumiga, milles kirjeldatakse välisministeeriumi võetud kohustust luua uus andmekaitseraamistiku Privacy Shield ombudsmani ametikoht USA signaaliluuretegevust puudutavate järelepärimiste jaoks ja

— justiitsministeeriumi kiri kaitsemeetmete ja piirangute kohta, mis on kehtestatud USA valitsuse juurdepääsule õiguskaitse ja avalikku huvi silmas pidades.

Võite olla kindel, et Ameerika Ühendriigid suhtuvad nimetatud kohustustesse tõsiselt.

([1]) Juhul kui komisjoni piisavusotsus ELi-USA andmekaitseraamistiku Privacy Shield poolt osutatava kaitse kohta rakendub ka Islandi, Norra ja Liechtensteini suhtes, katab andmekaitseraamistiku Privacy Shield pakett nii Euroopa Liitu kui ka kolme kõnealust riiki.

30 päeva jooksul pärast lõpliku heakskiidu saamist piisavuse kohta saadetakse kogu andmekaitseraamistiku Privacy Shield pakett ametlikule teatajale *Federal Register* avaldamiseks.

Soovime jätkata teiega koostööd andmekaitseraamistiku Privacy Shield rakendamisel ja selle protsessi järgmise etapi ühisel käivitamisel.

Lugupidamisega

Penny Pritzker

*1. lisa*

**Kiri aseriigisekretäri kohusetäitjalt rahvusvahelise kaubanduse alal Ken Hyattilt**

Austatud Věra Jourová
Õigus- ja tarbijaküsimuste ning soolise võrdõiguslikkuse volinik
European Commission
Rue de la Loi/Westraat 200
1049 Brussels
Belgium

Lugupeetud volinik Jourová

Väliskaubandusameti nimel on mul hea meel kirjeldada täiustatud isikuandmete kaitset, mida ELi-USA andmekaitseraamistik Privacy Shield („Privacy Shield" või „raamistik") pakub, ja kaubandusministeeriumi („ministeerium") võetud kohustusi tagamaks, et Privacy Shield toimiks tõhusalt. Selle ajaloolise ettevõtmise lõpule viimine on suur saavutus eraelu puutumatuse ja äritegevuse huvides mõlemal pool Atlandi ookeani. See annab inimestele ELis kindlustunde, et nende andmed on kaitstud ning et neil on probleemide lahendamiseks olemas õiguskaitsevahendid. See annab turvalisustunde, mis aitab kaasa Atlandi-ülesele majanduse kasvule, tagades et tuhanded Euroopa ja Ameerika ettevõtted võivad jätkata investeerimist ning tegeleda üle meie riigipiiride ulatuva ettevõtlusega. Privacy Shield on valminud enam kui kahe aasta jooksul tehtud tõsise töö ja koostöö tulemusena teiega, meie kolleegid Euroopa Komisjonis („komisjon"). Me loodame koostöö jätkumist komisjoniga, tagamaks et Privacy Shield funktsioneerib nagu ette nähtud.

Oleme koos komisjoniga välja arendanud andmekaitseraamistiku Privacy Shield, mis võimaldab USAs asuvatel organisatsioonidel täita ELi õiguse kohaseid andmekaitse piisavuse nõudeid. Uus raamistik on mitmes olulises aspektis kasulik nii üksikisikutele kui ka ettevõtjatele. Esiteks määratakse selles kindlaks ELi üksikisikute isikuandmete puutumatuse kaitse abinõud. Selle kohaselt peavad USAs asuvad osalevad organisatsioonid välja töötama nõuetekohased puutumatusnormid, tegema avalikult teatavaks, et nad võtavad kohustuse järgida andmekaitseraamistiku Privacy Shield põhimõtteid, nii et selle täitmist saab USA õiguse alusel nõuda, igal aastal ministeeriumile asjaomaste põhimõtete järgimist uuesti kinnitama, võimaldama ELi üksikisikutele tasuta sõltumatut vaidluste lahendamist ning alluma USA föderaalsele kaubanduskomisjonile („FTC") ja transpordiministeeriumile („DOT") või teistele täitevasutustele. Teiseks võimaldab Privacy Shield tuhandetel USAs asuvatel äriühingutel ning Euroopa äriühingute tütarettevõtetel USAs saada Euroopa Liidust isikuandmeid, hõlbustamaks Atlandi-ülest äritegevust toetavate andmete edastamist. Atlandi-ülesed majandussuhted on juba praegu maailmas kõige ulatuslikumad, moodustades poole kogu maailmamajanduse kogutoodangust ja ulatudes kaupade ja teenuste osas ligi miljardi dollarini, toetades miljonite töökohtade olemasolu mõlemal pool Atlandi ookeani. Ettevõtjaid, kes sõltuvad Atlandi-ülestest andmevoogudest, leidub kõikides majandusharudes, sealhulgas nii Fortune'i nimekirja 500 suurima kui ka väikeste ja keskmise suurusega ettevõtete hulgas. Atlandi-ülesed andmevood võimaldavad USA organisatsioonidel töödelda Euroopa üksikisikutele kaupade, teenuste ja töötamisvõimaluste pakkumiseks vajalikke andmeid. Ületades õigusraamistike erinevusi, toetab Privacy Shield eraelu puutumatuse põhimõtteid, mida mõlemad pooled jagavad, edendades kaubandust ja nii Euroopa kui ka Ameerika Ühendriikide majanduslikke eesmärke.

Äriühingu otsus kinnitada asjaomase uue raamistiku põhimõtete järgimist on küll vabatahtlik, ent kui ta on teinud avalikuks oma otsuse järgida andmekaitseraamistiku Privacy Shield põhimõtteid, võib selle kohustuse täitmist USA õiguse alusel nõuda kas föderaalne kaubanduskomisjon või transpordiministeerium, sõltuvalt sellest, kumma pädevusse andmekaitseraamistikuga Privacy Shield ühinenud organisatsioon kuulub.

**Andmekaitseraamistiku Privacy Shield põhimõtteid järgivad täiendused**

Loodav andmekaitseraamistik Privacy Shield tugevdab eraelu puutumatust järgmiselt:

— nõudes, et üksikisikutele antaks teate põhimõtte kohaselt täiendavat teavet, sealhulgas kinnitus selle kohta, et organisatsioon on ühinenud andmekaitseraamistikuga Privacy Shield, kinnitus isiku juurdepääsuõiguse kohta oma isikuandmetele ja teave vaidluste lahendamiseks pädeva asjakohase sõltumatu organi kohta;

— tugevdades andmekaitseraamistikuga Privacy Shield ühinenud organisatsiooni poolt kolmandale isikule, kes on vastutav töötleja, edastatavate isikuandmete kaitset, nõudes et pooled sõlmiksid andmete edastamise kohta lepingu, milles nähakse ette, et asjaomaseid andmeid tohib töödelda ainult piiratud ja konkreetsetel eesmärkidel kooskõlas isiku poolt antud nõusolekuga ning et saaja tagab Privacy Shield põhimõtetes sätestatuga samal tasemel kaitse;

— tugevdades andmekaitseraamistikuga Privacy Shield ühinenud organisatsiooni poolt kolmandale isikule, kes on tema esindaja, edastavate isikuandmete kaitset, nõudes et raamistikuga ühinenud organisatsioon: võtab mõistlikke ja asjakohaseid meetmeid tagamaks, et esindaja töötleb saadud isikuandmeid ka tegelikult viisil, mis on kooskõlas Privacy Shield põhimõtetega, mille järgimise kohustuse organisatsioon on võtnud; võtab volitamatust töötlemisest teada saades mõistlikud ja asjakohased meetmed selle peatamiseks ja heastamiseks ning esitab ministeeriumile viimase nõudmisel kokkuvõtte või koopia kõnealustest esindajaga sõlmitud lepingu eraelu puutumatust käsitlevatest sätetest;

— nähes ette, et andmekaitseraamistikuga Privacy Shield ühinenud organisatsioon on vastutav selliste isikuandmete töötlemise eest, mis on edastatud selles raamistikus ja mille ta seejärel edastab kolmandale isikule, kes tegutseb tema nimel tema esindajana, ning et raamistikuga ühinenud organisatsioon jääb Privacy Shield põhimõtete kohaselt ka siis vastutavaks, kui tema esindaja töötleb asjaomaseid isikuandmeid viisil, mis ei ole kooskõlas nende põhimõtetega, välja arvatud juhul, kui organisatsioon tõestab, et ta ei ole vastutav sündmuse eest, mille tagajärjel kahju tekkis;

— selgitades, et andmekaitseraamistikuga Privacy Shield ühinenud organisatsioonid peavad isikuandmete puhul piirduma ainult nende andmetega, mis on töötlemise eesmärke arvestades asjakohased;

— nõudes, et organisatsioon kinnitaks igal aastal ministeeriumile oma kohustust pidada kinni andmekaitseraamistiku Privacy Shield põhimõtetest selliste andmete suhtes, mille ta raamistikus osaledes sai, juhul kui ta raamistikust lahkub ja soovib kõnealused andmed enda käsutusse jätta;

— nõudes, et seataks sisse sõltumatu kaebuste menetlemise mehhanism, mis on üksikisikutele tasuta;

— nõudes, et organisatsioonid ja nende poolt valitud sõltumatud kaebuste menetlemise mehhanismid reageeriks kiiresti järelepärimistele ja ministeeriumi nõudmistele esitada andmekaitseraamistikuga Privacy Shield seotud teavet;

— nõudes, et organisatsioonid reageeriks viivitamata Privacy Shield põhimõtete järgimist käsitlevatele kaebustele, mille on esitanud ELi liikmesriikide ametiasutused ministeeriumi kaudu; ja

— nõudes, et andmekaitseraamistikuga Privacy Shield ühinenud organisatsioon avalikustaks kõik FTC-le esitatud raamistikuga seotud vastavus- või hindamisaruannete osad, kui FTC või kohus on teinud organisatsiooni suhtes otsuse põhimõtete rikkumise kohta.

**Andmekaitseraamistiku Privacy Shield programmi haldamine ja järelevalve kaubandusministeeriumi poolt**

Ministeerium kinnitab kohustust pidada usaldusväärset nimekirja nende USA organisatsioonide kohta, kes on kinnitanud ministeeriumile, et nad järgivad andmekaitseraamistiku põhimõtteid ja kohustuvad neist kinni pidama („andmekaitseraamistikuga Privacy Shield ühinenute nimekiri“), ning avalikustab selle. Ministeerium hoiab andmekaitseraamistikuga Privacy Shield ühinenute nimekirja ajakohastatuna, eemaldades sealt organisatsioonid, kes raamistikust vabatahtlikult lahkuvad, jätavad andmata iga-aastase kinnituse ministeeriumi poolt kehtestatud korras või kelle suhtes on leitud, et nende tegevus ei ole püsivalt kooskõlas Privacy Shield põhimõtetega.Ministeerium säilitab ja avalikustab ka usaldusväärsed andmed nende USA organisatsioonide kohta, kes on varasemalt ministeeriumile põhimõtete järgimist kinnitanud, ent kes on andmekaitseraamistikuga Privacy Shield ühinenute nimekirjast eemaldatud, sealhulgas nende kohta, kes eemaldati, kuna nad järjepidevalt ei järginud põhimõtteid. Ministeerium toob välja ka põhjuse, mille tõttu organisatsioon nimekirjast eemaldati.

Lisaks kohustub ministeerium tugevdama andmekaitseraamistiku Privacy Shield haldamist ja järelevalvet. Täpsemalt teeb ministeerium järgmist:

Annab andmekaitseraamistiku Privacy Shield veebisaidil täiendavat teavet

— peab andmekaitseraamistikuga Privacy Shield ühinenute nimekirja, samuti ka arvestust nende organisatsioonide kohta, kes varem on kinnitanud Privacy Shield põhimõtete järgimist, ent kellele enam ei ole tagatud andmekaitseraamistiku Privacy Shield soodustused;

— annab nähtaval kohal selgituse selle kohta, et organisatsioonid, kes on eemaldatud andmekaitseraamistikuga Privacy Shield ühinenute nimekirjast, ei saa enam kasutada raamistiku soodustusi, ent peavad sellele vaatamata jätkama Privacy Shield põhimõtete järgimist selliste isikuandmete suhtes, mille nad said ajal, mil nad raamistikus osalesid, niikaua kuni nad neid andmeid säilitavad; ja

— lisab lingid FTC poolt käsitletavatele andmekaitseraamistikuga Privacy Shield seotud juhtumitele, mis on avaldatud FTC veebisaidil.

Kontrollib nende nõuete täitmist, millele vastavust ise kinnitatakse

— kontrollib enne organisatsiooni põhimõtete järgimise kinnituse (või iga-aastase taaskinnituse) lõpule viimist ja organisatsiooni lisamist andmekaitseraamistikuga Privacy Shield ühinenute nimekirja, kas organisatsioon on:

  — esitanud nõutavad kontaktandmed organisatsiooni kohta;

  — kirjeldanud organisatsiooni tegevust seoses EList saadavate isikuandmetega;

  — märkinud ära, millist liiki isikuandmeid tema poolt antud kinnitus hõlmab;

  — kui organisatsioonil on olemas avalik veebisait, lisanud veebiaadressi, millelt leiab organisatsiooni puutumatusnormid ja need on antud veebiaadressil ka kättesaadavad, või kui organisatsioonil ei ole avalikku veebisaiti, on lisanud teabe, kus tema puutumatusnormid on avalikkusele kättesaadavad;

  — lisanud oma asjakohastesse puutumatusnormidesse avalduse, et ta järgib Privacy Shield põhimõtteid ja juhul kui puutumatusnormid on kättesaadavad veebis, siis ka hüperlingi ministeeriumi andmekaitseraamistiku Privacy Shield veebisaidile;

  — on määranud konkreetse organi, millel on pädevus läbi vaadata mis tahes nõudeid organisatsiooni vastu seoses võimalike kõlvatute tavade või pettusega ja puutumatusele kohaldatavate seaduste või normide rikkumisega (ja mis on loetletud Privacy Shield põhimõtetes või tulevases Privacy Shield põhimõtete lisas);

  — kas organisatsioon soovib täita punkti a) alapunktides i) ja iii) sätestatud nõudeid kaebuste menetlemise, täitmise tagamise ja vastutuse põhimõtte kohta, kohustudes sel eesmärgil koostööd tegema asjakohaste ELi andmekaitseasutustega, on osutanud oma kavatsusele teha koostööd andmekaitseasutustega andmekaitseraamistiku Privacy Shield raames läbiviidavates uurimistes ja kaebuste lahendamisel, eriti nende järelpärimistele vastamise kaudu, juhul kui ELi riikide kodanikud on esitanud kaebused otse oma riikide andmekaitseasutustele;

  — on toonud välja kõik eraelu puutumatuse programmid, milles organisatsioon osaleb;

  — on teinud kindlaks meetodi, mille abil toimub Privacy Shield põhimõtete järgimise tagamise kontroll (nt sisemine, kolmas isik);

  — on määratlenud, nii oma kinnitust esitades kui ka oma puutumatusnormides sõltumatu kaebuste menetlemise mehhanismi, mida on võimalik kasutada kaebuste läbivaatamiseks ja lahendamiseks;

  — on lisanud oma puutumatusnormidesse, juhul kui need on veebis kättesaadavad, hüperlingi lahendamata kaebuste uurimiseks ettenähtud sõltumatu kaebuste menetlemise mehhanismi veebisaidile või kaebuse esitamise vormile ja

  — kui organisatsioon on osutanud, et ta soovib saada EList töösuhte kontekstis kasutamiseks töötajate isikuandmeid, avaldanud, et kohustub andmekaitseasutustega koostööd tegema ja nende nõudeid järgides tegutsema selliste kaebuste lahendamisel, mis puudutavad tema tegevust seoses nimetatud andmetega, on edastanud ministeeriumile koopia oma puutumatusnormidest ning viidanud, kus need on asjaomastele töötajatele tutvumiseks kättesaadavad.

— teeb koostöös sõltumatute kaebuste menetlemise mehhanismidega kindlaks, et organisatsioonid on ka tegelikult registreerinud end mehhanismis, millele nad on oma kinnituses viidanud, juhul kui selline registreerimine on nõutav.

Tugevdab kontrolli andmekaitseraamistikuga Privacy Shield ühinenute nimekirjast eemaldatud organisatsioonide üle

— teatab andmekaitseraamistikuga Privacy Shield ühinenute nimekirjast „püsiva mittevastavuse tõttu“ eemaldatud organisatsioonidele, et nad ei tohi hoida enda käsutuses teavet, mis on kogutud asjaomase raamistiku kaudu ja

— saadab küsimustikud organisatsioonidele, kelle esitatud kinnitused on aegunud või kes on vabatahtlikult andmekaitseraamistikust Privacy Shield lahkunud, et teha kindlaks, kas organisatsioon tagastab või kustutab isikuandmed, mille ta raamistikus osalades sai või jätkab nende andmete suhtes Privacy Shield rakendamist ning kas isikuandmed säilitatakse, samuti teeb kindlaks, kellele selles organisatsioonis edaspidi edastada andmekaitseraamistikuga Privacy Shield seotud küsimused.

Osalemise kohta esitatud valeväidete otsimine ja nendega tegelemine

— vaatab läbi nende organisatsioonide puutumatusnormid, kes varem osalesid Privacy Shield programmis, ent on nüüd andmekaitseraamistikuga Privacy Shield ühinenute nimekirjast eemaldatud, et välja selgitada mis tahes valeväited asjaomases programmis osalemise kohta;

— kontrollib regulaarselt, kui organisatsioon: a) loobub programmis Privacy Shield osalemisest, b) ei kinnita uuesti põhimõtete järgimist või c) on eemaldatud andmekaitseraamistikuga Privacy Shield ühinenute hulgast, eriti kui see on toimunud „püsiva mittevastavuse tõttu", kas asjaomane organisatsioon on eemaldanud kõikidest asjakohastest avalikustatud puutumatusnormidest mis tahes viited andmekaitseraamistikule Privacy Shield, mis viitavad, et organisatsioon jätkab aktiivselt andmekaitseraamistikus Privacy Shield osalemist ja et tal on õigus asjaomase programmi soodustusi kasutada. Kui ministeerium teeb kindlaks, et sellised viited ei ole eemaldatud, siis hoiatab ta organisatsiooni, et edastab asja vajadusel asjakohasele asutusele võimalike täitemeetmete võtmiseks, kui organisatsioon jätkuvalt väidab, et ta järgib andmekaitseraamistiku Privacy Shield põhimõtteid. Kui organisatsioon ei eemalda viiteid ega kinnita andmekaitseraamistiku Privacy Shield põhimõtete järgimist, esitab ministeerium omal algatusel asja FTC-le, DOT-le või muule asjakohasele täitevasutusele, ning võtab asjakohastel juhtudel meetmeid andmekaitseraamistikuga Privacy Shield vastavust tõendava tähise kasutusele võtmiseks;

— püüab muul viisil kindlaks teha valeväiteid osalemise kohta andmekaitseraamistikus Privacy Shield ning andmekaitseraamistiku Privacy Shield põhimõtete järgimist tõendava tähise väärkasutamise kohta, sealhulgas teeb otsinguid internetis, et kindlaks teha, kus on nähtavalt esitatud raamistiku põhimõtete järgimist tõendav tähis või millistes puutumatusnormides on raamistikule viidatud;

— tegeleb kohe probleemidega, mille me teeme omal algatusel kindlaks osalemise kohta esitatud valeväidete ja andmekaitseraamistiku Privacy Shield põhimõtete järgimist tõendava tähise väärkasutamise üle tehtava järelevalve käigus, sealhulgas hoiatab organisatsioone, et nad ei esitaks eespool kirjeldatud viisil valeandmeid oma osalemise kohta programmis Privacy Shield;

— võtab muid oma pädevuses olevaid parandusmeetmeid, sealhulgas kasutab õiguskaitsevahendeid, ning edastab asjad FTC-le, DOT-le või muule asjakohasele täitevasutusele ja

— vaatab viivitamata läbi ja tegeleb kaebustega, mis meile laekuvad programmis osalemise valeväidete kohta.

Ministerium vaatab programmis Privacy Shield osalemise kohta esitatud valeväidete tõhusamaks tuvastamiseks ja nende valeväidetega tegelemiseks üle organisatsioonide puutumatusnormid. Eeskätt vaatab ministeerium üle nende organisatsioonide puutumatusnormid, kelle kinnitus on aegunud selle tõttu, et nad ei ole Privacy Shield põhimõtete järgimist uuesti kinnitanud. Niisugusel juhul vaatab ministeerium puutumatusnormid läbi, et kindlaks teha, kas kõnealused organisatsioonid on kõikidest asjakohastest avaldatud puutumatusnormidest eemaldanud kõik viited, mis osutavad, et nad osalevad jätkuvalt aktiivselt andmekaitseraamistikus Privacy Shield. Taoliste ülevaatuste abil teeme me kindlaks organisatsioonid, kes ei ole asjaomaseid viiteid eemaldanud, ning saadame neile Department's Office of General Counsel'i nimel kirja, milles hoiatame võimaliku täitemeetmete eest juhul, kui viiteid ei eemaldata. Ministeerium võtab järelmeetmed, tagamaks et organisatsioonid kas eemaldavad mittekohased viited või kinnitavad uuesti põhimõtete järgimist. Lisaks püüab ministeerium tuvastada niisugused valeväiteid programmis Privacy Shield osalemise kohta, mille on esitanud organisatsioonid, kes ei ole kunagi asjaomases programmis osalenud, ning võtab nende organisatsioonide suhtes samasugused parandusmeetmed.

Viib perioodiliselt omal algatusel läbi vastavuskontrolle ning programmi hindamisi.

— valvab pidevalt põhimõtete tegeliku järgimise üle, sealhulgas saadab osalevatele organisatsioonidele üksikasjalikke küsimustikke, tegemaks kindlaks probleeme, mis vajavad järelmeetmete võtmist. Eriti viiakse sellised vastavuskontrollid läbi juhul kui: a) ministeerium on saanud konkreetse tõsiseltvõetava kaebuse, et organisatsioon ei järgi põhimõtteid, b) organisatsioon ei vasta rahuldavalt ministeeriumi järelepärimistele andmekaitseraamistikku Privacy Shield puudutavates küsimustes või c) on olemas usutavad tõendid, et organisatsioon ei järgi andmekaitseraamistikus Privacy Shield võetud kohustusi. Ministeerium konsulteerib vastavuskontrollide osas pädevate andmekaitseasutustega, kui see on asjakohane, ja

— annab perioodiliselt hinnangu programmi Privacy Shield haldamise ja järelevalve kohta, tagamaks et tehtavad jõupingutused on asjakohased ning võimaldavad vajadusel tegeleda uute esilekerkivate probleemidega.

Ministeerium on lisanud ressursse programmi Privacy Shield haldamiseks ja järelevalveks, sealhulgas on kahekordistanud programmi haldamise ja järelevalve eest vastutavate töötajate arvu. Me jätkame vajalike ressursside eraldamist, et tagada programmi tõhus järelevalve ning haldamine.

Kohandab andmekaitseraamistiku Privacy Shield veebisaidi sihtgruppidele

Ministeerium kohandab andmekaitseraamistikku Privacy Shield, pidades silmas veebisaidi kolme sihtgruppi: ELi üksikisikud, ELi ettevõtjad ja USA ettevõtjad. Otse ELi üksikisikutele ja ELi ettevõtjatele suunatud materjali lisamine aitab mitmel viisil läbipaistvuse saavutamist hõlbustada. ELi üksikisikuid silmas pidades selgitatakse järgmist: 1) õigused, mida andmekaitseraamistik Privacy Shield annab ELi üksikisikutele; 2) ELi üksikisikutele kättesaadavad kaebuste menetlemise mehhanismid, juhuks kui nad leiavad, et mõni organisatsioon ei ole täitnud tema poolt võetud põhimõtete järgimise kohustust ning 3) kuidas leida teavet ühe organisatsiooni poolt antud põhimõtete järgimise kinnituse kohta. ELi ettevõtjatel hõlbustab veebisait kontrollida järgmist: 1) kas organisatsioonile on tagatud andmekaitseraamistiku Privacy Shield soodustused; 2) millist liiki teave on hõlmatud organisatsiooni antud kinnituses Privacy Shield põhimõtete järgimise kohta; 3) puutumatusnormid, mis kuuluvad asjaomasele teabele kohaldamisele ja 4) meetod, mida organisatsioon kasutab põhimõtete järgimise tõendamiseks.

Tugevdab koostööd andmekaitseasutustega

Koostöövõimaluste suurendamiseks andmekaitseasutustega seab ministeerium sisse spetsiaalse kontaktpunkti ministeeriumis, mille kaudu hakkab toimuma sidepidamine andmekaitseasutustega. Juhul, kui andmekaitseasutus leiab, et organisatsioon ei järgi põhimõtteid, sealhulgas peale kaebuse saamist ELi üksikisikult, võib andmekaitseasutus pöörduda määratud kontaktpunkti ministeeriumis organisatsiooni täiendavale kontrollimisele suunamiseks. Kontaktpunktile antakse samuti teada organisatsioonidest, kes esitavad valeväiteid osalemise kohta programmis Privacy Shield, vaatamata sellele, et nad ei ole kunagi kinnitanud põhimõtete järgimist. Kontaktpunkt abistab andmekaitseasutusi, kes soovivad saada teavet konkreetse organisatsiooni poolt antud kinnituse või eelneva osalemise kohta programmis, samuti vastab kontaktpunkt andmekaitseasutuste järelepärimistele andmekaitseraamistiku Privacy Shield konkreetsete nõuete rakendamise kohta. Teiseks varustab ministeerium andmekaitseasutusi andmekaitseraamistiku Privacy Shield kohta käivate materjalidega nende oma veebisaitidele lisamiseks, et suurendada läbipaistvust ELi üksikisikute ja ELi ettevõtjate jaoks. Suurenenud teadlikkus andmekaitseraamistiku Privacy Shield ning sellega kaasnevate õiguste ja kohustuste kohta peaks hõlbustama probleemide ilmnemisel nende tuvastamist ja asjakohast lahendamist.

Hõlbustab põhimõtete järgimata jätmise kohta esitatud kaebuste menetlemist

Ministeeriumile laekuvad määratud kontaktpunkti kaudu andmekaitseasutuste poolt edastatud kaebused, kui mõni andmekaitseraamistikuga Privacy Shield ühinenud organisatsioon ei järgi Privacy Shield põhimõtteid. Ministeerium teeb kõik selleks, et aidata kaasa kaebuse lahendamisele koos andmekaitseraamistikuga Privacy Shield ühinenud organisatsiooniga. 90 päeva jooksul pärast kaebuse saamist saadab ministeerium andmekaitseasutusele aruande. Selliste kaebuste esitamise hõlbustamiseks koostab ministeerium standardvormi, mida andmekaitseasutused saavad kasutada kaebuse esitamiseks ministeeriumi määratud kontaktpunktile. Määratud kontaktpunkt peab järge kõikide andmekaitseasutuste poolt ministeeriumile saadetud kaebuste üle ning allpool kirjeldatud aasta ülevaates esitab ministeerium aruande, milles analüüsib kokkuvõtlikult aasta jooksul laekunud kaebusi.

Kinnitab vahekohtu menetluskorra ja valib vahekohtunikud koostöös komisjoniga

Ministeerium täidab oma 1. lisa kohased kohustused ning pärast kokkuleppe saavutamist avaldab menetluskorra.

Ühine kontrollimehhanism andmekaitseraamistiku Privacy Shield toimimise üle

Kaubandusministeerium, FTC ja muud asutused peavad vastavalt vajadusele iga-aastaseid koosolekuid komisjoniga, huvitatud andmekaitseasutustega ja artikli 29 alusel asutatud töörühma asjakohaste esindajatega, kus ministeerium esitab ülevaated programmi Privacy Shield kohta. Iga-aastastel koosolekutel arutatakse muu hulgas jooksvaid küsimusi, mis on seotud andmekaitseraamistiku Privacy Shield toimimise, rakendamise, järelvalve ja jõustamisega, sealhulgas ministeeriumile andmekaitseasutustelt laekunud taotlustega, omal algatusel läbiviidud vastavuskontrollide tulemustega ning seal võidakse arutada ka asjakohaseid seadusemuudatusi. Esimene iga-aastane läbivaatamine ja sellele järgnevalt vajaduse korral teostatavad läbivaatamised hõlmavad dialoogi ka teistel asjakohastel teemadel, nagu näiteks automatiseeritud otsuste vastuvõtmine, sealhulgas ELi ja USA käsitlusviiside sarnasuste ja erinevustega seotud aspektid.

Seaduste ajakohastamine

Ministeerium teeb mõistlikke jõupingutusi komisjoni informeerimiseks olulistest muudatustest Ameerika Ühendriikide seadustes, mis on asjakohased andmekaitseraamistiku Privacy Shield raames isikuandmete kaitse ja USA ametiasutustele isikuandmetele juurdepääsuks ja nende edaspidiseks kasutamiseks rakendatavate piirangute ja kaitsemeetmete suhtes.

Riikliku julgeoleku erand

Riikliku julgeoleku huvides andmekaitseraamistiku Privacy Shield põhimõtete järgimise piirangute kohta on Robert Litt (USA riikliku luurejuhi ameti (ODNI) õigusnõunik) saatnud Justin Antonipillai ja Ted Dean'i nimele kaubandusministeeriumile kaks kirja, mis on Teile edastatud. Kõnealustes kirjades käsitletakse ulatuslikult muu hulgas ka eeskirju, kaitsemeetmeid ja piiranguid, mida kohaldatakse USA poolt läbiviidava signaaliluuretegevuse kohta. Lisaks kirjeldatakse kõnealustes kirjades, millist läbipaistvust luureühendus asjaomastes küsimustes võimaldab. Võttes arvesse, et komisjon on parajasti andmekaitseraamistikku Privacy Shield hindamas, võimaldab kõnealustes kirjades esitatud teave järeldada, et raamistik hakkab kooskõlas selles sisalduvate põhimõtetega nõuetekohaselt toimima. Me saame aru, et te võite leida teavet, mis on luureühenduse poolt üldsusele kättesaadavaks tehtud, ja muud teavet, et anda sellest teada iga-aastasel andmekaitseraamistiku Privacy Shield toimimise läbivaatamisel.

Lähtudes andmekaitseraamistiku Privacy Shield põhimõtetest ning lisatud kirjadest ja materjalidest, sealhulgas ministeeriumi poolt andmekaitseraamistiku Privacy Shield haldamise ja järelevalvega seoses võetud kohustustest, loodame, et komisjon otsustab, et ELi-USA andmekaitseraamistik Privacy Shield pakub piisavat kaitset ELi õiguse kohaselt, ning et jätkub andmete edastamine Euroopa Liidust nendele organisatsioonidele, kes programmis Privacy Shield osalevad.

Lugupidamisega

Ken Hyatt

*2. lisa*

**Vahekohtumudel**

*I LISA*

Käesolevas I lisas sätestatakse tingimused, mille alusel andmekaitseraamistikuga Privacy Shield ühinenud organisatsioonid on kohustatud kaebusi vahekohtus lahendama vastavalt kaebuste käsitlemise, täitmise tagamise ja vastutuse põhimõttele. Allpool kirjeldatud siduv vahekohtumenetluse kasutamise võimalus kuulub kohaldamsiele ELi-USA andmekaitseraamistikuga Privacy Shield hõlmatud isikuandmete suhtes esitatavate teatud „jääknõuete" puhul. Kõnealuse valikuvõimaluse andmise eesmärgiks on pakkuda üksikisikutele kiire, sõltumatu ja õiglane mehhanism, mille nad võivad valida väidetavate põhimõtete rikkumiste lahendamiseks, mida ei ole lahendatud muude võimalike andmekaitseraamistiku Privacy Shield mehhanismide abil.

A. **Kohaldamisala**

Kõnealune võimalus on üksikisikule kättesaadav allesjäänud nõuetega vahekohtu poole pöördumiseks, et teha kindlaks, kas andmekaitseraamistikuga Privacy Shield ühinenud organisatsioon on rikkunud Privacy Shield põhimõtete järgseid kohustusi asjaomase üksikisiku suhtes ja kas selline rikkumine jääb täielikult või osaliselt heastamata. Kõnealune võimalus on ainult nimetatud eesmärkidel kasutamiseks. Kõnealune võimalus ei ole kasutamiseks näiteks põhimõtete suhtes tehtavate erandite ([1]) või väidete suhtes, mis puudutavad andmekaitseraamistiku Privacy Shield piisavust.

B. **Kättesaadavad õiguskaitsevahendid**

Kõnealuse vahekohtu võimaluse raames on andmekaitseraamistiku Privacy Shield paneelil (mis koosneb kolmest vahekohtunikust, kelles pooled on kokku leppinud) volitused kehtestada konkreetse üksikisiku suhtes rakendatavad mitterahalised õiglased kaitsevahendid (näiteks juurdepääsu võimaldamine, parandamine, kustutamine või üksikisiku küsimuse all olevate andmete tagastamine), mis on vajalikud põhimõtete rikkumise heastamiseks ainult asjaomasele üksikisikule. Kõnealused volitused on ainsad, mis vahekohtunikel on õiguskaitsevahendite suhtes. Õiguskaitsevahendeid kaaludes peavad vahekohtunikud arvesse võtma ka teiste andmekaitseraamistiku Privacy Shield mehhanismide poolt juba rakendatud õiguskaitsevahendeid. Kahjuhüvitisi, kulude ja tasude hüvitamist või muid õiguskaitsevahendeid ette ei nähta. Kumbki pool maksab ise oma advokaaditasud.

C. **Vajalikud sammud enne vahekohtu poole pöördumist**

Üksikisik, kes otsustab kasutada kõnealust vahekohtumenetluse võimalust, peab enne vahekohtule nõude esitamist tegema järgmist: 1) pöörduma väidetava rikkumisega otse organisatsiooni poole ja võimaldama organisatsioonil asi lahendada põhimõtete jaos III.11(d)(i) sätestatud ajavahemiku jooksul; 2) kasutama põhimõtete kohast sõltumatut kaebuste menetlemise mehhanismi, mis on üksikisikutele tasuta; ja 3) esitada juhtum oma andmekaitseasutuse kaudu lahendamiseks kaubandusministeeriumile ning võimaldada kaubandusministeeriumil lahendada asi parimal moel aja jooksul, mis on sätestatud kaubandusministeeriumi väliskaubandusameti kirjas ja mis on üksikisikutele tasuta.

Kõnealuse vahekohtumenetluse võimalust ei saa kasutada, kui üksikisiku poolt väidetav sama põhimõtete rikkumist 1) on juba varem vahekohtumenetluses menetletud; 2) on olnud aluseks lõplikule kohtuotsusele kohtuasjas, milles kõnealune üksikisik oli üheks pooleks; või 3) mille osas pooled on eelnevalt kokkuleppele jõudnud. Lisaks ei saa kõnealust võimalust kasutada, kui ELi andmekaitseasutusel on 1) põhimõtete jagude III.5 või III.9 kohased volitused; või 2) volitused lahendada väidetav rikkumine otse organisatsiooniga. Andmekaitseasutuse volitus lahendada sama nõuet ELi vastutava töötleja vastu ei välista kõnealuse vahekohtumenetluse võimaluse kasutamist teise õigussubjekti vastu, kes ei ole andmekaitseasutuse volitustega seotud.

D. **Otsuste siduvus**

Üksikisiku otsus kasutada siduvat vahekohtumenetlust on täiesti vabatahtlik. Vahekohtu otsused on siduvad kõikidele vahekohtumenetluse pooltele. Pöördudes vahekohtu poole, loobub üksikisik võimalusest saada sama rikkumise suhtes abi mõnest teisest foorumist, välja arvatud juhul, kui mitterahalised õiglased õiguskaitsevahendid ei heasta täielikult väidetavat rikkumist, mispuhul üksikisiku pöördumine vahekohtu poole ei takista kahjuhüvitise sissenõudmist, mida tavaliselt tehakse kohtu kaudu.

([1]) Põhimõtete jagu I.5.

E. **Läbivaatus ja jõustamine**

Föderaalse vahekohtu seaduse (Federal Arbitration Act) ([1]) kohaselt on üksikisikutel ja andmekaitseraamistikuga Privacy Shield ühinenud organisatsioonidel õigus taotleda kohtulikku läbivaatust ning vahekohtu otsuste jõustamist Ameerika Ühendriikide seaduste alusel. Kõikidel sellistel juhtudel tuleb pöörduda föderaalsesse ringkonnakohtusse, mille territooriumile jääb andmekaitseraamistikuga Privacy Shield ühinenud organisatsiooni peamine tegevuskoht.

Käesolev vahekohtumenetluse valimise võimalus on mõeldud vaid üksikisikuid puudutavate vaidluste lahendamiseks ja mitte veenvate või siduvate pretsedentide loomiseks teisi isikuid puudutavates asjades, sealhulgas tulevaste vaidluste lahendamiseks vahekohtutes, ELi või USA kohtutes või FTC menetlustes.

F. **Vahekohtu koosseis**

Pooled valivad vahekohtunikud allpool vaadeldud vahekohtunike nimekirjast.

Kooskõlas kohaldatava õigusega koostavad Ameerika Ühendriikide kaubandusministeerium ja Euroopa Komisjon nimekirja vähemalt 20 vahekohtunikust, kes valitakse nende sõltumatuse, aususe ja asjatundlikkuse alusel. Seoses kõnealuse protsessiga kohaldatakse järgmist.

Vahekohtunikud:

1) jäävad nimekirja kolmeks aastaks, kui ei ilmne erandlikke asjaolusid või põhjuseid, ning seda määramist võib pikendada üks kord täiendavaks kolmeaastaseks perioodiks;

2) ei ole ühegi partei ega andmekaitseraamistikuga Privacy Shield ühinenud organisatsiooni, või USA või ELi või ELi liikmesriigi või muu valitsusasutuse, avalik-õigusliku asutuse või täitevasutusega seotud ega toimi nende juhtnööride järgi ning

3) peavad olema lubatud töötama juristina USAs ja olema asjatundjad USA eraelu puutumatust käsitlevate ning ELi isikuandmete kaitset käsitlevate õigusaktide alal.

G. **Vahekohtumenetlus**

Kooskõlas kehtivate seadustega lepivad kaubandusministeerium ja Euroopa Komisjon kuus kuud peale piisavusotsuse vastuvõtmist kokku olemasolevate, kindlalt väljakujunenud USA vahekohtumenetluste (nagu näiteks AAA või JAMS) kasutuselevõtmiseks andmekaitseraamistiku Privacy Shield paneeli poolt, kõikidel alljärgnevatel tingimustel:

1. Üksikisik võib algatada siduva vahekohtumenetluse, kooskõlas eespool kirjeldatud vahekohtu poole pöördumise eelset menetlust käsitleva sättega, saates organisatsioonile „teate". Teade peab sisaldama kokkuvõtet lõigus C kirjeldatud sammudest, mis on nõude lahendamiseks tehtud, kirjeldust väidetava rikkumise kohta ja üksikisiku valikul mis tahes toetavaid materjale ja dokumente ja/või asjaomast nõuet puudutavate õigusaktide käsitlust.

([1]) Föderaalse vahekohtu seaduse (Federal Arbitration Act, FAA) 2. peatüki kohaselt „kuulub õigussuhtest – sõltumata sellest, kas see on lepinguline või mitte –, mida loetakse äriliseks, sealhulgas FAA 2. jaos kirjeldatud tehing, leping või kokkulepe, tuleneva vahekohtus sõlmitud kokkuleppe või vahekohtuotsuse suhtes kohaldamisele konventsioon [on the Recognition and Enforcement of Foreign Arbitral Awards of June 10, 1958, 21 U.S.T. 2519, T.I.A.S. No. 6997 („New York Convention")]." 9 U.S.C. § 202. Lisaks sätestatakse FAAs, et „kokkuleppe või otsuse suhtes, mis tuleneb sellisest õigussuhtest ja mis jääb täies ulatuses Ameerika Ühendriikide kodanike vahele, ei kohaldata konventsiooni [New York], juhul kui see õigussuhe ei ole hõlma välismaal asuvat kinnisvara, see ei näe ette välismaal täitmist või täitmisele pööramist, või sellel on muu mõistlik seos ühe või mitme välisriigiga." Samas sätestatakse 2. peatükis, et „kõik vahekohtumenetluse pooled võivad pöörduda mis tahes kohtu poole, kellel on käesoleva peatüki kohane pädevus, et saada kinnitav kohtuotsus vahekohtumenetluse teise poole suhtes. Kohus kinnitab otsuse, juhul kui ta ei leia ühtegi kõnealuses konventsioonis [New York] sätestatud põhjust otsuse tunnustamise või täitmise kinnitamisest keeldumiseks või edasilükkamiseks." *Id.* § 207. Edasi sätestatakse 2. peatükis, et „Ameerika Ühendriikide ringkonnakohtutel.. on esimese kohtuastme pädevus. .. hagi või menetluse suhtes (New Yorki konventsiooni kohaselt), vaatamata vaidlusalusele summale." *Id.* § 203.
2. peatükis sätestatakse ka, et „1. peatükk kehtib käesoleva peatüki alusel esitatud nõuete ja algatatud menetluste suhtes sellises ulatuses, milles kõnealune peatükk ei ole vastuolus käesoleva peatükiga või konventsiooniga [New York], mille Ameerika Ühendriigid on ratifitseerinud." *Id.* § 208. 1. peatükk sätestab omakorda, et kirjalik säte. ... lepingus, mis tõendab tehingut, mis hõlmab äritegevust, mille suhtes tuleb lahendus leida vahekohtumenetluse teel seejärel sellise lepingu või tehingu alusel tekkinud vaidluse või keeldumise pärast kogu või mis tahes selle osa täitmisest, või kirjalik leping sellisest lepingust, tehingust või keeldumisest tekkinud olemasoleva vastuolu vahekohtule lahendamiseks esitamiseks, on kehtiv, tühistamatu ja jõustatav, välja arvatud põhjustel, mida näeb ette seadus või õiglane kohtumenetlus mis tahes lepingu ülesütlemiseks. *Id.* § 2. Edasi sätestab 1. peatükk, et „mis tahes vahekohtumenetluse pool võib pöörduda selleks määratud kohtusse, saamaks vahekohtu otsust kinnitavat otsust, ja kohus peab seejärel sellise otsuse tegema, välja arvatud juhul kui vahekohtu otsus on tühistatud, muudetud või parandatud vastavalt [FAA] jagudes 10 ja 11 sätestatule." *Id.* § 9.

2. Töötatakse välja menetluskord tagamaks, et üht ja sama üksikisiku poolt väidetavat rikkumist ei heastataks ega menetletaks kaks korda.

3. FTC tegevus võib toimuda paralleelselt vahekohtumenetlusega.

4. Asjaomasel vahekohtumenetluse läbiviimsiel ei või osaleda mitte ükski USA, ELi või ELi liikmesriigi või muu valitsusasutuse, avalik-õigusliku asutuse või täitevasutuse esindaja, välja arvatud juhul, kui ELi andmekaitseasutus osutab ELi üksikisiku palvel abi vaid teate ettevalmistamisel, ent ELi andmekaitseasutus ei tohi saada juurdepääsu kõnealuste vahekohtute poolt tuvastatud asjaoludele või muudele materjalidele.

5. Vahekohtumenetlus toimub Ameerika Ühendriikides ning üksikisik võib valida osalemise video või telefoni teel, mis talle võimaldatakse tasuta. Isiklikult kohalviibimine ei ole nõutav.

6. Vahekohtu keel on inglise keel, kui pooled ei lepi kokku teisiti. Põhjendatud juhtudel ja võttes arvesse seda, kas üksikisikut esindab advokaat või ei, võimaldatakse üksikisikutele vahekohtu istungitel tasuta suuline tõlge, samuti ka vahekohtu materjalide kirjalik tõlge, välja arvatud juhul, kui kohus leiab, et konkreetseid asjaolusid arvesse võttes oleksid kulud põhjendamatult ebaproportsionaalsed.

7. Vahekohtunikele edastatavad materjalid hoitakse konfidentsiaalsetena ning neid kasutatakse ainult seoses vahekohtu tegevusega.

8. Konkreetset üksikisikut puudutavad menetluseelsed meetmed on vajadusel lubatud, ent pooled peavad sellega seotud teavet käsitama konfidentsiaalsena ning neid võib kasutada üksnes vahekohtumenetluse eesmärkidel.

9. Vahekohus peaks otsuseni jõudma 90 päeva jooksul alates teatise laekumisest küsimuse all olevale organisatsioonile, kui pooled teisiti kokku ei lepi.

H. **Kulud**

Vahekohtunikud peaksid püüdma astuda mõistlikke samme vahekohtu kulude või tasude minimeerimiseks.

Kohaldatavatest õigusnormidest lähtudes aitab kaubandusministeerium, kooskõlastatult Euroopa Komisjoniga, kaasa fondi loomisele, kuhu andmekaitseraamistikuga Privacy Shield ühinenud organisatsioonid peavad tegema iga-aastaseid sissemakseid, mille suurus sõltub osaliselt organisatsiooni suurusest ja millega kaetakse vahekohtumenetluse kulud, kaasa arvatud vahekohtunike tasud, mis võivad ulatuda ette nähtud ülemmääradeni. Fondi hakkab haldama kolmas isik, kellel tuleb regulaarselt esitada aruandeid fondi tegevuse kohta. Iga-aastase läbivaatamise käigus vaatavad kaubandusministeerium ja Euroopa Komisjon üle fondi tegevuse, sealhulgas vajaduse muuta sissemaksete suurust või tasude ülemmäärasid, ning võtavad muu hulgas arvesse peetud vahekohtumenetluste arvu ning seonduvaid kulusid ja ajalisi faktoreid, kusjuures vastastikuse arusaama kohaselt ei või andmekaitseraamistikuga Privacy Shield ühinenud organisatsioone rahaliselt ülemäära koormata. Käesoleva sätte alusel ega ka mitte ühestki käesoleva sätte alusel tegutsevast fondist ei kaeta advokaaditasusid.

*II LISA*

**ELI-USA ANDMEKAITSERAAMISTIKU PRIVACY SHIELD PÕHIMÕTTED VÄLJA ANTUD AMEERIKA ÜHENDRIIKIDE KAUBANDUSMINISTEERIUMI POOLT**

I. ÜLEVAADE

1. Kuigi Ameerika Ühendriikide eesmärk sarnaselt Euroopa Liiduga on eraelu puutumatuse kaitse suurendamine, lähenevad Ameerika Ühendriigid eraelu puutumatusele teisiti kui Euroopa Liit. Ameerika Ühendriigid kasutavad sektoripõhist lähenemist, mis tugineb õigusnormide, regulatsiooni ja iseregulatsiooni koosmõjul. Võttes arvesse kõnealuseid erinevusi ja selleks, et pakkuda Ameerika Ühendriikide organisatsioonidele usaldatavat mehhanismi isikuandmete edastamiseks Euroopa Liidust Ameerika Ühendriikidesse, samal ajal ELi andmesubjektide huvides jätkuvalt tõhusaid kaitsemeetmeid rakendades ja neile kaitset tagades, nagu on sätestatud Euroopa õigusaktides, mis käsitlevad nende isikuandmete töötlemist, mis edastatakse kolmandatesse riikidesse, annab kaubandusministeerium välja käesolevad andmekaitseraamistiku Privacy Shield põhimõtted, sealhulgas täiendavad põhimõtted (edaspidi „põhimõtted"), täites oma põhikirja kohast ülesannet, milleks on rahvusvahelise kaubanduse soodustamine, edendamine ja arendamine (15 U.S.C. § 1512). Põhimõtted töötati välja koostöös Euroopa Komisjoni, tootjate ja muude huvirühmadega kaubandustegevuse lihtsustamiseks Ameerika Ühendriikide ja Euroopa Liidu vahel. Need on mõeldud kasutamiseks ainult isikuandmeid Euroopa Liidust vastu võtvatele Ameerika Ühendriikide organisatsioonidele, et saavutada vastavus programmi Privacy Shield põhimõtetega ja seeläbi saada kasu Euroopa Komisjoni piisavusotsusest ([1]). Põhimõtted ei mõjuta direktiivi 95/46/EÜ („direktiiv") rakendamiseks vastu võetud siseriiklikke õigusnorme, mida kohaldatakse isikuandmete töötlemisele liikmesriikides. Samuti ei piira Privacy Shield põhimõtted Ameerika Ühendriikide õiguse alusel eraelu puutumatuse suhtes kohaldatavaid kohustusi.

2. Selleks, et toetuda andmekaitseraamistikule Privacy Shield, mis võimaldab Euroopa Liidust edastatud isikuandmeid saada, peab organisatsioon kinnitama põhimõtete järgimist kaubandusministeeriumile (või tema poolt määratud isikule) („ministeerium"). Organisatsiooni otsus ühineda andmekaitseraamistikuga Privacy Shield on vabatahtlik, ent raamistiku põhimõtetest tegelik kinnipidamine on kohustuslik: organisatsioonid, kes kinnitavad ministeeriumile põhimõtete järgimist ning teatavad avalikult, et nad põhimõtteid järgivad, peavad tegutsema täielikus vastavuses nende põhimõtetega. Selleks, et liituda programmiga Privacy Shield, peab organisatsioon a) tunnustama föderaalse kaubanduskomisjoni („FTC"), transpordiministeeriumi või muu täitevasutuse, kes tagab tõhusalt põhimõtete järgimise, volitusi uurimise läbiviimiseks ja sunni rakendamiseks *(muud ELi poolt tunnustatud Ameerika Ühendriikide täitevasutused võitakse lisada tulevikus juurde ühe lisana)*; b) avalikult kinnitama põhimõtete järgimise kohustust; c) tegema avalikuks kõnealuste põhimõtetega kooskõlas olevad puutumatusnormid; ning d) rakendama neid täielikult. Organisatsiooni mittevastavuse kohta saab kaebuse esitada föderaalse kaubanduskomisjoni seaduse (Federal Trade Commission Act) paragrahvi 5 alusel, mis keelustab äritegevuses kasutatavad või äritegevust mõjutavad kõlvatud tavad ja pettuse (15 U.S.C. § 45(a)), või selliseid tegusid reguleeriva muu seaduse või määruse alusel.

3. Kaubandusministeerium usaldusväärset nimekirja nende USA organisatsioonide kohta, kes on kinnitanud ministeeriumile, et nad järgivad andmekaitseraamistiku põhimõtteid ja kohustuvad neist kinni pidama („andmekaitseraamistikuga Privacy Shield ühinenute nimekiri"), ning avalikustab selle. Programmi Privacy Shield soodustused on tagatud sellest päevast alates, kui ministeerium lisab organisatsiooni andmekaitseraamistikuga Privacy Shield ühinenute nimekirja. Ministeerium eemaldab organisatsiooni andmekaitseraamistikuga Privacy Shield ühinenute nimekirjast, kui organisatsioon lahkub vabatahtlikult programmist Privacy Shield või jätab ministeeriumile esitamata oma iga-aastase kinnituse. Organisatsiooni eemaldamine andmekaitseraamistikuga Privacy Shield ühinenute nimekirjast tähendab, et ta ei või enam Euroopa Komisjoni piisavusotsuse alusel antava soodustusena saada EList isikuandmeid. Organisatsioon peab jätkama Privacy Shield põhimõtete rakendamist isikuandmete suhtes, mille ta sai programmis Privacy Shield osaledes, ning kinnitama ministeeriumile igal aastal põhimõtetest kinnipidamist, niikaua kuni ta säilitab kõnealuseid andmeid; vastasel juhul peab organisatsioon andmed tagastama või kustutama või tagama andmete „piisava" kaitse muid heakskiidetud meetodeid kasutades. Ministeerium eemaldab andmekaitseraamistikuga Privacy Shield ühinenute nimekirjast ka need organisatsioonid, kes ei ole püsivalt põhimõtteid järginud; Kõnealused organisatsioonid jäävad ilma programmi Privacy Shield soodustustest ning peavad tagastama või kustutama isikuandmed, mille nad said, kui nad osalesid programmis Privacy Shield.

4. Ministeerium säilitab ja avalikustab ka usaldusväärsed andmed USA organisatsioonide kohta, kes on varasemalt ministeeriumile põhimõtete järgimist kinnitanud, ent kes on andmekaitseraamistikuga Privacy Shield ühinenute nimekirjast eemaldatud. Ministeerium annab selge hoiatuse, et kõnealused organisatsioonid ei osale programmis Privacy Shield; et eemaldamine andmekaitseraamistikuga Privacy Shield ühinenute nimekirjast tähendab, et selline

([1]) Juhul kui komisjoni piisavusotsus ELi-USA andmekaitseraamistiku Privacy Shield poolt osutatava kaitse kohta rakendub ka Islandi, Norra ja Liechtensteini suhtes, katab andmekaitseraamistiku Privacy Shield pakett nii Euroopa Liitu kui ka kolme kõnealust riiki. Seega loetakse seal, kus on viidatud ELile ja liikmesriikidele, nende hulka ka Island, Liechtenstein ja Norra.

organisatsioon ei saa väita, et ta toimib andmekaitseraamistikuga Privacy Shield kooskõlas ja ta peab hoiduma mis tahes avaldustest või eksitavatest tavadest, mis viitavad, et ta osaleb programmis Privacy Shield; ja sellistel organisatsioonidel ei ole enam õigust saada soodustusi Euroopa Komisjoni piisavusotsuse alusel, mis võimaldaks kõnealustel organisatsioonidel saada EList isikuandmeid. Sellise organisatsiooni suhtes, kes väidab, et ta osaleb jätkuvalt programmis Privacy Shield või esitab muid programmiga Privacy Shield seotud valeandmeid pärast seda, kui ta on andmekaitseraamistikuga Privacy Shield ühinenute nimekirjast eemaldatud, võivad FTC, transpordiministeerium või muud täitevasutused rakendada täitemeetmeid.

5. 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. Vastavalt eraelu puutumatuse kaitse suurendamise eesmärgile peaksid organisatsioonid püüdma neid põhimõtteid täielikult ja läbipaistvalt rakendada, sealhulgas sätestama oma puutumatusnormides, kui eespool toodud punkti b erandeid rakendatakse korrapäraselt. Samal põhjusel eeldatakse, et kui on võimalik teha valik Privacy Shield põhimõtete ja/või Ameerika Ühendriikide seaduste alusel, valivad organisatsioonid võimalusel kõrgema kaitse taseme.

6. Organisatsioonid on kohustatud järgima põhimõtteid kõikide isikuandmete suhtes, mis on edastatud andmekaitseraamistikule Privacy Shield tuginedes, pärast seda kui nad on kõnealuse raamistikuga ühinenud. Organisatsioon, kes soovib programmi Privacy Shield soodustusi laiendada EList töösuhte kontekstis edastatavatele personali puudutavatele isikuandmetele, peab sellest teatama ministeeriumile, kui ta kinnitab põhimõtete järgimist, ning peab järgima ise kinnitamise kohta käiva täiendava põhimõtte nõudeid.

7. Andmekaitseraamistiku Privacy Shield põhimõtete ja raamistikuga ühinenud organisatsioonide asjakohaste puutumatusnormide tõlgendamise ja neile vastavuse küsimustes kohaldatakse Ameerika Ühendriikide seadusi, välja arvatud kui organisatsioonid on kohustunud tegema koostööd Euroopa andmekaitseasutustega. Kõiki põhimõtteid kohaldatakse vastavalt nende asjakohasusele, kui ei ole sätestatud teisiti.

8. Mõisted:

   a) Isikuandmed – identifitseeritud või identifitseeritava üksikisiku kohta käivad direktiivi reguleerimisalasse kuuluvad andmed, mida Ameerika Ühendriikides asuv organisatsioon Euroopa Liidust saab ja mis tahes vormis salvestab.

   b) Isikuandmete töötlemine (edaspidi „töötlemine“) – iga isikuandmetega tehtav toiming või toimingute kogum, olenemata sellest, kas see on automatiseeritud või mitte, näiteks kogumine, salvestamine, korrastamine, säilitamine, kohandamine või muutmine, väljavõtete tegemine, järelpärimise teostamine, kasutamine, üleandmine või levitamine ja kustutamine või hävitamine;

   c) Vastutav töötleja – isik või organisatsioon, kes määrab üksi või koos teistega kindlaks isikuandmete töötlemise eesmärgid ja vahendid;

9. Põhimõtete jõustumise kuupäev on Euroopa Komisjoni piisavusotsuse lõpliku heakskiidu kuupäev.

II. PÕHIMÕTTED

1. **Teade**

   a) Organisatsioon peab üksikisikutele teada andma järgmistest asjaoludest:

      i) oma osalemisest programmis Privacy Shield ja lisama lingi veebiaadressile, kus asub andmekaitseraamistikuga Privacy Shield ühinenute nimekiri,

      ii) millist liiki isikuandmeid kogutakse ja, kui asjakohane, nimetama ära ka organisatsiooni üksused või tütarettevõtjad, kes samuti Privacy Shield põhimõtteid järgivad,

iii) oma kohustusest järgida Privacy Shield põhimõtteid kõikide EList andmekaitseraamistikule Privacy Shield tuginedes saadud isikuandmete suhtes,

iv) nende isikuandmete kogumise ja kasutamise eesmärgid,

v) kuidas järelepärimiste või kaebuste esitamiseks võtta ühendust organisatsiooniga ning kõikide asjakohaste asutustega ELis, kes on pädevad vastama kõnealustele järelepärimistele või kaebustele,

vi) mis eesmärkidel ja millist liiki kolmandatele isikutele ta avalikustab isikuandmed,

vii) üksikisikute õigus juurdepääsuks oma isikuandmetele,

viii) valikud ja vahendid, mida organisatsioon pakub üksikisikutele nende isikuandmete kasutamise ja avalikustamise piiramiseks,

ix) milline on see sõltumatu organ, kes on määratud vaidlusi lahendama ja kes osutab vajalikku abi üksikisikutele tasuta, ning kas selleks on: 1) andmekaitseasutuse poolt loodud paneel, 2) alternatiivne sõltumatu organ vaidluste lahendamiseks ELis või 3) Ameerika Ühendriikides asuv alternatiivne sõltumatu organ vaidluste lahendamiseks,

x) organisatsioon tunnustab Federal Trade Commission'i, transpordiministeeriumi või muu Ameerika Ühendriikide täitevasutuse volitusi uurimise läbiviimiseks ja sunni rakendamiseks,

xi) teatud tingimustel on üksikisikul võimalus tugineda siduvale vahekohtuotsusele,

xii) nõue avaldada isikuandmed seadustega kooskõlas oleva taotluse alusel riigiasutustele, sealhulgas riikliku julgeoleku või õiguskaitselisteks vajaduste täitmiseks, ning

xiii) organisatsiooni kohustused kolmandatele isikutele andmete edastamisel.

b) Selline teade tuleb esitada selges ja arusaadavas keeles, 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.

2. **Valikuvõimalus**

a) Organisatsioon peab pakkuma üksikisikutele võimaluse valida (opt out), kas nende isikuandmeid i) avaldatakse kolmandale isikule või ii) kasutatakse eesmärgil, mis on oluliselt erinev sellest, milleks neid algselt koguti või milleks üksikisik seejärel loa andis. Üksikisikutele tuleb võimaldada selge, arusaadav ja kergesti kättesaadav mehhanism valiku teostamiseks.

b) Erandina eelmises lõigus märgitust ei ole valikuvõimalust vaja pakkuda, kui andmed avaldatakse kolmandale isikule, kes täidab esindajana ülesandeid organisatsiooni nimel ja selle juhtnööre järgides. Organisatsioon peab alati esindajaga lepingu sõlmima.

c) Tundliku teabe osas (st isikuandmed, mis täpsustavad meditsiinilist või tervislikku seisundit, rassilist või etnilist päritolu, poliitilisi vaateid, religioosseid või filosoofilisi vaateid, ametiühingu liikmelisust või teavet üksikisiku seksuaalelu kohta) peavad organisatsioonid saama üksikisikult kinnitava selgesõnalise nõusoleku (opt in), kui teave i) avalikustatakse kolmandale osapoolele või ii) seda kasutatakse muudel eesmärkidel kui see, milleks seda algselt koguti või milleks üksikisik seejärel loa andis nõustuva (opt in) valikuga. Lisaks peab organisatsioon käsitlema tundliku teabena selliseid kolmandalt isikult saadavaid isikuandmeid, mida kolmas isik määratleb ja käsitleb tundliku teabena.

3. **Vastutus kolmandale osapoolele andmete edastamise eest**

a) Isikuandmete edastamisel kolmandale isikule, kes on vastutav töötleja, peavad organisatsioonid järgima teate ja valikuvõimaluse põhimõtteid. Organisatsioonid peavad samuti sõlmima lepingu kolmanda osapoolega, kes on vastutav töötleja, milles nähakse ette, et asjaomaseid andmeid tohib töödelda ainult piiratud ja konkreetsetel eesmärkidel, kooskõlas isiku poolt antud nõusolekuga, ning et saaja tagab põhimõtetes sätestatuga samal tasemel kaitse ja teatab organisatsioonile, kui ta teeb otsuse, et ei suuda asjaomast kohustust enam täita. Lepingus sätestatakse, et kui selline otsus tehakse, siis kolmas osapool, kes on vastutav töötleja, lõpetab töötlemise või võtab heastamiseks muid mõistlikke ja asjakohaseid meetmeid.

b) Isikuandmete edastamisel kolmandale isikule, kes on tema esindaja, peab organisatsioon: i) edastama sellised andmed ainult piiratud ja konkreetsetel eesmärkidel; ii) tegema kindlaks, et esindaja on kohustatud tagama eraelu puutumatuse kaitse vähemalt põhimõtetes sätestatuga samal tasemel; iii) võtma mõistlikud ja asjakohased meetmed tagamaks, et esindaja töötleb edastatud isikuandmeid ka tegelikult viisil, mis on kooskõlas organisatsiooni poolt võetud põhimõtteid järgivate kohustustega; iv) nõudma, et agent teataks organisatsioonile, kui ta teeb otsuse, et ei suuda enam täita kohustust tagada kaitse põhimõtetes nõutaval tasemel; v) saades, sealhulgas alapunktis iv kohaselt teadlikuks volitamatust töötlemisest võtab mõistlikud ja asjakohased meetmed selle peatamiseks ja heastamiseks; ja vi) esitab nõudmisel ministeeriumile kokkuvõtte või koopia kõnealustest eraelu puutumatust käsitlevatest, asjaomase esindajaga sõlmitud lepingu sätetest.

4. **Turvalisus**

a) Organisatsioonid, mis tekitavad, säilitavad, kasutavad või levitavad isikuandmeid, peavad rakendama mõistlikke ja kohaseid ettevaatusabinõusid nende kaitsmiseks kadumise, väärkasutuse ja volitamatu juurdepääsu, avalikustamise, muutmise ja hävitamise eest, võttes nõuetekohaselt arvesse töötlemisega seotud riske ning isikuandmete laadi.

5. **Andmete terviklikkus ja eesmärgi piiramine**

a) Vastavalt põhimõtetele peavad isikuandmed olema piiratud teabega, mis on töötlemise eesmärke arvesse võttes asjakohane ([1]). Organisatsioon ei tohi isikuandmeid töödelda viisil, mis ei vasta eesmärkidele, milleks need koguti või milleks üksikisik seejärel loa andis. Nendel eesmärkidel vajalikus ulatuses peab organisatsioon võtma mõistlikke meetmeid, tagamaks et isikuandmed on kavatsetud kasutuseks usaldusväärsed, täpsed, täielikud ja ajakohased. Organisatsioon peab põhimõtteid järgima nii kaua, kuni kõnealune teave tema kästuses on.

b) Informatsiooni võib säilitada kujul, mis identifitseerib või võimaldab identifitseerida ([2]) üksikisikut ainult niikaua, kuni see on vajalik töötlemiseks 5a tähenduses. Kõnealune kohustus ei takista organisatsioonidel isikuandmete töötlemist pikemal ajaperioodil, kui töötlemine toimub mõistliku aja jooksul ja määral, mis vastab avalikes huvides arhiveerimise, ajakirjanduslikele, kirjanduse ja kunsti, teadusliku või ajaloo-alase uurimise ja statistilise analüüsi eesmärkidele. Kõnealustel juhtudel kehtivad sellise töötlemise suhtes raamistiku muud põhimõtted ja sätted. Organisatsioonid peaksid võtma mõistlikke ja kohaseid meetmeid kõnealuse sätte järgimiseks.

6. **Juurdepääs**

a) Üksikisikutel peab olema juurdepääs organisatsiooni käes olevatele neid puudutavatele isikuandmetele ning võimalus andmeid parandada, muuta või kustutada, kui need on ebatäpsed või neid on töödeldud vastuolus põhimõtetega, välja arvatud kui juurdepääsu võimaldamise tülikus või kulu asjaomasel juhul oleks puutumatust ähvardava ohuga ebaproprotsionaalne või kui see rikuks teiste isikute õigusi peale asjaomase isiku.

([1]) Olenevalt olukorrast võivad nõuetele vastavad töötlemiseesmärgid näiteks hõlmata mõistlikul määral kliendisuhteid teenivaid, nõuetele vastavuse ja juriidilistel kaalutlustel põhinevaid, auditeerimise, julgeoleku ja pettuste ennetamise, organisatsiooni õigushüvede säilitamise või kaitsmise või muid eesmärke, mis vastavad mõistliku inimese ootustele andmete kogumise kontekstis.

([2]) Kõnealuses kontekstis on üksikisik „identifitseeritav" juhul, kui üksikisiku identifitseerimine oleks organisatsiooni või kolmanda isiku poolt mõistlikult teostatav juhul, kui neil oleks juurdepääs andmetele, võttes arvesse tõenäoliselt kasutamiseks sobivaid identifitseerimisvahendeid (muu hulgas võttes arvesse identifitseerimise raha- ja ajakulu ning töötlemise ajal kättesaadavat tehnoloogiat) ning seda, millisel kujul andmeid säilitatakse.

7. **Kaebuste menetlemine, täitmise tagamine ja vastutus**

a) Tõhus puutumatuse kaitse peab hõlmama jõulisi mehhanisme põhimõte järgimise tagamiseks, kaebuste esitamise võimalust üksikisikutele, keda põhimõtete eiramine on mõjutanud, ning tagajärgi organisatsioonile, kui põhimõtteid ei järgita. Need mehhanismid peavad sisaldama minimaalselt:

i) kergesti kättesaadavaid sõltumatuid kaebuste menetlemise mehhanisme, mille abil iga üksikisiku kaebusi ja vaidlusi uuritakse ja lahendatakse tulemuslikult üksikisiku jaoks ja kooskõlas põhimõtetega, ning määratakse kahjuhüvitis juhul, kui kohaldatav seadus või erasektori initsiatiiv seda ette näeb;

ii) kontrollimeetmeid veendumaks, et kinnitused ja väited, mida organisatsioonid oma puutumatustavade kohta on esitanud, vastavad tõele ja et kõnealuste tavade rakendamine vastab esitatule, eriti juhtumite puhul, kus on esinenud põhimõtete mittejärgmine, ja

iii) põhimõtete järgimist kinnitanud organisatsioonide kohustuse heastada põhimõtete järgimata jätmisest tekkivad probleemid ning tagajärjed sellistele organisatsioonidele. Sanktsioonid peavad olema piisavalt ranged tagamaks, et organisatsioonid tegutseksid kooskõlas põhimõtetega.

b) Organisatsioonid ja nende poolt valitud sõltumatud kaebuste menetlemise mehhanismid peavad reageerima kiiresti järelepärimistele ja ministeeriumi nõudmistele esitada andmekaitseraamistikuga Privacy Shield seotud teavet. Kõik organisatsioonid peavad viivitamata reageerima kaebustele, mis käsitlevad põhimõtete järgimist ja mille on esitanud ELi liikmesriikide ametiasutused ministeeriumi kaudu. Organisatsioonid, kes on otsustanud teha koostööd andmekaitseasutusega, sealhulgas organisatsioonid, kes töötlevad personali isikuandmeid, peavad uurimise ja kaebuste lahendamise küsimustes aru andma otse kõnealustele asutustele.

c) Organisatsioonid on kohustatud kaebusi lahendama ning järgima I lisas sätestatud tingimusi juhul, kui üksikisik soovib tugineda siduvale vahekohtuotsusele, olles sellekohase teate saatnud kõnealusele organisatsioonile ning järgides menetluseeskirju ja I lisas sätestatud tingimusi.

d) Andmete edastamise puhul on andmekaitseraamistikuga Privacy Shield ühinenud organisatsioon vastutav nende isikuandmete töötlemise eest, mille ta saab andmekaitseraamistiku Privacy Shield tingimustel ja edastab seejärel kolmandale osapoolele, kes tegutseb tema nimel tema esindajana. Andmekaitseraamistikuga Privacy Shield ühinenud organisatsioon jääb põhimõtete kohaselt ka siis vastutavaks, kui tema esindaja töötleb asjaomaseid isikuandmeid viisil, mis ei ole kooskõlas põhimõtetega, välja arvatud juhul, kui organisatsioon tõendab, et ta ei ole vastutav sündmuse eest, mille tagajärjel kahju tekkis.

e) Kui FTC või kohus otsustavad, et organisatsioon ei järgi põhimõtteid, peab organisatsioon avalikustama kõik asjakohased andmekaitseraamistikuga Privacy Shield seotud ja FTCle esitatud vastavus- või hindamisaruannete osad konfidentsiaalsusnõuetega kooskõlas olevas ulatuses. Ministeerium on loonud andmekaitseasutuste jaoks kontaktpunkti, kuhu need võivad pöörduda mis tahes andmekaitseraamistikuga Privacy Shield ühinenud organisatsioonide poolt põhimõtete järgimata jätmisega seotud probleemide puhul. FTC vaatab esmajärjekorras läbi ministeeriumi ja ELi asutuste poolt esitatud kaebused põhimõtete mittejärgimise kohta ning vahetab õigeaegselt teavet kaebuse kohta selle esitanud asutusega, järgides kehtivaid konfidentsiaalsuspiiranguid.

III. TÄIENDAVAD PÕHIMÕTTED

1. **Tundlikud andmed**

a) Organisatsioon ei ole kohustatud hankima kinnitavat selgesõnalist nõusolekut (opt in) tundlike andmete töötlemiseks, kui see:

i) toimub andmesubjekti või teise isiku elulistes huvides;

ii) on vajalik seadusest tuleneva nõude või kaitse tuvastamiseks;

iii) on vajalik meditsiiniabi või diagnoosi andmiseks;

iv) viiakse läbi fondi, ühenduse või muu poliitilise, filosoofilise, religioosse või ametiühingusuunitlusega mittetulundusasutuse õiguspärase tegevuse raames ning tingimusel, et töötlemine seondub ainult asjaomase asutuse liikmete või isikutega, kellel on kõnealuse asutusega korrapärased kontaktid tema eesmärkide tõttu, ning tingimusel, et andmeid ei avalikustata kolmandatele isikutele ilma andmesubjektide nõusolekuta;

v) on organisatsioonile vajalik kohustuste täitmiseks tööõiguse valdkonnas või

vi) on seotud üksikisiku poolt avalikult teatavaks tehtud andmetega.

2. **Erandid ajakirjandusele**

a) Võttes arvesse ajakirjandusvabaduse põhiseaduslikku kaitset Ameerika Ühendriikides ning direktiivi erandit ajakirjanduslikule materjalile ja juhul, kui Ameerika Ühendriikide konstitutsiooni esimeses paranduses sisalduvad vaba ajakirjanduse õigused puutuvad kokku eraelu puutumatuse kaitse huvidega, lähtutakse selliste huvide tasakaalustamisel esimesest parandusest, kui on tegemist Ameerika Ühendriikide isikute või organisatsioonidega.

b) Andmekaitseraamistiku Privacy Shield põhimõtete nõudeid ei kohaldata ajakirjandusliku materjali trükis või eetris avaldamiseks või muul moel avalikuks edastamiseks kogutud isikuandmete suhtes, sõltumata sellest, kas neid kasutatakse või mitte, samuti massiteabevahendite arhiivide levitatavast varem avaldatud materjalist leitud teabe suhtes.

3. **Sekundaarvastutus**

a) Internetiteenuste pakkujad (ISPd), telekommunikatsioonifirmad või muud organisatsioonid ei ole andmekaitseraamistiku Privacy Shield põhimõtete alusel vastutavad, kui nad teise organisatsiooni nimel vaid edastavad, marsruudivad või puhverdavad andmeid. Nii nagu direktiiv, ei tekita ka programm Privacy Shield ise sekundaarvastutust. Kui organisatsioon tegutseb kõigest kolmandate isikute edastatavate andmete kanalina ning ei määratle nende isikuandmete eesmärke ja töötlemisvahendeid, ei ole ta selles ulatuses vastutav.

4. **Nõuetekohane hoolsus ja auditite läbiviimine**

a) Audiitorite ja investeerimispankurite tegevus võib hõlmata isikuandmete töötlemist ilma üksikisiku teadmise või nõusolekuta. See on lubatud teate, valikuvõimaluse ja juurdepääsu põhimõtete alusel allpool kirjeldatud tingimustel.

b) Aktsiaseltsid ja osaühingud, sealhulgas andmekaitseraamistikuga Privacy Shield ühinenud organisatsioonid, kuuluvad regulaarsele auditeerimisele. Selliseid auditeid, eriti neid, mille käigus kontrollitakse potentsiaalseid õiguserikkumisi, võib enneaegne avalikustamine ohtu seada. Samuti peab andmekaitseraamistikuga Privacy Shield ühinenud organisatsioon, kes on seotud võimaliku ühinemise või ülevõtmisega, teostama või läbima nõuetekohase hoolsuse kontrolli. Sellega kaasneb tihti isikuandmete, näiteks juhtivate ja olulisemate töötajate kohta andmete kogumine ja töötlemine. Enneaegne avalikustamine võib tehingut takistada või isegi olla vastuolus väärtpaberite suhtes kohaldatavate õigusaktidega. Nõuetekohase hoolsusega tegelevatel investeerimispankuritel ja advokaatidel või audiitoritel, kes auditi läbi viivad, on lubatud andmeid töödelda ilma üksikisiku teadmiseta ainult sellises ulatuses ja ajavahemikul, mis on vajalik seadusest või avalikust huvist tulenevatel ning muudel juhtudel, mil nende põhimõtete rakendamine kahjustaks organisatsiooni õigustatud huve. Selliste õigustatud huvide hulka kuuluvad organisatsioonide kohustuste ja raamatupidamistoimingute teostamise vastavuse jälgimine ning konfidentsiaalsusvajadus, mis on seotud võimalike omandamiste, ühinemiste, ühisettevõtete või investeerimispankurite või audiitorite poolt teostatavate muude sarnaste toimingutega.

5. **Andmekaitseasutuste roll**

a) Organisatsioonid täidavad oma kohustust teha koostööd Euroopa andmekaitseasutustega, nagu allpool on kirjeldatud. Programmi Privacy Shield alusel peavad EList isikuandmeid saavad Ameerika Ühendriikide organisatsioonid kohustuma rakendama tõhusaid mehhanisme tagamaks vastavust andmekaitseraamistiku Privacy Shield põhimõtetele. Täpsemalt peavad osalevad organisatsioonid tagama, vastavuses kaebuste menetlemise, täitmise tagamise ja vastutuse põhimõttega, järgmise: a) i) kaebuste esitamise võimalus üksikisikutele, keda andmed puudutavad; a) ii) kontrollimeetmed veendumaks, et kinnitused ja väited, mida nad on oma puutumatusnormide kohta esitanud, vastavad tõele; a) iii) kohustuse heastada põhimõtete järgimata jätmisest tekkivad probleemid ning tagajärjed sellistele organisatsioonidele. Organisatsioon võib vastata kaebuste menetlemise, täitmise tagamise ja vastutuse põhimõtte punkti a alapunktidele i ja iii, kui ta järgib siin sätestatud nõudeid koostöö kohta andmekaitseasutustega.

b) Organisatsioon kohustub tegema koostööd andmekaitseasutustega, kui ta avaldab oma andmekaitseraamistiku Privacy Shield põhimõtete järgimise kinnituses kaubandusministeeriumile (vt täiendav põhimõte ise kinnitamise kohta), et organisatsioon:

i) soovides järgida programmi Privacy Shield kaebuste menetlemise, täitmise tagamise ja vastutuse põhimõtte punkti a alapunktide i ja iii nõudeid, kohustub tegema koostööd andmekaitseasutustega;

ii) teeb koostööd andmekaitseasutustega programmi Privacy Shield alusel esitatud kaebuste uurimisel ja lahendamisel ning

iii) järgib andmekaitseasutuste nõuandeid, kui andmekaitseasutused leiavad, et organisatsioon peab programmi Privacy Shield põhimõtete järgimiseks astuma konkreetseid samme, sealhulgas meetmed põhimõtete järgimata jätmise tõttu üksikisikutele tekitatud kahju heastamiseks või hüvitamiseks, ja esitab andmekaitseasutustele kirjaliku kinnituse selliste meetmete võtmise kohta.

c) Andmekaitseasutuste paneelide tegevus

i) Andmekaitseasutuste koostöö toimub teabe ja nõuannete vormis järgmiselt:

1. Andmekaitseasutuste nõuanded edastatakse Euroopa Liidu tasemel moodustatud andmekaitseasutuste mitteametliku paneeli kaudu, mis muu hulgas aitab tagada ühtlustatud ja ühtse lähenemise.

2. Paneel nõustab Ameerika Ühendriikide organisatsioone üksikisikute lahendamata kaebuste asjus, mis on seotud EList programmi Privacy Shield alusel edastatud isikuandmete käsitlemisega. Nõustamise eesmärgiks on tagada andmekaitseraamistiku Privacy Shield põhimõtete õige kohaldamine ning see hõlmab andmekaitseasutuste poolt sobilikuks peetavaid heastamisvahendeid asjakohas(t)ele isiku(te)le.

3. Paneel annab nõu vastuseks asjaomaste organisatsioonide taotluste ja/või otse üksikisikutelt saadud kaebustele organisatsioonide vastu, kes on kohustunud andmekaitseasutustega programmi Privacy Shield eesmärkidel koostööd tegema, julgustades selliseid üksikisikuid eelkõige kasutama sisemisi kaebuste käsitlemise menetlusi, mida organisatsioon võib pakkuda, ning vajadusel neid selles aidates.

4. Nõuanded väljastatakse pärast seda, kui kummalgi vaidluse poolel on olnud mõistlik võimalus esitada selgitused ja soovitud tõendid. Paneel püüab väljastada nõuande nii kiiresti, kui seda võimaldab nõue järgida häid menetlustavasid. Reeglina püüab paneel nõuande väljastada 60 päeva jooksul pärast kaebuse või taotluse saamist ning võimaluse korral kiiremini.

5. Paneel avalikustab temale läbivaatamiseks esitatud kaebuste tulemused, kui peab seda vajalikuks.

6. Nõuannete väljastamisest läbi paneeli ei tulene mitte mingisugust vastutust paneelile ega üksikutele andmekaitseasutustele.

ii) Nagu eespool märgitud, peavad sellise vaidluste lahendamise võimaluse valivad organisatsioonid kohustuma andmekaitseasutuste nõuandeid järgima. Kui organisatsioon ei järgi nõuannet 25 päeva jooksul pärast selle väljastamist ning ei ole viivitust rahuldavalt põhjendanud, teavitab paneel oma kavatsusest saata materjal edasi kas föderaalsele kaubanduskomisjonile, transpordiministeeriumile või muule Ameerika Ühendriikide föderaalsele või valitsusasutusele, millel on seadusest tulenevad volitused võtta sunnimeetmeid pettuse või valeandmete esitamise korral, või järeldada, et koostöölepingut on tõsiselt rikutud ning see loetakse seetõttu kehtetuks. Viimasel juhul teavitab paneel Ameerika Ühendriikide kaubandusministeeriumi nõutavate muutuste sisseviimiseks andmekaitseraamistikuga Privacy Shield ühinenute nimekirja. Andmekaitseasutustega koostöö kohustuse mittetäitmist, samuti andmekaitseraamistiku Privacy Shield põhimõtete mittejärgimist käsitletakse pettusena föderaalse kaubanduskomisjoni seaduse (FTC Act) paragrahvi 5 või muu sarnase põhimääruse alusel.

d) Organisatsioon, kes soovib oma programmi Privacy Shield soodustusi laiendada EList töösuhte kontekstis edastatavatele personali isikuandmetele, peab kohustuma tegema koostööd andmekaitseasutustega nende andmete osas (vt täiendav põhimõte personali isikuandmete kohta).

e) Sellise võimaluse valivad organisatsioonid peavad maksma aastatasu paneeli tegevuskulude katteks ning neilt võidakse täiendavalt paluda võimalike tõlkekulude tasumist, mis tulenevad nende vastu suunatud taotluste või kaebuste läbivaatamisest. Aastatasu ei ületa 500 USA dollarit ning on väiksemate äriühingute jaoks väiksem.

6. **Põhimõtete järgimise kinnitamine**

a) Programmi Privacy Shield soodustused on tagatud alates kuupäevast, mil ministeerium lisab organisatsiooni esitatud kinnituse andmekaitseraamistikuga Privacy Shield ühinenute nimekirja, peale seda, kui on kontrollinud, et kinnitus on täielik.

b) Andmekaitseraamistiku Privacy Shield põhimõtete järgimise kinnitamiseks peavad organisatsioonid andma kaubandusministeeriumile üle kinnituse, millele on alla kirjutanud vastutav isik programmiga Privacy Shield ühineva organisatsiooni nimel ning mis sisaldab vähemalt järgmist teavet:

i) organisatsiooni nimi, postiaadress, e-posti aadress, telefoni- ja faksinumbrid;

ii) organisatsiooni tegevuse kirjeldus EList saadavate isikuandmetega seoses ning

iii) organisatsiooni puutumatusnormide kirjeldus selliste isikuandmete puhul, sealhulgas:

1. kui organisatsioonil on olemas avalik veebisait, siis veebiaadress, kus on kättesaadavad tema puutumatusnormid või kui organisatsioonil ei ole avalikku veebisaiti, siis teave selle kohta, kus avalikkusel on võimalik tema puutumatusnormidega tutvuda;

2. rakendamise kuupäev;

3. kontaktandmed kaebuste, juurdepääsunõuete ning muude andmekaitseraamistiku Privacy Shield alusel tekkivate küsimuste käsitlemiseks;

4. konkreetne täitevasutus, millel on pädevus läbi vaadata mis tahes nõudeid organisatsiooni vastu seoses võimalike kõlvatute tavade või pettusega ja eraelu puutumatusele kohaldatavate (ning põhimõtetes või tulevases põhimõtete lisas loetletud) õigusnormide rikkumisega;

5. kõikide eraelu puutumatuse programmide nimed, milles organisatsioon osaleb;

6. kontrollimeetod (nt sisemine, kolmas isik) (vt täiendavat põhimõtet kontrolli kohta) ja

7. sõltumatu kaebuste menetlemise mehhanism, mida saab kasutada lahendamata kaebuste uurimiseks.

c) Organisatsioon, kes soovib programmi Privacy Shield soodustusi laiendada EList töösuhte kontekstis edastatavatele töötajate isikuandmetele, võib seda teha sellise täitevasutuse olemasolul, kes on loetletud põhimõtetes või tulevases põhimõtete lisas ja kellel on pädevus võtta vastu töötajate isikuandmetest tulenevaid nõudeid organisatsiooni vastu. Lisaks peab organisatsioon sellele oma vastavust kinnitavas esildises viitama ja teatama, et kohustub tegema koostööd asjaomase ELi asutuse või asutustega täiendavate personali isikuandmete kohta käivate ja andmekaitseasutuste rolli põhimõtete alusel, vastavalt sellele, kumb on kohaldatav, ning järgima nimetatud asutuste nõuandeid. Organisatsioon peab esitama ministeeriumile ka koopia oma puutumatus-normidest ning teatama, kus need on tutvumiseks kättesaadavad töötajatele, keda need puudutavad.

d) Ministeerium peab andmekaitseraamistikuga Privacy Shield ühinenute nimekirja organisatsioonide kohta, kes esitavad tervikliku esildise kinnituse kohta, tagades seeläbi programmi Privacy Shield soodustuste kättesaadavuse, ning uuendab kõnealust nimekirja iga-aastaste taaskinnitusi sisaldavate esildiste ja täiendavate vaidluste lahendamise ja täitmise tagamise põhimõtete kohaste teavituste alusel. Sellised kinnitust sisaldavad esildised tuleb esitada vähemalt kord aastas. vastasel juhul kustutatakse organisatsioon andmekaitseraamistikuga Privacy Shield ühinenute nimekirjast ja kaasnevaid soodustusi enam ei anta. Nii andmekaitseraamistikuga Privacy Shield ühinenute nimekiri kui ka organisatsoonide poolt üle antavad kinnitused tehakse avalikkusele kättesaadavaks. Kõik organisatsioonid, kelle ministeerium lisab andmekaitseraamistikuga Privacy Shield ühinenute nimekirja,

peavad ka oma asjakohastes avalikustatud puutumatusnormides deklareerima, et järgivad andmekaitseraamistiku Privacy Shield põhimõtteid. Kui puutumatusnormid on kättesaadavad veebis, siis peab seal sisalduma ka hüperlink ministeeriumi andmekaitseraamistiku Privacy Shield veebisaidile, samuti hüperlink lahendamata kaebuste uurimiseks ettenähtud sõltumatu kaebuste menetlemise mehhanismi veebisaidile või kaebuse vormile.

e) Eraelu puutumatuse põhimõtted rakenduvad koheselt peale kinnitamist. Tunnistades, et põhimõtted hakkavad mõjutama ärisidemeid kolmandate isikutega, viivad andmekaitseraamistiku Privacy Shield põhimõtete järgimist kinnitanud organisatsioonid nii kiiresti kui võimalik esimese kahe kuu jooksul peale raamistiku jõustumist oma ärisidemed kolmandate osapooltega vastavusse andmete edasisaatmise põhimõttega, ent mitte mingil juhul hiljem kui üheksa kuud peale kuupäeva, mil nad kinnitasid Privacy Shield põhimõtete järgimist. Sel vahepealsel perioodil, kui organisatsioonid edastavad andmeid kolmandale osapoolele, järgivad nad (i) teate ja valikuvõimaluse põhimõtteid ja (ii) kui isikuandmeid edastatakse kolmandale isikule, kes on esindaja, teevad nad kindlaks, et esindaja on kohustatud tagama kaitse vähemalt põhimõtetes nõutaval tasemel.

f) Organisatsioon peab järgima andmekaitseraamistiku Privacy Shield põhimõtteid kõikide EList andmekaitseraamistikule Privacy Shield tuginedes saadud isikuandmete suhtes. Kohustus järgida andmekaitseraamistiku Privacy Shield põhimõtteid ei ole ajaliselt piiratud organisatsiooni poolt programmi Privacy Shield soodustuste kasutamise ajal saadavate andmete osas. Kohustus tähendab, et organisatsioon jätkab põhimõtete kohaldamist selliste andmete suhtes nii kaua, kuni organisatsioon neid säilitab, kasutab või avalikustab, isegi kui ta seejärel mis tahes põhjusel programmist Privacy Shield lahkub. Organisatsioon, kes lahkub programmist Privacy Shield, ent soovib programmi raames saadud andmeid säilitada, peab kinnitama ministeeriumile igal aastal põhimõtete järgimist või teabele „piisava“ kaitse tagamist teiste heakskiidetud meetoditega (nt kasutades lepingut, mis sisaldab täies ulatuses asjakohaseid standardseid Euroopa Komisjoni poolt heaks kiidetud lepingusätteid); vastasel korral peab organisatsioon teabe tagastama või kustutama. Programmist Privacy Shield lahkuv organisatsioon peab eemaldama kõikidest asjakohastest puutumatusnormidest kõik viited andmekaitseraamistikule Privacy Shield, mis osutavad, et organisatsioon jätkab aktiivselt programmis Privacy Shield osalemist ja omab õigust sellest tulenevatele soodustustele.

g) Organisatsioon, mis lakkab eksisteerimast eraldiseisva üksusena ühinemise või ülevõtmise tõttu, peab sellest eelnevalt teavitama ministeeriumi. Teates tuleks ka märkida, kas ühendav üksus või ühinemise tulemuse tekkiv üksus i on kohustatud edasi järgima andmekaitseraamistiku Privacy Shield põhimõtteid ülevõtmist või ühinemist reguleerivate õigusnormide alusel või ii valib andmekaitseraamistiku Privacy Shield põhimõtetest kinnipidamise kinnitamise või rakendab muid tagatisi, näiteks kirjalikke lepinguid, mis tagavad andmekaitseraamistiku Privacy Shield põhimõtete järgimise. Kui ei kohaldata ei punkti i ega ii, tuleb andmekaitseraamistiku Privacy Shield alusel saadud andmed viivitamatult kustutada.

h) Kui organisatsioon lahkub mingil põhjusel programmist Privacy Shield, peab ta eemaldama kõik avaldused, mis osutavad, et organisatsioon jätkab programmis Privacy Shield osalemist või omab õigust sellest tulenevatele soodustustele. ELi-USA andmekaitseraamistikuga Privacy Shield põhimõtete järgimist tõendav tähis, kui seda kasutatakse, tuleb samuti eemaldada. Organisatsiooni poolt avalikkusele valeandmete esitamise korral andmekaitseraamistiku Privacy Shield põhimõtete järgimise kohta võib FTC või muu asjakohane valitsusasutus süüdistuse esitada. Ministeeriumile valeandmete esitamise korral võidakse kohaldada valeandmete seadust (False Statements Act, 18 U.S.C. § 1001).

7. **Kontrollimine**

a) Organisatsioonid peavad ette nägema kontrollimeetmed tõendamaks, et kinnitused ja väited, mida nad oma andmekaitseraamistiku Privacy Shield põhimõtete järgmise tavade kohta eraelu puutumatuse osas on esitanud, vastavad tõele ja asjaomaste tavade rakendamine vastab esitatule ning on kooskõlas andmekaitseraamistiku Privacy Shield põhimõtetega.

b) Kaebuste esitamise, täitmise tagamise ja vastutuse põhimõtte kontrollinõude järgimiseks peab organisatsioon selliseid tunnistusi ja väiteid kontrollima enesehindamise või välise vastavuskontrolli kaudu.

c) Enesehindamismeetodi korral peab selline kontroll näitama, et organisatsiooni poolt avalikustatud puutumatusnormid EList saadavate isikuandmete osas on täpsed, terviklikud, selgelt esitatud, täielikult rakendatud ja kättesaadavad. Samuti peab kontroll näitama, et organisatsiooni puutumatusnormid vastavad andmekaitseraamistiku Privacy Shield põhimõtetele; et üksikisikuid on teavitatud sisemisest kaebuste lahendamise korrast ja sõltumatutest mehhanismidest, mille kaudu on võimalik nende kaebusi menetleda; et on

paika pandud kord töötajate koolitamiseks selle rakendamise suhtes ja nende suhtes kohaldatav distsiplinaarmenetlus juhul, kui nad seda ei järgi; ning et on paika pandud sisekord perioodiliste objektiivsete kontrollide korraldamiseks eespool toodule vastavuse suhtes. Enesehindamise kinnitusele peaks alla kirjutama vastutav isik või organisatsiooni muu volitatud esindaja vähemalt kord aastas ning see peaks olema nõudmisel kättesaadav üksikisikutele või seoses põhimõtete järgimata jätmise uurimise või sellekohase kaebusega

d) Kui organisatsioon on valinud välise vastavuskontrolli, peab selline kontroll näitama, et organisatsiooni poolt avalikustatud puutumatusnormid EList saadavate isikuandmete osas vastavad andmekaitseraamistiku Privacy Shield põhimõtetele, et neid järgitakse ja et üksikisikuid on teavitatud kaebuste esitamise mehhanismidest. Kontrolliviisideks võivad piiranguta olla auditeerimine, juhuslik kontroll, „peibutiste" kasutamine või vajaduse korral tehnoloogilised vahendid. Välise vastavuskontrolli eduka läbiviimise kinnitusele peab alla kirjutama kas kontrollija või vastutav isik või organisatsiooni muu volitatud esindaja vähemalt kord aastas ning see peaks olema nõudmisel kättesaadav üksikisikutele või seoses põhimõtete järgimata jätmise uurimise või sellekohase kaebusega.

e) Organisatsioonid peavad säilitama oma dokumendid programmi Privacy Shield põhimõtete rakendamise kohta ja tegema need põhimõtete järgimata jätmise uurimise või sellekohase kaebuse korral nõudmisel kättesaadavaks kaebuste läbivaatamise eest vastutavale sõltumatule asutusele või asutusele, kel on pädevus kõlvatute tavade või pettuste uurimiseks. Organisatsioonid peavad viivitamata vastama ministeeriumi järelepärimistele ja muudele teabenõuetele, mis on seotud põhimõtete järgimisega organisatsiooni poolt.

8. **Juurdepääs**

a) Juurdepääsu põhimõtte rakendamine

i) Andmekaitseraamistiku Privacy Shield põhimõtete kohaselt on juurdepääsuõigus eraelu puutumatuse kaitse põhimine asjaolu. Eelkõige võimaldab see üksikisikutel kontrollida nende kohta säilitatavate andmete õigsust. Juurdepääsu põhimõte tähendab, et üksikisikutel on õigus:

1. saada organisatsioonilt kinnitus selle kohta, kas organisatsioon töötleb või ei töötle nendega seotud isikuandmeid ([1]);

2. saada sellist teavet, mille täpsust ja töötlemise õiguspärasust neil oleks võimalik kontrollida; ning

3. lasta andmed parandada, muuta või kustutada, kui need ei ole õiged või kui neid töödeldakse põhimõtteid rikkudes.

ii) Üksikisikud ei pea põhjendama oma isikuandmetele juurdepääsu taotlusi. Üksikisikute juurdepääsutaotlustele reageerimisel peaksid organisatsioonid esmajoones huvi tundma, mis nende taotluste esitamiseni üldse viis. Näiteks kui juurdepääsutaotlus on ebamäärane või laiaulatuslik, võib organisatsioon üksikisikuga alustada dialoogi, et taotluse põhjust paremini mõista ning vastavad andmed leida. Organisatsioon võiks uurida, millis(t)e organisatsiooni osa(de)ga üksikisik suhtles või milline on juurdepääsutaotluse aluseks olevate andmete (või nende kasutuse) laad.

iii) Kooskõlas juurdepääsu põhimõtte põhjapaneva tähtsusega peaksid organisatsioonid alati tegema heauskseid pingutusi juurdepääsu võimaldamiseks. Näiteks kui on vaja kaitsta konkreetseid andmeid ning neid on võimalik hõlpsasti eraldada muudest isikuandmetest, mille kohta on esitatud juurdepääsutaotlus, peaks organisatsioon kaitstud andmed eraldama ja muud andmed kättesaadavaks tegema. Kui organisatsioon otsustab, et juurdepääsu tuleb mingil konkreetsel juhul piirata, peab ta juurdepääsu taotlenud üksikisikule esitama selgituse, miks ta sellise otsuse tegi, ja teabe kontaktpunkti kohta täiendavate päringute saatmiseks.

b) Juurdepääsu võimaldamise tülikus või kulud

i) Õigust isikuandmetele juurde pääseda tohib piirata vaid erandlikel juhtudel, kui sellega rikutakse teiste isikute seaduslikke õigusi või kui juurdepääsu võimaldamise tülikus või kulud on asjaomasel juhul ebaproportsionaalsed ohuga üksikisiku eraelu puutumatusele. Kulud ja probleemid on olulised tegurid, mida tuleks arvesse võtta, kuid needd ei ole otsustavad tegurid juurdepääsu võimaldamise mõistlikkuse üle otsustamisel.

([1]) Organisatsioon peaks vastama üksikisikute päringutele, mis puudutavad isikuandmete töötlemise eesmärki, töödeldavate isikuandmete kategooriaid ning seda, kellele või millise kategooria saajatele isikuandmed avalikustatakse.

ii) Näiteks kui isikuandmeid kasutatakse otsuste tegemiseks, mis üksikisikut oluliselt mõjutavad (nt oluliste soodustuste nagu kindlustus, hüpoteeklaen või töökoha võimaldamine või sellest keeldumine), siis kooskõlas käesolevate täiendavate põhimõtete muude sätetega peab organisatsioon need andmed avalikustama ka siis, kui seda võimaldada on suhteliselt keeruline või kallis. Kui nõutavad isikuandmed ei ole tundlikud või neid ei kasutata otsuste tegemiseks, mis üksikisikut oluliselt mõjutavad, ent on kergesti kättesaadavad ja neile ei ole kulukas juurdepääsu võimaldada, peab organisatsioon võimaldama juurdepääsu sellistele andmetele.

c) Konfidentsiaalne äriinfo

i) Konfidentsiaalne äriinfo on andmed, mille avalikustamise vältimiseks organisatsioon on võtnud meetmed ja mille avalikustamine võiks aidata turul olevat konkurenti. Organisatsioonid võivad juurdepääsu võimaldamisest keelduda või seda piirata täies ulatuses, milles juurdepääsu võimaldamisel paljastuks organisatsiooni enda konfidentsiaalne äriinfo, näiteks organisatsiooni turundusjäreldused või -klassifikatsioonid, või mõne teise organisatsiooni konfidentsiaalne äriinfo, mille puhul kohaldatakse lepingulist konfidentsiaalsuskohustust.

ii) Kui konfidentsiaalset äriinfot on võimalik hõlpsasti eraldada muudest isikuandmetest, mille kohta on esitatud juurdepääsutaotlus, peaks organisatsioon eraldama konfidentsiaalse äriinfo ja mittekonfidentsiaalse info kättesaadavaks tegema.

d) Andmebaaside korraldus

i) Juurdepääsu võib organisatsioon võimaldada asjaomaste isikuandmete avalikustamise vormis ning üksikisiku juurdepääs organisatsiooni andmebaasile ei ole nõutav.

ii) Juurdepääs tuleb võimaldada ainult organisatsiooni poolt isikuandmete säilitamise ulatuses. Juurdepääsu põhimõttest endast ei teki kohustust isikuandmete faile hoida, säilitada, reorganiseerida või restruktureerida.

e) Mis juhul võib juurdepääsu piirata

i) Kuna organisatsioonid peavad alati tegema heauskselt jõupingutusi üksikisikutele juurdepääsu võimaldamiseks nende isikuandmetele, on asjaolud, mille puhul organisatsioonid võivad juurdepääsu piirata, piiratud ning kõik juurdepääsu piiramise põhjused peavad olema konkreetsed. Direktiivi alusel võib organisatsioon piirata andmetele juurdepääsu ulatuses, milles avalikustamine võib häirida olulise vastukaaluga avalike huvide kaitset, näiteks riigi julgeolekut; riigikaitset; avalikku julgeolekut. Lisaks võib juurdepääsu võimaldamisest keelduda, kui isikuandmeid töödeldakse üksnes teaduslikel või statistilistel eesmärkidel. Muud põhjused juurdepääsu võimaldamisest keeldumiseks või selle piiramiseks on:

1. see raskendab õigusnormide täitmist või jõustamist või hagi aluseid, sealhulgas seaduserikkumiste ennetamist, uurimist või avastamist või õigust õiglasele kohtumõistmisele;

2. avalikustamine kahjustab teiste isikute seaduslikke õigusi või olulisi huve;

3. see toob kaasa õigusliku või muu ametialase privileegi või kohustuse rikkumise;

4. see kahjustab töötajate julgeolekukontrolli või töövaidluste käsitlemist või on seotud töötajate töökohtade planeerimise ja äriühingute ümberkorraldamisega või

5. see kahjustab heakvaliteedilise juhtimisega seotud järelevalve, kontrolli või regulatiivtoimingute teostamiseks või organisatsiooni tulevasteks või käimasolevateks läbirääkimisteks vajalikku konfidentsiaalsust;

ii) Erandit taotlev organisatsioon peab tõendama selle vajalikkust ning teatama üksikisikutele juurdepääsu piiramise põhjused ning kontaktpunkti, kuhu täiendavate järelepärimistega pöörduda.

f) Õigus saada kinnitus ning tasu nõudmine juurdepääsu võimaldamise kulude katteks

i) Üksikisikul on õigus nõuda kinnitust, kas asjaomane organisatsioon omab või ei oma tema kohta käivaid isikuandmeid. Üksikisikul on samuti õigus, et talle tehtaks teatavaks tema kohta käivad isikuandmed. Organisatsioon võib nõuda tasu, mis ei ole ülemäära suur.

ii) Tasu nõudmine võib olla põhjendatud, näiteks kui juurdepääsu taotlemine on selgelt ülemäärane, eriti kui nõudmisi esitatakse korduvalt.

iii) Juurdepääsu võimaldamisest ei tohi keelduda kulude ettekäändel, kui üksikisik nõustub kulud korvama.

g) Korduvad või kiuslikud juurdepääsutaotlused i.

Organisatsioon võib seada mõistlikud piirangud selle kohta, mitmele ühe üksikisiku juurdepääsutaotlusele nad teatava ajavahemiku vältel vastavad. Selliseid piiranguid seades tuleks organisatsioonil kaaluda niisuguseid tegureid nagu andmete uuendamise sagedus, andmete kasutamise eesmärk ja andmete laad.

h) Petturlikud juurdepääsutaotlused

Organisatsioon ei pea juurdepääsu võimaldama, kui talle ei esitata piisavalt andmeid taotluse esitanud isiku tuvastamiseks.

i) Ajaraamistik vastuste andmiseks

Organisatsioonid peaksid vastama juurdepääsutaotlustele mõistliku aja jooksul, mõistlikul viisil ning vormis, mis on üksikisikule kergesti arusaadav. Andmesubjektidele regulaarsete ajavahemike järel teavet andev organisatsioon võib rahuldada individuaalse juurdepääsutaotluse tema poolt regulaarse teabe avaldamise käigus, kui see ei põhjusta ülemäärast viivitust.

9. **Personaliandmed**

a) Hõlmatus andmekaitseraamistikuga Privacy Shield

i) Kui ELis asuv organisatsioon edastab töösuhte kontekstis kogutud isikuandmeid oma (endiste või praeguste) töötajate kohta Ameerika Ühendriikides asuvale programmis Privacy Shield osalevale ema- või sidusettevõtjale või sõltumatule teenuse osutajale, laienevad edastamisele programmi Privacy Shield soodustused. Sellisel juhul allus andmete kogumine ja töötlemine enne edastamist selle EL liikmesriigi siseriiklikule õigusele, kus need koguti, ning nende edastamisel tuleb järgida kõiki tingimusi või piiranguid selle õiguse alusel.

ii) Andmekaitseraamistiku Privacy Shield põhimõtted on asjakohased ainult eraldi tuvastatud või tuvastatavate registriandmete edastamisel või neile juurdepääsul. Statistiline aruandlus, mis tugineb personali koondandmetele ja ei sisalda isikuandmeid, või anonüümsete andmete kasutamine ei põhjusta eraelu puutumatuse kaitse alaseid probleeme.

b) Teate ja valikuvõimaluse põhimõtete rakendamine

i) Ameerika Ühendriikide organisatsioon, mis on saanud töötajate kohta andmeid EList programmi Privacy Shield alusel, võib seda avalikustada kolmandatele osapooltele või erinevatel eesmärkidel ainult kooskõlas teate ja valikuvõimaluse põhimõtetega. Näiteks kui organisatsioon kavatseb kasutada töösuhte kaudu kogutud isikuandmeid töösuhtega mitteseotud eesmärkidel, näiteks turunduskommunikatsioonis, peab Ameerika Ühendriikide organisatsioon eelnevalt pakkuma nõutavat valikuvõimalust üksikisikutele, keda see puudutab, välja arvatud juhul, kui nad juba on andnud loa teavet sellisel eesmärgil kasutada. Selline kasutus ei tohi olla vastuolus eesmärkidega, milleks isikuandmeid algselt koguti või milleks üksikisik algselt loa andis. Lisaks ei tohi selliseid valikuvõimalusi kasutada töövõimaluste piiramiseks ega rakendada selliste töötajate suhtes karistusi.

ii) Tuleb märkida, et mõnedest Euroopa Liidu liikmesriikidest andmete edastamisele ette nähtud teatavad üldiselt rakendatavad tingimused võivad välistada selliste andmete kasutamise muudel eesmärkidel isegi pärast edastamist EList välja ning selliseid tingimusi tuleb täita.

iii) Lisaks peaksid tööandajad tegema mõistlikke pingutusi, et tulla vastu töötajate eraelu puutumatuse alastele eelistustele. See võib hõlmata näiteks isikuandmetele juurdepääsu piiramist, teatud andmete juurest nimede kustutamist või koodide või pseudonüümide kasutamist, kui asjakohaseks eesmärgiks ei vajata tegelikke nimesid.

iv) Selles ulatuses ja ajavahemikuks, mis on vajalik organisatsiooni teovõime kahjustamise vältimiseks edutamiste, ametisse nimetamiste või muude sarnaste töösuhteid puudutavate otsuste langetamiseks, ei pea organisatsioon teadet ja valikuvõimalust pakkuma.

c) Juurdepääsu põhimõtte rakendamine

Juurdepääsu käsitlevad täiendavad juurdepääsu põhimõtted annavad juhiseid põhjuste kohta, mis võivad õigustada juurdepääsu võimaldamisest keeldumist või selle piiramist töötajatega seoses. Muidugi peavad tööandjad Euroopa Liidus järgima kohalikke õigusnorme ning tagama Euroopa Liidu töötajatele juurdepääsu sellistele andmetele, mida nõuab seadus nende koduriigis, olenemata andmete töötlemise ja salvestamise asukohast. Programmi Privacy Shield kohaselt teeb selliseid andmeid Ameerika Ühendriikides töötlev organisatsioon sellise juurdepääsu võimaldamisel koostööd kas otse või läbi EL tööandja.

d) Jõustamine

i) Kui isikuandmeid kasutatakse ainult töösuhte kontekstis, jääb esmane vastutus töötaja ees andmetega seoses ELis asuvale organisatsioonile. Sellest järeldub, et kui Euroopa töötajad esitavad kaebusi oma andmekaitse alaste õiguste rikkumise kohta ja neid ei rahulda sisekontrolli, kaebuse esitamise ja edasikaebamise kord (või mis tahes rakendatav töövaidluste lahendamise kord kokkuleppel ametiühinguga), tuleks nad suunata osariigi või riigi andme- või töökaitseasutusse jurisdiktsioonis, kus töötajad töötavad. See hõlmab ka juhtumeid, kui väidetava isikuandmete väärkasutuse eest vastutab Ameerika Ühendriikide organisatsioon, kes on saanud andmed tööandjalt, ning seetõttu on tegemist andmekaitseraamistiku Privacy Shield põhimõtete väidetava rikkumisega. See on kõige tõhusam viis kohaliku tööõigusega ja töölepingutega ning andmekaitseseadusega kehtestatud, üksteisega sageli kattuvate õiguste ja kohustuste käsitlemiseks.

ii) Programmis Privacy Shield osalev Ameerika Ühendriikide organisatsioon, kes kasutab EL personaliandmeid, mis edastatakse Euroopa Liidust töösuhte kontekstis, ja kes soovib selliseid edastusi sooritada programmi Privacy Shield alusel, peab niisiis sellisel juhul kohustuma tegema uurimisalast koostööd EL pädevate asutustega ning järgima nende nõuandeid.

e) Kolmandale isikule andmete edastamise eest vastutuse põhimõtte rakendamine

Programmis Privacy Shield osaleva organisatsiooni juhuslikeks töösuhtega seotud operatiivvajadusteks võib raamistikuga hõlmatud isikuandmed, nagu näiteks väikese arvu töötajate isikuandmed lennupiletite broneerimiseks, hotellitoa või kindlustuse tellimiseks, edastada vastutavale töötlejale ilma juurdepääsu põhimõtte rakendamiseta või vastutava töötlejaga, kes on kolmas isik, lepingut sõlmimata, mis tavaliselt on nõutav andmete kolmandale isikule edastamise põhimõtte kohaselt, eeldusel, et programmis Privacy Shield osalev organisatsioon on järginud teate ja valikuvõimaluse põhimõtteid.

10. **Kohustuslikud lepingud andmete edastamiseks kolmandale isikule**

a) Lepingud andmete töötlemise kohta

i) Kui isikuandmed edastatakse EList Ameerika Ühendriikidesse üksnes töötlemise eesmärgil, on selleks vaja lepingut, olenemata sellest, et volitatud töötleja osaleb programmis Privacy Shield.

ii) Euroopa Liidu vastutavad töötlejad peavad alati lepingu sõlmima, kui edastamine toimub üksnes töötlemise eesmärgil, olenemata sellest, kas töötlemine toimub ELis või väljaspool seda ning kas volitatud töötleja osaleb või ei osale programmis Privacy Shield. Lepingu eesmärgiks on tagada, et volitatud töötleja:

1. tegutseb üksnes vastutava töötleja suuniste alusel;

2. rakendab vajalikke tehnilisi ja organisatsioonilisi meetmeid kaitsmaks isikuandmeid juhusliku või ebaseadusliku hävitamise või juhusliku kaotsimineku, muutmise, ebaseadusliku avalikustamise või juurdepääsu eest, ja saab aru, kas andmete edastamine on lubatud; ning

3. võttes arvesse töötlemise laadi, abistab vastutavat töötlejat sellistele üksikisikutele vastamisel, kes kasutavad oma põhimõtete kohaseid õigusi.

iii) Kuna programmis Privacy Shield osalejad tagavad piisava kaitse, ei vaja üksnes töötlemise eesmärgil sõlmitavad lepingud programmis Privacy Shield osalejatega eelnevat luba (või selline luba antakse Euroopa Liidu liikmesriikide poolt automaatselt), mida nõutaks programmis Privacy Shield mitteosalevate või muul põhjusel piisavat kaitset mittetagavate vastuvõtjate puhul.

b) Andmete edastamine kontrollitavate äriühingute või üksuste grupis

Kui isikuandmeid edastatakse kahe vastutava töötleja vahel kontrollitavate äriühingute või üksuste grupis, ei ole kolmandale isikule andmete edastamise eest vastutuse põhimõtte kohaselt alati tarvis lepingut sõlmida. Vastutavad töötlejad kontrollitavate äriühingute või üksuste grupis võivad edastada andmeid, tuginedes muudele dokumentidele, nagu näiteks ELi kohustuslikud eeskirjad äriühingutele või muudele grupisisestele vahenditele (nt vastavuse ja kontrolli programmid), tagades jätkuvalt põhimõtete kohase isikuandmete kaitse. Kõnealuste edastamiste puhul jääb andmekaitseraamistikuga Privacy Shield ühinenud organisatsioon vastutavaks põhimõtete järgimise eest.

c) Andmete edastamine vastutavate töötlejate vahel

Vastutavate töötlejate vaheliste edastamiste puhul ei pea vastutav töötleja, kes on saaja, olema andmekaitseraamistikuga Privacy Shield ühinenud organisatsioon või omama sõltumatut kaebuste menetlemise mehhanismi. Andmekaitseraamistikuga Privacy Shield ühinenud organisatsioon peab sõlmima saajaga, kes on kolmandast isikust vastutav töötleja, lepingu, millega tagatakse andmekaitseraamistiku Privacy Shield tingimustega samal tasemel kaitse, välja arvatud nõue, et kolmandast isikust vastutav töötleja peab olema andmekaitseraamistikuga Privacy Shield ühinenud organisatsioon või omama sõltumatut kaebuste menetlemise mehhanismi, juhul kui ta teeb kättesaadavaks võrdväärse mehhanismi.

11. **Vaidluste lahendamine ja täitmise tagamine**

a) Kaebuste menetlemise, täitmise tagamise ja vastutuse põhimõttes sätestatakse nõuded andmekaitseraamistiku Privacy Shield täitmise tagamiseks. Põhimõtte punkti a alapunkti ii nõuete täitmine on sätestatud täiendavas põhimõttes kontrolli kohta. Täiendav põhimõte käsitleb punkti a alapunkte i ja iii, mis mõlemad nõuavad sõltumatut kaebuste menetlemise mehhanismi. Need mehhanismid võivad võtta erineva vormi, kuid peavad vastama kaebuste menetlemise, täitmise tagamise ja vastutuse põhimõtte nõuetele. Organisatsioonid saavutavad nõuetega vastavuse järgmiselt: i) nad järgivad erasektori poolt välja töötatud eraelu puutumatuse programme, mis toovad oma reeglitesse sisse andmekaitseraamistiku Privacy Shield põhimõtted ja hõlmavad kaebuste menetlemise, täitmise tagamise ja vastutuse põhimõttes kirjeldatud liiki tõhusaid täitmise tagamise mehhanisme; ii) nad järgivad üksikisikute kaebuste menetlemise ja vaidluste lahendamisega tegelevate järelevalveasutuste juhiseid või iii) nad kohustuvad tegema koostööd Euroopa Liidus asuvate andmekaitseasutustega või nende volitatud esindajatega.

b) See loend on näitlik ja mittetäielik. Erasektor võib välja töötada täiendavaid täitmise tagamise mehhanisme, kui need vastavad kaebuste menetlemise, täitmise tagamise ja vastutuse põhimõtte ja täiendavate põhimõtete nõuetele. Tuleb tähele panna, et kaebuste menetlemise, täitmise tagamise ja vastutuse põhimõtte nõuded

lisanduvad nõuetele selle kohta, et iseregulatsioonipüüdlused peavad olema jõustatavad föderaalse kaubanduskomisjoni seaduse (Federal Trade Commission Act) artikli 5 alusel, mis keelustab kõlvatud tavad ja pettuse, või selliseid tegusid reguleeriva muu seaduse või määruse alusel.

c) Aitamaks tagada vastavust nende poolt andmekaitseraamistiku Privacy Shield suhtes võetud kohustustega ja toetamaks programmi haldamist, peavad organisatsioonid ja nende sõltumatud kaebuste menetlemise mehhanismid andma nõudmisel ministeeriumile andmekaitseraamistikuga Privacy Shield seotud teavet. Lisaks peavad organisatsioonid viivitamata reageerima kaebustele, mis käsitlevad nende poolt põhimõtete järgimist ja mille on esitanud andmekaitseasutused ministeeriumi kaudu. Vastuses tuleb ära märkida, kas kaebus oli põhjendatud, ja kui oli, siis kuidas organisatsioon probleemi lahendab. Ministeerium kaitseb tema poolt vastu võetud teabe konfidentsiaalsust kooskõlas Ameerika Ühendriikide õigusega.

d) Kaebuste menetlemise mehhanismid

i) Tarbijaid tuleb julgustada esitama mis tahes kaebusi osjaomasele organisatsioonile enne siirdumist sõltumatute kaebuste menetlemise mehhanismide juurde. Organisatsioonid peavad vastama tarbijale 45 päeva jooksul alates kaebuse laekumisest. Kaebuste menetlemise mehhanismi sõltumatust võib tõendada eriti näiteks objektiivsuse, läbipaistva koosseisu ja finantseerimise ning tõestatud varasemate otsuste abil. Kaebuste menetlemise, täitmise tagamise ja vastutuse põhimõtte alusel peab üksikisikutele kättesaadav kaebuste menetlemine olema kergesti kättesaadav ja üksikisikutele tasuta. Vaidlusi lahendavad asutused peaksid tutvuma kõikide üksikisikutelt saadud kaebustega, mis ei ole selgelt alusetud või tähtsusetud. See ei takista kaebuste menetlemise mehhanismi eest vastutaval organisatsioonil kehtestada valikunõudeid, kuid sellised nõuded peaksid olema läbipaistavad ja õigustatud (näiteks jätta kõrvale kaebused, mis ei mahu programmi reguleerimisalasse või kuuluvad läbivaatamisele mõnel muul foorumil) ning nad ei tohiks ohustada kohustust põhjendatud kaebused läbi vaadata. Lisaks peaksid kaebuste menetlemise mehhanismid andma üksikisikutele täielikku ja kergesti kättesaadavat teavet selle kohta, kuidas toimub vaidluste lahendamine, kui nad kaebuse esitavad. Selline info peaks sisaldama teadet mehhanismi puutumatustavade kohta kooskõlas andmekaitseraamistiku Privacy Shield põhimõtetega. Samuti peaksid nad kaebuste lahendamise protsessi hõlbustamiseks tegema koostööd näiteks kaebuste standardvormide väljatöötamisel.

ii) Sõltumatud kaebuste menetlemise mehhanismid peaksid oma veebisaitidel avaldama teabe andmekaitseraamistiku Privacy Shield põhimõtete kohta ning teenuste kohta, mida nad andmekaitseraamistiku Privacy Shield kohaselt osutavad. Kõnealune teave peab sisaldama järgmist: 1) teave andmekaitseraamistiku Privacy Shield põhimõtete kohastele sõltumatutele kaebuste menetlemise mehhanismidele esitatavate nõuete kohta või nimetatud teabe juurde viiv link; 2) link ministeeriumi andmekaitseraamistiku Privacy Shield veebisaidile; 3) selgitus selle kohta, et nende vaidluste lahendamise teenus, mis on seotud andmekaitseraamistikuga Privacy Shield, on üksikisikutele tasuta; 4) kirjeldus selle kohta, kuidas on võimalik esitada andmekaitseraamistikuga Privacy Shield seotud kaebust; 5) ajaraamistik, mille jooksul andmekaitseraamistikuga Privacy Shield seotud kaebused läbi vaadatakse ning 6) erinevate võimalike õiguskaitsevahendite kirjeldus.

iii) Sõltumatud kaebuste menetlemise mehhanismid peavad igal aastal avaldama nende vaidluste lahendamise teenuse kohta koondstatistikat sisaldava aruande. Aastaaruanne peab sisaldama: 1) aruandeaastal laekunud andmekaitseraamistikuga Privacy Shield seotud kaebuste koguarv; 2) laekunud kaebuste liigid; 3) vaidluste lahendamise kvaliteedinäitajad, nagu näiteks kaebuste lahendamisele kulunud aeg ja 4) kaebuste lahendamise tulemused, eriti kohaldatud õiguskaitsevahendite ja sanktsioonide arv ning liigid.

iv) Vastavalt I lisas sätestatule on üksikisikul võimalus pöörduda allesjäävate nõuetega vahekohtu poole, et teha kindlaks, kas andmekaitseraamistikuga Privacy Shield ühinenud organisatsioon on rikkunud oma põhimõtete järgseid kohustusi asjaomase üksikisiku suhtes ja kas selline rikkumine jääb täielikult või osaliselt heastamata. Kõnealune võimalus on ainult nimetatud eesmärkidel kasutamiseks. Kõnealune võimalus ei ole kasutamiseks näiteks põhimõtete ([1]) suhtes tehtavate erandite või väidete suhtes, mis puudutavad andmekaitseraamistiku Privacy Shield piisavust. Kõnealuse vahekohtu võimaluse raames on andmekaitseraamistiku Privacy Shield paneelil (mis koosneb kolmest vahekohtunikust, kelles pooled on kokku leppinud) volitused kehtestada konkreetse üksikisiku suhtes rakendatavad mitterahalised õiglased kaitsevahendid (näiteks juurdepääsu võimaldamine, parandamine, kustutamine või üksikisiku küsimuse all olevate andmete tagastamine), mis on vajalikud põhimõtete rikkumise heastamiseks ainult asjaomasele üksikisikule. Föderaalse vahekohtu seaduse (Federal Arbitration Act) kohaselt on üksikisikutel ja andmekaitseraamistikuga Privacy Shield ühinenud organisatsioonidel õigus taotleda kohtulikku läbivaatust ning vahekohtu otsuste jõustamist Ameerika Ühendriikide seaduste alusel.

([1]) Põhimõtete jagu I.5.

e) Õiguskaitsevahendid ja sanktsioonid

Vaidlusi lahendava organi pakutud mis tahes õiguskaitsevahendite tulemuseks peaks olema mittevastavuse mõju heastamine organisatsiooni poolt, kuivõrd see on teostatav, ning see, et organisatsioon edasisel töötlemisel järgib põhimõtteid, ja kui see on asjakohane, et kaebuse esitanud üksikisiku isikuandmete töötlemine lakkab. Sanktsioonid peavad olema piisavalt ranged, et kindlustada põhimõtete järgimine organisatsiooni poolt. Mitmed erineva rangusastmega sanktsioonid võimaldavad vaidlusi lahendavatel asutustel asjakohaselt reageerida erineval tasemel põhimõtete järgimata jätmisele. Sanktsioonid peaksid hõlmama nii põhimõtete järgimata jätmise tuvastamise avalikustamist kui ka teatavatel asjaoludel nõuet andmed kustutada ([1]). Muud sanktsioonid võiksid hõlmata programmis osaleja tunnuse kasutusõiguse peatamist ja eemaldamist, põhimõtete järgimata jätmise tagajärjel üksikisikutele tekitatud kahju hüvitamist ning keelavaid otsuseid. Kui programmiga Privacy Shield ühinenud organisatsioonid ei järgi vaidlusi lahendavate erasektori asutuste ja iseregulatsiooniasutuste korraldusi, peavad need teavitama asjaomase pädevusega valitsusasutust või vastavalt asjakohasusele kohust, samuti ministeeriumi.

f) FTC tegevus

FTC on kohustatud eelisjärjekorras läbi vaatama kaebused väidetavate programmi Privacy Shield põhimõtete järgimata jätmiste kohta, mis on laekunud: i) eraelu puutumatuse iseregulatsiooniorganitelt ja teistelt sõltumatutelt vaidluste lahendamise organitelt; ii) ELi liikmesriikidelt, ja iii) ministeeriumilt, et otsustada, kas on rikutud föderaalse kaubanduskomisjoni seaduse (FTC Act) paragrahvi 5, mis keelustab kõlvatud tavad ja pettuse äritegevuses. Kui FTC järeldab, et tal on alust kahtlustada paragrahvi 5 rikkumist, võib ta asja lahendada nii, et hangib administratiivse keelustamiskorralduse (cease and desist order), millega keelustatakse rikkuv tegevus, või esitab kaebuse föderaalsele ringkonnakohtule, mille tulemuseks õnnestumise korral võib olla samasisuline föderaalkohtu otsus. See hõlmab ka valeväiteid andmekaitseraamistiku Privacy Shield põhimõtete järgimise kohta või osalemist programmis Privacy Shield organisatsioonide poolt, kes kas ei ole enam andmekaitseraamistikuga Privacy Shield ühinenute nimekirjas või ei ole kunagi ministeeriumile kinnitust esitanud. FTC võib keelustamiskorralduse rikkumise eest määrata tsiviiltrahve ja föderaalkohtu otsuse mittetäitmise eest taotleda vastutuselevõtmist tsiviil- või kriminaalkorras. FTC teavitab ministeeriumi sellistest meetmetest. Ministeerium julgustab teisi valitsusasutusi teda teavitama mis tahes taoliste kaebuste lahendamisest või muudest andmekaitseraamistiku Privacy Shield põhimõtete järgimist puudutavatest lahenditest.

g) Püsiv põhimõtete järgimata jätmine

i) Kui organisatsioon ei järgi põhimõtteid püsivalt, kaotab ta õiguse programmi Privacy Shield soodustustele. Organisatsioonid, kes ei järgi põhimõtteid püsivalt, eemaldatakse ministeeriumi poolt andmekaitseraamistikuga Privacy Shield ühinenute nimekirjast ning nad peavad tagastama või kustutama isikuandmed, mille nad programmi Privacy Shield tingimustel said.

ii) Püsiv põhimõtete järgimata jätmine tekib siis, kui ministeeriumile vastavust kinnitanud organisatsioon keeldub järgimast mis tahes eraelu puutumatuse iseregulatsiooniasutuse, sõltumatu vaidluste lahendamise organi või valitsusasutuse lõppotsust või kui selline asutus otsustab, et organisatsioon ei ole korduvalt põhimõtteid järginud sellisel määral, et organisatsiooni kinnitus põhimõtteid järgida ei ole enam usutav. Sellisel juhul peab organisatsioon ministeeriumi sellistest asjaoludest viivitamata teavitama. Selle nõude mittetäitmisel võidakse kohaldada valeandmete seadust (False Statements Act, 18 U.S.C. § 1001). Erasektori iseregulatsiooniprogrammist või sõltumatust vaidluste lahendamise mehhanismist loobumine ei vabasta organisatsiooni põhimõtete järgimise kohustusest ning tähendab püsivat põhimõtete järgimata jätmist.

iii) Ministeerium eemaldab organisatsiooni andmekaitseraamistikuga Privacy Shield ühinenute nimekirjast reageeringuna mis tahes teadetele, mida ta saab püsiva mittevastavuse kohta kas organisatsioonilt endalt, eraelu puutumatuse iseregulatsiooniasutuselt, teiselt sõltumatult vaidluste lahendamise organilt või valitsusasutuselt, kuid alles pärast põhimõtteid mittejärginud organisatsioonile 30 päevast etteteatamist, millele

([1]) Vaidlusi lahendavad asutused võivad omal äranägemisel otsustada, millistes olukordades nad neid sanktsioone rakendavad. Asjaomaste andmete tundlikkus on üheks teguriks otsuse võtmisel selle kohta, kas tuleks nõuda andmete kustutamist, samuti kas organisatsioon on andmeid kogunud, kasutanud või avalikustanud andmekaitseraamistiku Privacy Shield põhimõtteid jõhkralt eirates.

organisatsioonil on võimalus vastata. Sellele vastavalt selgub ministeeriumi hallatavast loendist, millistele organisatsioonidele on või ei ole enam tagatud programmi Privacy Shield soodustused.

iv) Organisatsioon, kes taotleb osalemist iseregulatsiooniorganis programmis Privacy Shield osaluse taastamise eesmärgil, peab sellele organile esitama täieliku teabe oma varasema osalemise kohta programmis Privacy Shield.

12. **Valikuvõimalus – keeldumise (opt out) ajastamine**

a) Üldiselt on valikuvõimaluse põhimõtte eesmärgiks tagada, et isikuandmeid kasutataks ja avalikustataks üksikisiku ootustele ja valikutele vastaval moel. Selle kohaselt peaks üksikisikul olema võimalus keelduda (opt out) isikuandmete otseturunduses kasutamisest (või valida see) mis tahes ajal organisatsiooni poolt kehtestatud mõistlikes piirides, näiteks jätmaks organisatsioonile aega keeldumise (opt out) sisseviimiseks. Organisatsioon võib ka nõuda piisavaid andmeid keeldumist (opt out) taotleva isiku kindlakstegemiseks. Ameerika Ühendriikides võivad üksikisikud seda valikut teostada keskse keeldumisprogrammi (opt out) abil, näiteks ühingu Direct Marketing Association postieelistuste teenuse kaudu. Ühingu Direct Marketing Association postieelistuste teenuses osalevad organisatsioonid peaksid sellest teenusest teavitama tarbijaid, kes ei soovi kommertsteavet saada. Igal juhul tuleks üksikisikule pakkuda käepärane ja taskukohane mehhanism selle valiku teostamiseks.

b) Samamoodi võib organisatsioon kasutada andmeid teatavatel otseturunduseesmärkidel, kui enne andmete kasutamist oleks põhjendamatu anda üksikisikule võimalus keeldumiseks (opt out), kui organisatsioon viivitamata annab samal ajal (ning nõudmisel igal ajal) üksikisikule võimaluse edaspidi keelduda (üksikisikule kulusid tekitamata) otseturundusteabe saamisest ning organisatsioon järgib üksikisiku soove.

13. **Reisiteave**

a) Väljaspool EL asuvatele organisatsioonidele on mitmetel erinevatel asjaoludel lubatud edastada lennuliinide reisijate broneerimisteavet ja muid reisiandmeid, näiteks andmeid boonusprogrammide või hotellide broneerimise ja erikohtlemise vajaduste kohta, näiteks religioossetele nõuetele vastavad eined või füüsilise abi vajadus. Direktiivi artikli 26 alusel võib isikuandmeid edastada kolmandasse riiki, mis ei taga piisavat kaitset artikli 25 lõike 2 tähenduses, tingimusel et i) on olemas vajadus pakkuda reisija poolt nõutud teenuseid või täita lepingujärgseid kohustusi, näiteks boonusprogrammi lepingust tulenevaid kohustusi või ii) selleks on saadud tarbijalt üheselt mõistetav nõusolek. Programmis Privacy Shield osalevad Ameerika Ühendriikide organisatsioonid pakuvad isikuandmetele piisavat kaitset ning võivad seetõttu EList edastatud andmeid vastu võtta neid tingimusi või direktiivi artiklis 26 sätestatud muid tingimusi täitmata. Kuna programm Privacy Shield hõlmab konkreetseid reegleid tundlike andmete kohta, võivad edastused programmis Privacy Shield osalejatele sisaldada selliseid andmeid (mida võib olla vaja koguda näiteks seoses füüsilise abiga, mida tarbijad vajavad). Igal juhul peab andmeid edastav organisatsioon siiski järgima selle EL liikmesriigi seadust, kus ta tegutseb, mis võib muu hulgas kehtestada eritingimusi tundlike andmete kasutamisele.

14. **Farmaatsia- ja meditsiinitooted**

a) ELi liikmesriikide seaduste või andmekaitseraamistiku Privacy Shield põhimõtete rakendamine

ELi liikmesriigi seadust kohaldatakse isikuandmete kogumisele ja mis tahes töötlemisele, mis leiab aset enne edastamist Ameerika Ühendriikidesse. Andmekaitseraamistiku Privacy Shield põhimõtteid kohaldatakse andmete suhtes siis, kui need on edastatud Ameerika Ühendriikidesse. Farmaatsiauuringuteks ja muudel eesmärkidel kasutatavatest andmetest tuleks võimalusel nimed kustutada.

b) Tulevased teadusuuringud

i) Teatavate meditsiiniliste või farmaatsiauuringute tulemusena saadud isikuandmetel on sageli suur väärtus tulevaste teadusuuringute jaoks. Kui ühe teadusuuringu jaoks kogutud isikuandmed edastatakse Ameerika Ühendriikide organisatsioonile, kes on ühinenud andmekaitseraamistikuga Privacy Shield, võib asjaomane organisatsioon kasutada neid andmeid uuteks teadusuuringuteks, kui alguses esitati asjakohane teade ja anti valikuvõimalus. Selline teade peaks teavitama tulevastest andmete kasutusviisidest, näiteks regulaarsed täiendamised, seonduvad uuringud või turundus.

ii) On arusaadav, et kõiki tulevasi andmete kasutamise viise ei ole võimalik välja tuua, kuna vajadus uuteks uuringuteks võib tekkida algandmete uuest tõlgendamisest, uutest meditsiinilistest avastustest ja arengutest ning tervishoiualastest ja regulatiivsetest arengutest. Kui see on asjakohane, peaks teade seega hõlmama selgitust, et isikuandmeid võidakse tulevikus kasutada ettenägematutes meditsiini- ja farmaatsiauuringutes. Kui andmeid ei kasutata kooskõlas üldise uuringueesmärgi või -märkidega, milleks isikuandmed algselt koguti või millega üksikisik seejärel nõustus, tuleb hankida uus nõusolek.

c) Kliinilistest katsetest loobumine

Osalejad võivad igal ajal otsustada või neid võidakse paluda kliinilistest katsetest loobuda. Loobumise eel kogutud isikuandmeid võib siiski töödelda koos teiste kogutud andmetega kliinilise katse osana, kui seda osalejale teates selgitati siis, kui ta osalema nõustus.

d) Edastamine reguleerimis- ja järelevalve eesmärkidel

Farmaatsia- ja meditsiiniseadmete firmadel on lubatud ELis läbi viidud kliiniliste katsete isikuandmeid esitada Ameerika Ühendriikide seadusandjatele reguleerimis- ja järelevalve eesmärkidel. Sarnaselt, kooskõlas teate ja valikuvõimaluse põhimõttega on lubatud edastada isikuandmeid muudele osapooltele peale seadusandjate, näiteks äriühingu teistesse asukohtadesse ja teistele uurijatele.

e) Pimeuuringud

i) Objektiivsuse tagamiseks ei saa paljudes kliinilistes katsetes osalejatele ja sageli ka uurijatele võimaldada juurdepääsu andmetele selle kohta, millist ravi milline osaleja saab. See seaks ohtu uuringu kehtivuse ja tulemused. Osalejatele kliinilistes katsetes (mida nimetatakse ka „pimeuuringuteks“) ei pea võimaldama katse ajal juurdepääsu oma ravi kohta käivatele andmetele, kui seda piirangut on selgitatud siis, kui osaleja katsega ühines, ja kui sellise teabe avalikustamine ohustaks uuringu usaldusväärsust.

ii) Nõusolek katses neil tingimustel osaleda on juurdepääsuõigusest loobumise mõistlik vorm. Pärast katse lõpuleviimist ja tulemuste analüüsi peaks osalejatele võimaldatama juurdepääs oma andmetele, kui nad seda soovivad. Seda peaksid nad taotlema eelkõige arstilt või muult meditsiinitöötajalt, kellelt nad kliinilise katse ajal ravi said, või siis sponsororganisatsioonilt.

f) Toote ohutuse ja tõhususe jälgimine

Farmaatsia- või meditsiiniseadmete firma ei pea rakendama andmekaitseraamistiku Privacy Shield teate, valikuvõimaluse, edasise edastamise ja juurdepääsu põhimõtteid toote ohutuse ja tõhususe jälgimise toimingutes, sealhulgas vastunäidustusjuhtumite aruandlus ja patsientide/katsealuste poolt teatavate ravimite või meditsiiniseadmete kasutamise jälgimine, selles ulatuses, milles nende põhimõtete järgimine segaks reguleerivate nõuete

järgimist. See kehtib näiteks meditsiiniteenuste pakkujate, farmaatsia- ja meditsiiniseadmete firmadele kui ka farmaatsia- ja meditsiiniseadmete firmade aruannete osas sellisele valitsusasutusele nagu Food and Drug Administration.

g) Kodeeritud andmed

Uurimisandmed kodeeritakse alati päritolukohas põhiuurija poolt ainulaadse koodiga, et üksikute andmesubjektide identiteeti mitte paljastada. Selliste uuringute sponsoriteks olevad farmaatsiafirmad selle koodi võtit ei saa. Ainulaadne koodi võti on ainult uurijal, et temal oleks võimalik uuritavaid eriolukordades tuvastada (nt kui on vajalik edaspidine meditsiiniline tähelepanu). Sellisel moel kodeeritud andmete edastamine EList Ameerika Ühendriikidesse ei kujuta endast andmekaitseraamistiku Privacy Shield põhimõtete kohast isikuandmete edastamist.

15. **Avalikud registrid ja avalikult kättesaadav teave**

a) Organisatsioon peab rakendama andmekaitseraamistiku Privacy Shield turvalisuse, andmete terviklikkuse ja eesmärgi piiramise, kaebuste menetlemise, täitmise tagamise ja vastutuse põhimõtteid avalikest allikatest kättesaadavate isikuandmete suhtes. Kõnealuseid põhimõtteid tuleb rakendada ka isikuandmete suhtes, mis on kogutud avalikest registritest, st sellistest valitsusasutuste või nende üksuste poolt mis tahes tasemel peetavatest registritest, mis on üldsusele tutvumiseks avatud.

b) Avalike registrite andmetele ei ole vaja rakendada teate, valikuvõimaluse ega kolmandale isikule edastamise eest vastutuse põhimõtteid, kui neid ei kombineerita mitteavalike registrite andmetega ning järgitakse asjakohase pädevuse alusel kehtestatud kasutustingimusi. Samuti ei ole teate, valikuvõimaluse või kolmandale isikule edastamise eest vastutuse põhimõtet üldjuhul vaja rakendada avalikult kättesaadavale teabele, välja arvatud kui Euroopa edastaja osutab, et selline teave allub piirangutele, mis nõuavad nende põhimõtete rakendamist organisatsiooni poolt andmete kavandatud eesmärgil kasutamiseks. Organisatsioon ei vastuta selle eest, kuidas selliseid andmeid kasutavad need, kes saavad asjaomase teabe avalikustatud materjalidest.

c) Kui leitakse, et organisatsioon on tahtlikult isikuandmed avalikustanud põhimõtteid rikkudes, et organisatsioon ise või keegi teine neist eranditest kasu võiks saada, lõpeb tema õigus programmi Privacy Shield soodustustele.

d) Avalikest andmebaasidest saadud andmetele ei ole vaja kohaldada juurdepääsu põhimõtet, kui need ei ole kombineeritud muude isikuandmetega, välja arvatud kui väikestes kogustes mitteavaliku registri andmeid kasutatakse avalike registrite andmete indekseerimiseks või organiseerimiseks. Tuleb siiski järgida asjakohase pädevusega asutuse poolt kehtestatud kasutustingimusi. Kui avalike registrite andmed on kombineeritud muude, mitteavalike registrite andmetega (muude kui eespool konkreetselt märgitud), peab organisatsioon siiski võimaldama juurdepääsu kõikidele sellistele andmetele, kui sellele ei kohaldata muid lubatud erandeid.

e) Nii nagu ka avalike registrite andmete puhul, ei ole vaja võimaldada juurdepääsu andmetele, mis on juba üldsusele kättesaadavad, kui neid ei ole kombineeritud üldsusele mittekättesaadavate andmetega. Avalikult kättesaadava info müügiga tegelevad organisatsioonid võivad juurdepääsutaotlustele vastates nõuda organisatsiooni tavapärast tasu. Alternatiivina võivad isikud taotleda juurdepääsu enda kohta käivatele andmetele sellelt organisatsioonilt, kes need algselt kogus.

16. **Juurdepääsutaotlused riigiasutuste poolt**

a) Selleks, et pakkuda läbipaistvust riigiasutuste seadustega kooskõlas olevate taotluste suhtes isikuandmetele juurdepääsuks, võivad andmekaitseraamistikuga Privacy Shield ühinenud organisatsioonid anda perioodiliselt välja aruandeid selle kohta, kui mitu isikuandmete avaldamise taotlust nad riigiasutustelt õiguskaitselisteks või riikliku julgeoleku vajaduste täitmiseks on saanud, kohaldatavate seaduste alusel lubatud avalikustamise ulatuses.

b) Teavet, mida andmekaitseraamistikuga Privacy Shield ühinenud organisatsioonid asjaomastes aruannetes esitavad, koos luureühenduse poolt avaldatud ja muu teabega, võib kasutada iga-aastase andmekaitseraamistiku Privacy Shield põhimõtete kohase toimimise läbivaatamise jaoks esitatava teabena.

c) Teate põhimõtte punkti a alapunkti xii kohase teate puudumine ei ole takistuseks ega kahjusta organisatsiooni suutlikkust vastata seaduslikele taotlustele.

*I lisa*

**Vahekohtumudel**

Käesolevas I lisas sätestatakse tingimused, mille alusel andmekaitseraamistikuga Privacy Shield ühinenud organisatsioonid on kohustatud kaebusi vahekohtumenetluses lahendama kaebuste menetlemise, täitmise tagamise ja vastutuse põhimõtte kohaselt. Allpool kirjeldatud siduv vahekohtumenetluse kasutamise võimalus kuulub kohaldamsiele ELi-USA andmekaitseraamistikuga Privacy Shield hõlmatud isikuandmete suhtes esitatavate teatud „jääknõuete" puhul. Kõnealuse valikuvõimaluse andmise eesmärgiks on pakkuda üksikisikutele kiire, sõltumatu ja õiglane mehhanism, mille nad võivad valida väidetavate põhimõtete rikkumiste lahendamiseks, mida ei ole lahendatud muude võimalike andmekaitseraamistiku Privacy Shield mehhanismide abil.

A. **Kohaldamisala**

Kõnealune võimalus on üksikisikule kättesaadav allesjäänud nõuetega vahekohtu poole pöördumiseks, et teha kindlaks, kas andmekaitseraamistikuga Privacy Shield ühinenud organisatsioon on rikkunud Privacy Shield põhimõtete järgseid kohustusi asjaomase üksikisiku suhtes ja kas selline rikkumine jääb täielikult või osaliselt heastamata. Kõnealune võimalus on ainult nimetatud eesmärkidel kasutamiseks. Kõnealune võimalus ei ole kasutamiseks näiteks põhimõtete suhtes tehtavate erandite ([1]) või väidete suhtes, mis puudutavad andmekaitseraamistiku Privacy Shield piisavust.

B. **Kättesaadavad õiguskaitsevahendid**

Kõnealuse vahekohtu võimaluse raames on andmekaitseraamistiku Privacy Shield paneelil (mis koosneb kolmest vahekohtunikust, kelles pooled on kokku leppinud) volitused kehtestada konkreetse üksikisiku suhtes rakendatavad mitterahalised õiglased kaitsevahendid (näiteks juurdepääsu võimaldamine, parandamine, kustutamine või üksikisiku küsimuse all olevate andmete tagastamine), mis on vajalikud põhimõtete rikkumise heastamiseks ainult asjaomasele üksikisikule. Kõnealused volitused on ainsad, mis vahekohtunikel on õiguskaitsevahendite suhtes. Õiguskaitsevahendeid kaaludes peavad vahekohtunikud arvesse võtma ka teiste andmekaitseraamistiku Privacy Shield mehhanismide poolt juba rakendatud õiguskaitsevahendeid. Kahjuhüvitisi, kulude ja tasude hüvitamist või muid õiguskaitsevahendeid ette ei nähta. Kumbki pool maksab ise oma advokaaditasud.

C. **Vajalikud sammud enne vahekohtu poole pöördumist**

Üksikisik, kes otsustab kasutada kõnealust vahekohtumenetluse võimalust, peab enne vahekohtule nõude esitamist tegema järgmist: 1) pöörduma väidetava rikkumisega otse organisatsiooni poole ja võimaldama organisatsioonil asi lahendada põhimõtete jaos III.11(d)(i) sätestatud ajavahemiku jooksul; 2) kasutama põhimõtete kohast sõltumatut kaebuste menetlemise mehhanismi, mis on üksikisikutele tasuta; ja 3) esitada juhtum oma andmekaitseasutuse kaudu lahendamiseks kaubandusministeeriumile ning võimaldada kaubandusministeeriumil lahendada asi parimal moel aja jooksul, mis on sätestatud kaubandusministeeriumi väliskaubandusameti kirjas ja mis on üksikisikutele tasuta.

Kõnealuse vahekohtumenetluse võimalust ei saa kasutada, kui üksikisiku poolt väidetav sama põhimõtete rikkumist 1) on juba varem vahekohtumenetluses menetletud; 2) on olnud aluseks lõplikule kohtuotsusele kohtuasjas, milles kõnealune üksikisik oli üheks pooleks; või 3) mille osas pooled on eelnevalt kokkuleppele jõudnud. Lisaks ei saa kõnealust võimalust kasutada, kui ELi andmekaitseasutusel on 1) põhimõtete jagude III.5 või III.9 kohased volitused; või 2) volitused lahendada väidetav rikkumine otse organisatsiooniga. Andmekaitseasutuse volitus lahendada sama nõuet ELi vastutava töötleja vastu ei välista kõnealuse vahekohtumenetluse võimaluse kasutamist teise õigussubjekti vastu, kes ei ole andmekaitseasutuse volitustega seotud.

D. **Otsuste siduvus**

Üksikisiku otsus kasutada siduvat vahekohtumenetlust on täiesti vabatahtlik. Vahekohtu otsused on siduvad kõikidele vahekohtumenetluse pooltele. Pöördudes vahekohtu poole, loobub üksikisik võimalusest saada sama rikkumise suhtes abi mõnest teisest foorumist, välja arvatud juhul, kui mitterahalised õiglased õiguskaitsevahendid ei heasta täielikult väidetavat rikkumist, mispuhul üksikisiku pöördumine vahekohtu poole ei takista kahjuhüvitise sissenõudmist, mida tavaliselt tehakse kohtu kaudu.

([1]) Põhimõtete jagu I.5.

E. **Läbivaatus ja jõustamine**

Föderaalse vahekohtu seaduse (Federal Arbitration Act) kohaselt on üksikisikutel ja andmekaitseraamistikuga Privacy Shield ühinenud organisatsioonidel õigus taotleda kohtulikku läbivaatamist ning vahekohtu otsuste täitmisele pööramist Ameerika Ühendriikide seaduste alusel ([1]). Kõikidel sellistel juhtudel tuleb pöörduda föderaalsesse ringkonnakohtusse, mille territooriumile jääb andmekaitseraamistikuga Privacy Shield ühinenud organisatsiooni peamine tegevuskoht.

Käesolev vahekohtumenetluse valimise võimalus on mõeldud vaid üksikisikuid puudutavate vaidluste lahendamiseks ja mitte veenvate või siduvate pretsedentide loomiseks teisi isikuid puudutavates asjades, sealhulgas tulevaste vaidluste lahendamiseks vahekohtutes, ELi või USA kohtutes või FTC menetlustes.

F. **Vahekohtu koosseis**

Pooled valivad vahekohtunikud allpool vaadeldud vahekohtunike nimekirjast.

Kooskõlas kohaldatava õigusega koostavad Ameerika Ühendriikide kaubandusministeerium ja Euroopa Komisjon nimekirja vähemalt 20 vahekohtunikust, kes valitakse nende sõltumatuse, aususe ja asjatundlikkuse alusel. Seoses kõnealuse protsessiga kohaldatakse järgmist.

Vahekohtunikud:

1) jäävad nimekirja kolmeks aastaks, kui ei ilmne erandlikke asjaolusid või põhjuseid, ning seda määramist võib pikendada üks kord täiendavaks kolmeaastaseks perioodiks;

2) ei ole ühegi partei ega andmekaitseraamistikuga Privacy Shield ühinenud organisatsiooni, või USA või ELi või ELi liikmesriigi või muu valitsusasutuse, avalik-õigusliku asutuse või täitevasutusega seotud ega toimi nende juhtnööride järgi ning

3) peavad olema lubatud töötama juristina USAs ja olema asjatundjad USA eraelu puutumatust käsitlevate ning ELi isikuandmete kaitset käsitlevate õigusaktide alal.

G. **Vahekohtumenetlus**

Kooskõlas kehtivate seadustega lepivad kaubandusministeerium ja Euroopa Komisjon kuus kuud peale piisavusotsuse vastuvõtmist kokku olemasolevate, kindlalt väljakujunenud USA vahekohtumenetluste (nagu näiteks AAA või JAMS) kasutuselevõtmiseks andmekaitseraamistiku Privacy Shield paneeli poolt, kõikidel alljärgnevatel tingimustel:

1. Üksikisik võib algatada siduva vahekohtumenetluse, kooskõlas eespool kirjeldatud vahekohtu poole pöördumise eelset menetlust käsitleva sättega, saates organisatsioonile „teate". Teade peab sisaldama kokkuvõtet lõigus C kirjeldatud sammudest, mis on nõude lahendamiseks tehtud, kirjeldust väidetava rikkumise kohta ja üksikisiku valikul mis tahes toetavaid materjale ja dokumente ja/või asjaomast nõuet puudutavate õigusaktide käsitlust.

([1]) Föderaalse vahekohtu seaduse (Federal Arbitration Act, FAA) 2. peatüki kohaselt „kuulub õigussuhtest – sõltumata sellest, kas see on lepinguline või mitte –, mida loetakse äriliseks, sealhulgas FAA 2. jaos kirjeldatud tehing, leping või kokkulepe, tuleneva vahekohtus sõlmitud kokkuleppe või vahekohtuotsuse suhtes kohaldamisele konventsioon [on the Recognition and Enforcement of Foreign Arbitral Awards of June 10, 1958, 21 U.S.T. 2519, T.I.A.S. No. 6997 („New York Convention")]." 9 U.S.C. § 202. Lisaks sätestatakse FAAs, et „kokkuleppe või otsuse suhtes, mis tuleneb sellisest õigussuhtest ja mis jääb täies ulatuses Ameerika Ühendriikide kodanike vahele, ei kohaldata konventsiooni [New York], juhul kui see õigussuhe ei ole hõlma välismaal asuvat kinnisvara, see ei näe ette välismaal täitmist või täitmisele pööramist, või sellel on muu mõistlik seos ühe või mitme välisriigiga." Samas sätestatakse 2. peatükis, et „kõik vahekohtumenetluse pooled võivad pöörduda mis tahes kohtu poole, kellel on käesoleva peatüki kohane pädevus, et saada kinnitav kohtuotsus vahekohtumenetluse teise poole suhtes. Kohus kinnitab otsuse, juhul kui ta ei leia ühtegi kõnealuses konventsioonis [New York] sätestatud põhjust otsuse tunnustamise või täitmise kinnitamisest keeldumiseks või edasilükkamiseks." *Id.* § 207. Edasi sätestatakse 2. peatükis, et „Ameerika Ühendriikide ringkonnakohtutel.. on esimese kohtuastme pädevus. .. hagi või menetluse suhtes (New Yorki konventsiooni kohaselt), vaatamata vaidlusalusele summale." *Id.* § 203.
2. peatükis sätestatakse ka, et „1. peatükk kehtib käesoleva peatüki alusel esitatud nõuete ja algatatud menetluste suhtes sellises ulatuses, milles kõnealune peatükk ei ole vastuolus käesoleva peatükiga või konventsiooniga [New York], mille Ameerika Ühendriigid on ratifitseerinud." *Id.* § 208. 1. peatükk sätestab omakorda, et kirjalik säte. ... lepingus, mis tõendab tehingut, mis hõlmab äritegevust, mille suhtes tuleb lahendus leida vahekohtumenetluse teel seejärel sellise lepingu või tehingu alusel tekkinud vaidluse või keeldumise pärast kogu või mis tahes selle osa täitmisest, või kirjalik leping sellisest lepingust, tehingust või keeldumisest tekkinud olemasoleva vastuolu vahekohtule lahendamiseks esitamiseks, on kehtiv, tühistamatu ja jõustatav, välja arvatud põhjustel, mida näeb ette seadus või õiglane kohtumenetlus mis tahes lepingu ülesütlemiseks. *Id.* § 2. Edasi sätestab 1. peatükk, et „mis tahes vahekohtumenetluse pool võib pöörduda selleks määratud kohtusse, saamaks vahekohtu otsust kinnitavat otsust, ja kohus peab seejärel sellise otsuse tegema, välja arvatud juhul kui vahekohtu otsus on tühistatud, muudetud või parandatud vastavalt [FAA] jagudes 10 ja 11 sätestatule." *Id.* § 9.

2. Töötatakse välja menetluskord tagamaks, et üht ja sama üksikisiku poolt väidetavat rikkumist ei heastataks ega menetletaks kaks korda.

3. FTC tegevus võib toimuda paralleelselt vahekohtumenetlusega.

4. Asjaomasel vahekohtumenetluse läbiviimsiel ei või osaleda mitte ükski USA, ELi või ELi liikmesriigi või muu valitsusasutuse, avalik-õigusliku asutuse või täitevasutuse esindaja, välja arvatud juhul, kui ELi andmekaitseasutus osutab ELi üksikisiku palvel abi vaid teate ettevalmistamisel, ent ELi andmekaitseasutus ei tohi saada juurdepääsu kõnealuste vahekohtute poolt tuvastatud asjaoludele või muudele materjalidele.

5. Vahekohtumenetlus toimub Ameerika Ühendriikides ning üksikisik võib valida osalemise video või telefoni teel, mis talle võimaldatakse tasuta. Isiklikult kohalviibimine ei ole nõutav.

6. Vahekohtu keel on inglise keel, kui pooled ei lepi kokku teisiti. Põhjendatud juhtudel ja võttes arvesse seda, kas üksikisikut esindab advokaat või ei, võimaldatakse üksikisikutele vahekohtu istungitel tasuta suuline tõlge, samuti ka vahekohtu materjalide kirjalik tõlge, välja arvatud juhul, kui kohus leiab, et konkreetseid asjaolusid arvesse võttes oleksid kulud põhjendamatult ebaproportsionaalsed.

7. Vahekohtunikele edastatavad materjalid hoitakse konfidentsiaalsetena ning neid kasutatakse ainult seoses vahekohtu tegevusega.

8. Konkreetset üksikisikut puudutavad menetluseelsed meetmed on vajadusel lubatud, ent pooled peavad sellega seotud teavet käsitama konfidentsiaalsena ning neid võib kasutada üksnes vahekohtumenetluse eesmärkidel.

9. Vahekohus peaks otsuseni jõudma 90 päeva jooksul alates teatise laekumisest küsimuse all olevale organisatsioonile, kui pooled teisiti kokku ei lepi.

H. **Kulud**

Vahekohtunikud peaksid püüdma astuda mõistlikke samme vahekohtu kulude või tasude minimeerimiseks.

Kohaldatavatest õigusnormidest lähtudes aitab kaubandusministeerium, kooskõlastatult Euroopa Komisjoniga, kaasa fondi loomisele, kuhu andmekaitseraamistikuga Privacy Shield ühinenud organisatsioonid peavad tegema iga-aastaseid sissemakseid, mille suurus sõltub osaliselt organisatsiooni suurusest ja millega kaetakse vahekohtumenetluse kulud, kaasa arvatud vahekohtunike tasud, mis võivad ulatuda ette nähtud ülemmääradeni. Fondi hakkab haldama kolmas isik, kellel tuleb regulaarselt esitada aruandeid fondi tegevuse kohta. Iga-aastase läbivaatamise käigus vaatavad kaubandusministeerium ja Euroopa Komisjon üle fondi tegevuse, sealhulgas vajaduse muuta sissemaksete suurust või tasude ülemmäärasid, ning võtavad muu hulgas arvesse peetud vahekohtumenetluste arvu ning seonduvaid kulusid ja ajalisi faktoreid, kusjuures vastastikuse arusaama kohaselt ei või andmekaitseraamistikuga Privacy Shield ühinenud organisatsioone rahaliselt ülemäära koormata. Käesoleva sätte alusel ega ka mitte ühestki käesoleva sätte alusel tegutsevast fondist ei kaeta advokaaditasusid.

*III LISA*

**Kiri USA riigisekretärilt John Kerry'lt**

7. juuli 2016

Lugupeetud volinik Jourová

Mul on hea meel, et oleme jõudnud vastastikusele mõistmisele Euroopa Liidu – Ameerika Ühendriikide andmekaitseraamistiku Privacy Shield osas, mis hakkab hõlmama ka ombudsmani mehhanismi, mille kaudu on ELi ametiasutustel võimalik esitada ELi üksikisikute nimel päringuid USA signaaliluure tavade kohta.

17. jaanuaril 2014. aastal kuulutas president Barack Obama välja olulised luurereformid, mis on lisatud dokumenti Presidential Policy Directive 28 (PPD-28). PPD-28 alusel määrasin ma aseriigisekretäri Catherine A. Novelli, kes täidab ka rahvusvahelise infotehnoloogiaalase diplomaatia vanemkoordinaatori (Senior Coordinator for International Information Technology Diplomacy) ülesandeid, kontaktisikuks välisriikide valitsuste jaoks, kes soovivad väljendada muret USA signaaliluurealase tegevuse kohta. Lisaks sellele olen ma asutanud ka andmekaitseraamistiku Privacy Shield ombudsmani mehhanismi, mis on kooskõlas A lisas sätestatud tingimustega, mida on pärast mu 22. veebruari 2016. aasta kirja ajakohastatud. Olen andnud korralduse aseriigisekretär Novellile selle ülesande täitmiseks. Aseriigisekretär Novelli on USA luureühendusest sõltumatu ning allub otse mulle.

Olen andnud oma töötajatele korralduse eraldada vajalikud ressursid uue ombudsmani mehhanismi rakendamiseks ja ma olen kindel, et sellest saab tõhus abinõu ELi üksikisikute muredega tegelemiseks.

Siiralt Teie

John F. Kerry

*A lisa*

**ELi-USA andmekaitseraamistiku Privacy Shield ombudsmani mehhanism Signaaliluure kohta**

Tunnustades ELi-USA andmekaitseraamistiku Privacy Shield tähtsust, käivitab käesolev memorandum protsessi uue, dokumendiga Presidential Policy Directive 28 (PPD-28) kooskõlas oleva signaaliluure mehhanismi rakendamise ([1]).

Oma 17. jaanuari 2014. aasta kõnes kuulutas president Barack Obama välja olulised luurereformid. Selles kõnes ta rõhutas, et „meie jõupingutused aitavad kaitsta mitte üksnes meie rahvast, vaid ka meie sõpru ja liitlasi. Meie jõupingutused on ainult siis tõhusad, kui ka tavalised inimesed teistes riikides ei kahtle, et Ameerika Ühendriigid austavad ka nende eraelu puutumatust." President Obama andis teada uue presidendi poliitikasuunise PPD-28 väljaandmisest, mille eesmärgiks on „näha selgelt ette, mida me teeme ja mida ei tee, kui asi puudutab meie luuretegevust ookeani taga."

PPD-28 jagu 4(d) kohustab riigisekretäri määrama rahvusvahelise infotehnoloogiaalase diplomaatia vanemkoordinaatori (vanemkoordinaator) „kes … oleks kontaktisikuks välisriikide valitsuste jaoks, kes soovivad väljendada muret USA signaaliluurealase tegevuse kohta". Alates 2015. aasta jaanuarist on vanemkoordinaatori ülesandeid täitnud aseriigisekretär Novelli.

Memorandumis kirjeldatakse uut mehhanismi, mida vanemkoordinaator hakkab järgima, et hõlbustada taotluste menetlemist ning vastamist kõnealustele taotlustele, mis käsitlevad riiklike julgeolekuasutuste juurdepääsu andmetele, mida EList edastatakse Ameerika Ühendriikidesse andmekaitseraamistiku Privacy Shield, standardsete lepingupunktide, äriühingute kohta käivate siduvate eeskirjade, „erandite" ([2]) või „võimalike tulevaste erandite" alusel, ([3]) sammudes väljakujunenud rada pidi kohaldatavate Ameerika Ühendriikide õigusaktide ja poliitikavalikute järgi.

1. **Andmekaitseraamistiku Privacy Shield ombudsman.** Vanemkoordinaator hakkab täitma andmekaitseraamistiku Privacy Shield ombudsmani kohustusi ning teeb vastavalt vajadusele täiendavatele välisministeeriumi ametnikele kohustuseks abistada teda käesolevas memorandumis üksikasjalikult kirjeldatud kohustuste täitmisel. (Edaspidi nimetatakse koordinaatorit ja kõiki asjaomaseid kohustusi täitvaid ametnikke üheskoos „andmekaitseraamistiku Privacy Shield ombudsman".) Andmekaitseraamistiku Privacy Shield ombudsman hakkab tööle tihedas koostöös asjakohaste ametnikega teistest ministeeriumitest ja asutustest, kelle ülesandeks on taotluste menetlemine kooskõlas kohaldatava Ameerika Ühendriikide õiguse ja normidega. Ombudsman on luureühendusest sõltumatu. Ombudsman allub otse riigisekretärile, kes tagab, et ombudsman täidab oma kohustusi objektiivselt ning väärmõjudeta, mis võiksid tema antavaid otsuseid mõjutada.

2. **Tõhus koordineerimine.** Andmekaitseraamistiku Privacy Shield ombudsman saab allpool kirjeldatavaid järelevalveasutusi tõhusalt kasutada ja koordineerida selle tagamiseks, et ombudsmani vastused ELi üksikisikute kaebusi käsitleva asutuse poolt esitatud taotlustele põhineksid vajalikul teabel. Kui taotlus on seotud jälitustegevuse

([1]) Juhul kui komisjoni piisavusotsus ELi-USA andmekaitseraamistiku Privacy Shield poolt osutatava kaitse kohta rakendub ka Islandi, Norra ja Liechtensteini suhtes, katab andmekaitseraamistiku Privacy Shield pakett nii Euroopa Liitu kui ka kolme kõnealust riiki. Seega loetakse seal, kus on viidatud ELile ja liikmesriikidele, nende hulka ka Island, Liechtenstein ja Norra.

([2]) „Erandid" on käesolevas kontekstis ärieesmärkidel andmete edastamine või edastamine, mis toimub järgmistel tingimustel: a) andmesubjekt on andmete kavandatud edastamiseks andnud oma ühemõttelise nõusoleku või b) edastamine on vajalik andmesubjekti ja vastutava töötleja vahelise lepingu täitmiseks või andmesubjekti taotlusel võetud lepingueelsete meetmete rakendamiseks või c) edastamine on vajalik andmesubjekti huvides vastutava töötleja ja kolmanda isiku vahel sõlmitud lepingu sõlmimiseks või täitmiseks või d) edastamine on vajalik või seaduse kohaselt nõutav üldiste huvidega seotud olulistel põhjustel või õigusnõuete koostamiseks, esitamiseks või kaitsmiseks või e) edastamine on vajalik andmesubjekti eluliste huvide kaitsmiseks või f) edastatavad andmed on pärit registrist, mis õigusnormide kohaselt on mõeldud avalikkuse teavitamiseks ja on tutvumiseks avatud laiemale avalikkusele või kõigile õigustatud huvidega isikutele, kuivõrd konkreetsel juhul täidetakse tingimusi, mis õigusaktidega on tutvumiseks ette nähtud.

([3]) „Võimalikud tulevased erandid" tähendab selles kontekstis ärieesmärkidel andmete edastamist või edastamisi, mis toimuvad ühel järgmistest tingimustest, sellises ulatuses kuivõrd asjaomane tingimus on seaduslikuks aluseks isikuandmete edastamiseks EList USAsse: a) andmesubjekt on edastamiseks andnud selgesõnalise nõusoleku pärast seda, kui teda teavitati sellise edastamisega tema jaoks kaasnevatest võimalikest ohtudest, mis tulenevad kaitse piisavuse otsuse ja asjaomaste kaitsemeetmete puudumisest või b) edastamine on vajalik, et kaitsta andmesubjekti või muude isikute olulisi huve, kui andmesubjekt on füüsiliselt või õiguslikult võimetu nõusolekut andma või c) edastamise puhul kolmandasse riiki või rahvusvahelisse organisatsiooni ja muud erandid ega võimalikud tulevased erandid ei ole kohaldatavad, vaid juhul, kui edastamine toimub ühekordselt, käsitleb ainult piiratud arvu andmesubjekte, on vajalik vastutava töötleja kaaluka õigustatud huvi tõttu, mida ei kaalu üles andmesubjekti huvid või õigused ja vabadused, ning vastutav töötleja on andnud hinnangu kõikidele andmeedastust ümbritsevatele asjaoludele ja on kõnealuse hinnangu alusel esitanud isikuandmete kaitsmiseks sobivad kaitsemeetmed.

vastavusega USA seadustele, võib andmekaitseraamistiku Privacy Shield ombudsman teha koostööd ühega sõltumatutest järelevalveorganitest, kellel on pädevus uurimise läbiviimiseks.

a) Andmekaitseraamistiku Privacy Shield ombudsman töötab tihedas koostöös Ameerika Ühendriikide valitsuse teiste ametnikega, sealhulgas asjakohaste sõltumatute järelevalveasutustega, tagamaks, et täidetud taotlusi menetletakse ja lahendatakse kooskõlas kehtivate õigusnormide ja poliitikavalikutega. Eriti tihedalt on andmekaitseraamistiku Privacy Shield ombudsmanil võimalik koostööd teha asutusega Office of the Director of National Intelligence, justiitsministeeriumiga ja teiste Ameerika Ühendriikide asjakohaste rahvusliku julgeoleku tagamisega seotud ministeeriumite ja asutustega, samuti peainspektoritega, teabevabaduse seaduse (Freedom of Information Act) ametnikega ning kodanikuvabaduste ja eraelu puutumatuse küsimustega tegelevate ametnikega.

b) Ameerika Ühendriikide valitsus hakkab toetuma mehhanismidele, millega koordineeritakse ja valvatakse rahvusliku julgeoleku küsimuste üle ministeeriumite- ja asutusteüleselt, aitamaks kindlustada, et andmekaitseraamistiku Privacy Shield ombudsman on suuteline vastama punkti 3(b) kohaselt esitatud taotlustele kooskõlas punktis 4(e) sätestatuga.

c) Andmekaitseraamistiku Privacy Shield ombudsman võib edastada taotlustega seotud küsimused läbivaatamiseks ka eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjonile (Privacy and Civil Liberties Oversight Board).

3) **Taotluste esitamine**

a) Taotlus esitatakse kõigepealt riigiasutuste poolt liikmesriigi järelevalveasutustele, kes on pädevad teostama järelevalvet riiklike julgeolekuteenistuste üle ja/või töötlema isikuandmeid. Taotluse esitab ombudsmanile ELi keskne organ (edaspidi „ELi üksikisikute kaebuste käsitlemise organ“).

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:

— 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, standardsete lepingupunktide, äriühingute kohta käivate siduvate reeglite, erandite või võimalike tulevaste erandite alusel;

iv) tehes esialgse otsuse, et taotlus ei ole põhjendamatu, kiuslik või pahauskselt esitatud.

c) Kui taotlus koostatakse eesmärgiga, et seda hakkab käesoleva memorandumi alusel menetlema andmekaitseraamistiku Privacy Shield ombudsman, siis ei pea taotlusel ära näitama, et taotleja andmetele on juurdepääsu kasutanud Ameerika Ühendriikide valitsus signaaliluure tegevuste kaudu.

4. **Kohustus vahetada teavet taotlusi edastava ELi üksikisikute kaebuste menetlemise organiga**

a) Andmekaitseraamistiku Privacy Shield ombudsman teatab taotluse kättesaamisest selle esitanud ELi üksikisikute kaebuste menetlemise organile.

b) Andmekaitseraamistiku Privacy Shield ombudsman kontrollib esmalt, kas taotlus on täidetud kooskõlas punktiga 3(b). Kui andmekaitseraamistiku Privacy Shield ombudsman märkab puudujääke või tal on küsimusi taotluse täitmise kohta, siis ta pöördub taotluse esitanud ELi üksikisikute kaebuste käsitlemise organi poole kõnealuste probleemide lahendamiseks.

c) Kui andmekaitseraamistiku Privacy Shield ombudsman vajab taotluse asjakohase menetlemise hõlbustamiseks taotluse kohta rohkem teavet, või kui on vajalik, et konkreetne üksikisik, kes algselt taotluse esitas, teeks konkreetsed tegevusi, teatab andmekaitseraamistiku Privacy Shield ombudsman sellest taotluse esitanud ELi üksikisikute kaebuste menetlemise organile.

d) Andmekaitseraamistiku Privacy Shield ombudsman jälgib, kus maal taotluse menetlemine on ning esitab taotluse esitanud ELi üksikisikute kaebuste menetlemise organile asjakohaseid ülevaateid.

e) Kui taotlus on koostatud kooskõlas käesoleva memorandumi punktiga 3, annab andmekaitseraamistiku Privacy Shield ombudsman selle taotluse esitanud ELi üksikisikute kaebuste menetlemise organile õigeaegselt asjakohase vastuse, pidades jätkuvalt kinni andmete kaitsmise kohustusest kohaldatavatest õigusnormidest ja poliitikavalikutest lähtudes. Andmekaitseraamistiku Privacy Shield ombudsman annab taotluse esitanud ELi üksikisikute kaebuste menetlemise organile vastuse, milles kinnitab, et i) taotlust on nõuetekohaselt uuritud, ja ii) et 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. Andmekaitseraamistiku Privacy Shield ombudsman ei kinnita ega eita, et üksikisik on olnud jälgimise objekt, samuti ei kinnita andmekaitseraamistiku Privacy Shield ombudsman, millist konkreetset õiguskaitsevahendit kohaldati. Nagu kirjeldatakse allpool olevas punktis 5, menetletakse FOIAga seotud taotlusi asjaomase statuudi ja kohaldatavate määruste alusel.

f) Andmekaitseraamistiku Privacy Shield ombudsman suhtleb otse ELi individuaalse kaebusi menetleva asutusega, mis omakorda vastutab taotlust esitava üksikisikuga suhtlemise eest. Juhul kui otsene suhtlemine moodustab osa allpool kirjeldatud menetlustest, siis toimub selline suhtlemine vastavalt kehtivale korrale.

g) Käesolevas memorandumis olevaid kohustusi ei kohaldata üldiste väidete suhtes, mille järgi ei ole ELi-USA andmekaitseraamistik Privacy Shield kooskõlas Euroopa Liidu andmekaitse nõuetega. Käesolevas memorandumis olevad kohustused põhinevad Euroopa Komisjoni ja USA valitsuses ühisarvamusel selle kohta, et arvestades selle mehhanismi raames võetavate kohustuste kohaldamisala, võivad esineda ressursside piirangud, sealhulgas seoses teabevabaduse seaduse (Freedom of Information Act – FOIA) päringutega. Juhul kui andmeraamistiku Privacy Shield ombudsmani ülesannete täitmine ületab mõistlikke ressursipiiranguid ning takistab asjaomaste kohustuste täitmist, arutlab USA valitsus Euroopa Komisjoniga mis tahes kohandamist, mis võiks olla asjaomane, et olukorraga tegeleda.

5. **Teabepäringud.** Teabevabaduse seaduse (Freedom of Information Act – FOIA) raames võib esitada ja menetleda USA valitsuse andmetele juurdepääsu taotlusi.

a) Teabevabaduse seadus tagab kõikidele isikutele võimaluse taotleda juurdepääsu olemasolevatele föderaalameti andmetele, sõltumata taotleja kodakondusest. Käesolev põhimäärus on kodifitseeritud USA-s koodiga 5 U.S.C. § 552. Statuut koos täiendava teabega teabevabaduse seaduse kohta on saadaval veebisaitidel www.FOIA.gov ja http://www.justice.gov/oip/foia-resources. Igas asutuses on teabevabaduse seaduse vanemametnik ning kõik asutused on esitanud oma avalikul veebisaidil teabe selle kohta, kuidas esitada asutusele teabevabaduse seaduse taotlus. Asutustes on kehtestatud menetlused, mille alusel nad üksteisega konsulteerivad seoses teabevabaduse seaduse taotlustega, mis hõlmavad teise asutuse andmeid.

b) Näiteks:

i) Riiklik luurejuhi amet (Office of the Director of National Intelligence – ODNI) on loonud enda tarbeks riikliku luurejuhi ameti teabevabaduse seaduse portaali: http://www.dni.gov/index.php/about-this-site/foia. Selles portaalis antakse teavet taotluse esitamise, olemasoleva taotluse staatuse kontrollimise ning teabevabaduse seaduse raames riikliku luurejuhi ameti väljastatud ja avaldatud teabele juurdepääsu kohta. Riikliku luurejuhi ameti teabevabaduse seaduse (ODNI FOIA) portaalis on lingid muudele teabevabaduse seaduse veebisaitidele luureühenduse liikmete jaoks: http://www.dni.gov/index.php/about-this-site/foia/other-ic-foia-sites.

ii) Justiitsministeeriumi teabepoliitika amet annab põhjalikku teavet teabevabaduse seaduse kohta: http://www.justice.gov/oip. See ei hõlma üksnes teavet justiitsministeeriumile teabevabaduse seaduse taotluse esitamise kohta, vaid ka juhiseid USA valitsusele teabevabaduse seaduse nõuete tõlgendamise ja kohaldamise jaoks.

c) Teabevabaduse seaduse raames kehtivad valitsuse andmete suhtes teatavad loetletud erandid. Need hõlmavad piiranguid salastatud riikliku julgeoleku teabele, kolmandate isikute isikuandmetele ja uurimistoimingutega seotud teabele juurdepääsu kohta ning on võrreldavad iga ELi liikmesriigi seatud piirangutega, mis põhinevad nende enda teabele juurdepääsu seadusel. Neid piiranguid kohaldatakse võrdselt nii ameeriklaste kui ka mitte-ameeriklaste suhtes.

d) Vastavalt teabevabaduse seadusele taotletud andmete väljastamise kohta tekkinud vaidlused saab esitada halduskohtusse ning seejärel föderaalkohtusse. Kohus peab uuesti määratlema, kas andmeid hoitakse nõuetekohaselt, 5 U.S.C. § 552(a)(4)(B), ning saab kohustada valitsust võimaldama andmetele juurdepääsu. Mõnel juhul on kohtud ümber lükanud valitsuse väited selle kohta, et teavet tuleb hoida salajasena. Kuigi rahaliste nõuete hüvitamist ei ole ette nähtud, võivad kohtud ette näha advokaaditasud.

6. **Taotlused edasise tegevuse kohta.** Taotlus, milles väidetakse, et tegemist on seaduse rikkumise või muu üleastumisega, saadetakse edasi asjaomasele Ameerika Ühendriikide valitsusorganile, sealhulgas sõltumatutele järelevalveorganitele, kellel on pädevus uurida asjaomast taotlust ja tegeleda mittevastavusega nii, nagu on allpool kirjeldatud.

a) Peainspektorid on seaduse järgi sõltumatud; neil on ulatuslikud volitused teostada uurimisi, auditeid ja programmide läbivaatamist, sealhulgas seoses pettuste ja kuritarvitamise või seaduserikkumisega; ning nad saavad soovitada parandusmeetmeid.

i) Muudetud 1978. aasta peainspektori seaduses sätestati, et föderaalne peainspektor on enamikes asutustes sõltumatu ja objektiivne üksus, kelle ülesannete hulka kuulub võitlus raiskamise, pettuste ja kuritarvitamisega asjaomaste asutuste programmides ja toimingutes. Selleks on iga peainspektor vastutav selliste auditite ja uurimiste läbiviimise eest, mis on seotud asutuse programmide ja toimingutega. Lisaks sellele kuulub peainspektorite ülesannete hulka juhtimine ja koordineerimine ning nad soovitavad poliitilisi suundi tegevusele, mis on ette nähtud majanduse, tõhususe ja tulemuslikkuse edendamiseks ning pettuse ja kuritarvitamise vältimiseks asutuse programmides ja toimingutes.

ii) Kõikides luureühenduse (Intelligence Community) üksustes on olemas peainspektor (Office of the Inspector General), kes vastutab muu hulgas välisluure tegevuse järelevalve eest. Mitmed peainspektori aruanded luureprogrammide kohta on avalikustatud.

iii) Näiteks:

— Luurerühenduse peainspektori amet (Office of the Inspector General of the Intelligence Community – IC IG) loodi vastavalt 2010. eelarveaasta luure volitamise seaduse (Intelligence Authorization Act) paragrahvile 405. Luureühenduse peainspektori amet (IC IG) vastutab luureühenduse üleste auditite, uurimiste, kontrollide ja läbivaatamiste eest, millega avastatakse ja lahendatakse süsteemseid riske, haavatavusi ja puudusi, mis hõlmavad luureühenduse asutuste missioone, eesmärgiga positiivselt mõjutada luureühenduse ülest mastaabisäästu ja tõhusust. Luurerühenduse peainspektori ametil (IC IG) on õigus uurida kaebusi või teavet, mis on seotud väitega selle kohta, et rikutud on seadust, eeskirja, määrust, toime on pandud raiskamine, pettus, võimu kuritarvitamine, või on tegemist olulise või konkreetse ohuga rahva tervisele ja turvalisusele seoses riikliku luurejuhi ameti (ODNI) ja/või luureühendusee luureprogrammide ja -tegevusega. Luureühenduse peainspektori amet annab teavet selle kohta, kuidas võtta aruande esitamiseks luureühenduse peainspektori ametiga otse ühendust: http://www.dni.gov/index.php/about-this-site/contact-the-ig.

— USA justiitsministeeriumi (DOJ) peainspektori amet (OIG) on seadusega loodud sõltumatu üksus, mille ülesanne on avastada ja ära hoida raiskamist, pettusi, kuritarvitamist ja üleastumist seoses justiitsministeeriumi programmide ja personaliga ning edendada nende programmide säästlikkust ja tõhusust. Peainspektori amet (OIG) uurib väidetavaid tsiviil- ja kriminaalõiguse rikkumisi justiitsministeeriumi töötajate poolt, samuti auditeerib ja kontrollib justiitsministeeriumi programme. Peainspektori amet on pädev läbi vaatama kõik üleastumisega seotud kaebused, mis on esitatud justiitsministeeriumi töötajate vastu, sealhulgas föderaalse juurdlusbüroo (Federal Bureau of Investigation); Uimastivastase võitlusega tegeleva ameti (Drug Enforcement Administration); Föderaalse Vanglabüroo (Federal Bureau of Prisons); USA Föderaalse Politseiteenistuse (U.S. Marshals Service); Alkoholi, Tubaka ja Tulirelvade Ameti (Bureau of Alcohol, Tobacco, Firearms, and Explosives); USA föderaalsete prokuratuuride (United States Attorneys Offices); ning justiitsministeeriumi muude osakondade või ametite töötajate vastu. (Üks erand seisneb

selles, et väited üleastumise kohta ministeeriumi advokaadi või õiguskaitseorganite töötajate poolt, mis on seotud ministeeriumi advokaadi volitusega uurida, menetleda või anda õigusalaseid nõuandeid, kuulub ministeeriumi ametialase vastutuse ameti (Office of Professional Responsibility) vastutusalasse.) Lisaks sellele kohustab 26. oktoobril 2001. aastal jõustunud USA patrioodiseaduse (USA Patriot Act) paragrahv 1001 peainspektorit läbi vaatama teavet ja võtma vastu võtma kaebusi, milles väidetakse, et justiitsministeeriumi töötajad on rikkunud kodanikuõigusi ja -vabadusi. Peainspektori amet haldab järgmist avalikku veebisaiti – https://www.oig.justice.gov –, mis hõlmab abiliini kaebuste esitamiseks – https://www.oig.justice.gov/hotline/index.htm.

b) USA valitsuse eraelu puutumatuse ja kodanikuvabaduste ametitel ja üksustel (Privacy and Civil Liberties offices and entities) on samuti asjaomased vastutusalad. Näiteks:

i) 2007. aasta 9/11 komisjoni seaduse (9/11 Commission Act of 2007) rakendussoovituste paragrahvis 803, mis on kodifitseeritud USA-s koodeksis 42 U.S.C. § 2000-ee1, määratakse teatavates ministeeriumides ja asutustes (sealhulgas riigidepartemang, justiitsministeerium ja riiklik luurejuhi amet (ODNI)) eraelu puutumatuse ja kodanikuvabaduste ametnikud. Paragrahvis 803 on täpsustatud, et need eraelu puutumatust ja kodanikuvabadusi käsitlevad ametnikud täidavad peanõuniku ülesandeid, tagamaks muu hulgas, et sellises ministeeriumis, asutuses või üksuses on kehtestatud nõuetekohased menetlused nende kaebustega tegelemiseks, mis on laekunud üksikisikutelt, kes väidavad, et asjaomane ministeerium, asutus või üksus on rikkunud nende eraelu puutumatust või kodanikuvabadusi.

ii) Riikliku luurejuhi ameti kodanikuvabaduste ja eraelu puutumatuse bürood (ODNI CLPO) juhib riikliku luurejuhi ameti kodanikuvabaduste kaitse ametnik; see ametikoht loodi 1948. aasta muudetud riikliku julgeoleku seaduse (National Security Act of 1948) alusel. Riikliku luurejuhi ameti kodanikuvabaduste ja eraelu puutumatuse büroo ülesannete hulka kuulub selle tagamine, et luureühenduse liikmete poliitika ja töökord hõlmab privaatsuse ja kodanikuvabaduste piisavat kaitset, samuti riikliku luurejuhi ameti programmide ja tegevuse raames kodanikuvabaduste ja eraelu puutumatuse kuritarvitamise või rikkumisega seotud kaebuste läbivaatamine ja uurimine. Riikliku luurejuhi ameti kodanikuvabaduste ja eraelu puutumatuse büroo (ODNI CLPO) jagab avalikkusele teavet, sealhulgas juhiseid kaebuse esitamise kohta, oma veebisaidil: www.dni.gov/clpo. Juhul kui riikliku luurejuhi ameti kodanikuvabaduste ja eraelu puutumatuse büroole laekub kaebus seoses eraelu puutumatuse või kodanikuvabadustega, mis hõlmab luureühenduse programme või tegevust, kooskõlastab see muude luureühenduse liikmetega, kuidas seda kaebust luureühenduses edasi menetleda. Pange tähele, et riiklikul julgeolekuasutusel (NSA) on samuti kodanikuvabaduste ja eraelu puutumatuse büroo (Civil Liberties and Privacy Office), mille vastutusalade kohta leiab teavet selle veebisaidilt: https://www.nsa.gov/civil_liberties/. Juhul kui andmetest nähtub, et amet ei järgi eraelu puutumatusega seotud nõudeid (nt presidendi poliitikasuunise nr 28 (PPD-28) paragrahvis 4 esitatud nõue), siis on ametitel olemas vastavusmehhanismid, et juhtum läbi vaadata ja olukorda parandada. Asutustel on kohustus teatada presidendi poliitikasuunise nr 28 (PPD-28) vastavusega seotud juhtumitest riiklikule luurejuhi ametile.

iii) Justiitsministeeriumi eraelu puutumatuse ja kodanikuvabaduste amet (OPCL) toetab ministeeriumi eraelu puutumatuse ja kodanikuvabaduste vanemametniku tööülesandeid ja vastutust. Eraelu puutumatuse ja kodanikuvabaduste ameti (OPCL) peamine ülesanne on kaitsta Ameerika Ühendriikide kodanike eraelu puutumatust ja kodanikuvabadusi ministeeriumi eraelu puutumatuse seotud tegevuse läbivaatamise, järelevalve ja koordineerimise kaudu. Eraelu puutumatuse ja kodanikuvabaduste amet (OPCL) tagab ministeeriumi üksustele juriidilise nõustamise ja juhendamise; tagab, et ministeerium tegutseb kooskõlas eraelu puutumatusega, sealhulgas kooskõlas 1974. aasta eraelu puutumatuse seadusega (Privacy Act of 1974), nii 2002. aasta e-riigi seaduse (E-Government Act of 2002) kui ka föderaalse infoturbe haldamise seaduse (Federal Information Security Management Act) eraelu puutumatusega seotud sätetega ning samuti asjaomaste seaduste edendamiseks välja antud halduspoliitika suunistega; arendab ja pakub ministeeriumisisest koolitust eraelu puutumatuse kohta; abistab eraelu puutumatuse ja kodanikuvabaduste vanemametnikku (CPCLO) ministeeriumisiseste eraelu puutumatuse normide väljatöötamisel; valmistab ette eraelu puutumatusega seotud aruandlust presidendile ja Kongressile; valmistab ette eraelu puutumatusega seotud aruandlust presidendile ja Kongressile; ning vaatab läbi ministeeriumi teabe haldamise tavad, tagamaks, et need on kooskõlas eraelu puutumatuse ja kodanikuvabaduste kaitsega. Eraelu puutumatuse ja kodanikuvabaduste amet annab oma vastutusaladest avalikkusele teavet aadressil: http://www.justice.gov/opcl.

iv) Vastavalt 42 U.S.C. § 2000ee *et seq*. vaatab eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon (PCLOB) pidevalt läbi i) ministeeriumide, täitevasutuste ja -üksuste eeskirjad ja menetlused, samuti nende rakendamise, mis on seotud jõupingutustega kaitsta riiki terrorismi eest, tagamaks, et eraelu puutumatus ja kodanikuvabadused on kaitstud; ning ii) täitevvõimu muud meetmed, mis on seotud asjaomaste jõupingutustega, et määratleda, kas need meetmed kaitsevad nõuetekohaselt eraelu puutumatust ja kodanikuvabadusi ning on kooskõlas eraelu puutumatust ja kodanikuvabadusi reguleerivate seaduste, määruste ja eeskirjadega. Komisjon võtab vastu ja vaatab läbi aruanded ja muud teabe, mis on laekunud eraelu puutumatuse ametnikelt ja kodanikuvabaduste ametnikelt ning, kui see on asjakohane, annab neile soovitusi seoses nende tegevusega. 2007. aasta 9/11 komisjoni seaduse (9/11 Commission Act of 2007) rakendussoovituste paragrahviga 803, mis on kodifitseeritud USA-s koodiga 42 U.S.C. § 2000-ee1, reguleeritakse eraelu puutumatuse ja kodanikuvabaduste ametnike tööd kaheksas föderaalses asutuses (sealhulgas kaitseminister, sisejulgeolekuminister, riiklik luurejuht ja luure keskagentuuri direktor) ning kõiki muid eespool

nimetatud komisjoni poolt nimetatud täiendavaid asutusi esitama eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjonile (PCLOB) perioodilisi aruandeid, sealhulgas asjaomasele asutusele laekunud väidetava rikkumisega seotud kaebuste arv, laad ja menetlemine. Põhikirjas, millega on asutatud eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon (PCLOB), nähakse ette, et komisjon võtab nende aruanded vastu ning, kui see on asjakohane, annab eraelu puutumatuse ja kodanikuvabaduste ametnikele soovitusi seoses nende tegevusega.

*IV LISA*

**Föderaalse kaubanduskomisjoni (FTC) esinaise Edith Ramirezi kiri**

7. juuli 2016

**E-POSTI TEEL**

Věra Jourová
Õigus- ja tarbijaküsimuste ning soolise võrdõiguslikkuse volinik
European Commission
Rue de la Loi/Wetstraat 200
1049 Brussels
Belgium

Lugupeetud volinik Jourová

USA föderaalne kaubanduskomisjon (Federal Trade Commission – FTC) hindab võimalust kirjeldada uue ELi–USA andmekaitseraamistiku Privacy Shield („andmekaitseraamistik Privacy Shield" või „raamistik") rakendamist. Usume, et see raamistik hakkab mängima olulist rolli selles, et hõlbustada eraelu puutumatust kaitsvaid kaubanduslikke tehinguid üha enam seotud maailmas. See võimaldab äriühingutel teha maailmamajanduses olulisi toimingud, tagades samal ajal, et ELi tarbijatele jääksid alles olulised privaatsuse kaitsemeetmed. Föderaalne kaubanduskomisjon on juba ammu võtnud endale kohustuse kaitsta eraelu puutumatust piiriüleselt ning seab uue raamistiku rakendamise esmatähtsale kohale. Allpool selgitame föderaalse kaubanduskomisjoni tugeva eraelu puutumatuse kaitse põhimõtete rakendamise ajalugu üldiselt, sealhulgas meie algse programmi Safe Harbor täitmist ning samuti föderaalse kaubanduskomisjoni lähenemisviisi uue raamistiku rakendamise kohta.

Föderaalne kaubanduskomisjon avalikustas programmi Safe Harbor rakendamise kohustuse esmakordselt 2000. aastal. Sel ajal saatis toonane föderaalse kaubanduskomisjoni esimees Robert Pitofsky Euroopa Komisjonile kirja, milles kirjeldati föderaalse kaubanduskomisjoni lubadust otsusekindlalt rakendada programmi Safe Harbor eraelu puutumatuse kaitse põhimõtted. Föderaalne kaubanduskomisjon (FTC) on täitnud seda kohustust ligi 40 täitemeetme, arvukate täiendavate uurimiste ja üksikute Euroopa andmekaitseasutustega koostöö kaudu vastastikuse huvi küsimuste kohta.

Pärast seda, kui Euroopa Komisjon väljendas 2013. aasta novembris muret programmi Safe Harbor haldamise ja rakendamise kohta, alustasime meie ja USA kaubandusministeerium konsulteerimist Euroopa Komisjoni ametnikega, et leida võimalusi programmi rakendamist tõhustada. Samal ajal, kui neid konsultatsioone peeti, tegi Euroopa Kohus 6. oktoobril 2015 otsuse kohtuasjas Schrems, mille kohaselt tunnistati muu hulgas kehtetuks Euroopa Komisjoni otsus programmi Safe Harbor asjakohaseuse kohta. Pärast selle otsuse tegemist jätkasime tihedat koostööd kaubandusministeeriumi ja Euroopa Komisjoniga, püüdes tugevdada ELi üksikisikute eraelu puutumatuse kaitset. Andmekaitseraamistik Privacy Shield on nende käimasolevate konsultatsioonide tulemus. Sarnaselt programmiga Safe Harbour, kohustub föderaalne kaubanduskomisjon käesolevaga otsusekindlalt rakendama uut raamistikku. Käesolev kiri tuletab seda kohustust meelde.

Nimelt kinnitame kohustuse võtmist neljas põhivaldkonnas: 1) taotluse prioriseerimine ja uurimised; 2) andmekaitseraamistiku Privacy Shield liikmelisusega seotud valede või pettusel põhinevate andmetega tegelemine; 3) pidev järelevalve korralduste üle; ning 4) suurenenud seotus ja rakendamisalane koostöö ELi andmekaitseasutustega. Allpool on üksikasjalikumalt kirjeldatud kõiki neid kohustusi ja asjaomast tausta seoses föderaalse kaubanduskomisjoni (FTC) rolliga kaitsta tarbijate eraelu puutumatust ja rakendada programmi Safe Harbor, samuti eraelu puutumatuse üldist olukorda Ameerika Ühendriikides ([1]).

I. TAUSTTEAVE

## A. **Föderaalse kaubanduskomisjoni (FTC) eraelu puutumatuse kaitse rakendamine ja poliitikaalane tegevus**

Föderaalsel kaubanduskomisjonil (FTC) on laiaulatuslik tsiviilõigusliku kaitse volitus selleks, et edendada tarbijakaitset ja konkurentsi kaubandussektoris. Oma tarbijakaitse volituste raames rakendab föderaalne kaubanduskomisjon mitmesuguseid seadusi, et kaitsta tarbijaandmete privaatsust ja turvalisust. Föderaalse kaubanduskomisjoni (FTC)

([1]) Anname täiendavat teavet USA föderaalsete ja riiklike eraelu puutumatusega seotud seaduste kohta A liites. Lisaks on kokkuvõte meie hiljutistest eraelu puutumatuse ja turvalisusega seotud täitemeetmetest kättesaadav föderaalse kaubanduskomisjoni (FTC) veebisaidil https://www.ftc.gov/reports/privacy-data-security-update-2015.

jõustatud esmane seadus, föderaalse kaubanduskomisjoni (FTC) seadus, keelustab ebaõiglased ja pettusel põhinevad tegevused või tavad kaubandussektori siseselt või seda mõjutades ([1]). Esitlemist, väljajätmist või tava peetakse pettusel põhinevaks, kui see on oluline ja viib asjaolusid arvestades mõistlikult käituvad tarbijad tõenäoliselt eksiteele ([2]).Tegu või tava on ebaõiglane, kui see põhjustab või võib põhjustada olulist kahju, mida tarbijad ei saa mõistlikult vältida või mida ei ole võimalik korvata tarbijatele või konkurentsile suunatud tasakaalustava hüvitisega ([3]). Samuti jõustab föderaalne kaubanduskomisjon (FTC) suunatud põhimäärusi, mis kaitsevad andmeid, mis on seotud tervishoiu, laenude ja muude finantsküsimustega, samuti laste internetipõhise teabega, ning on väljastanud määruseid, mis rakendavad kõiki neid põhimäärusi.

Föderaalse kaubanduskomisjoni (FTC) pädevust föderaalse kaubanduskomisjoni (FTC) seaduse raames kohaldatakse küsimustes, mis on seotud kaubandusega või seda mõjutavad. Föderaalsel kaubanduskomisjonil ei ole pädevust kriminaalõigust käsitlevate õigusaktide rakendamise ega julgeolekuküsimuste üle. Samuti ei ulatu föderaalse kaubanduskomisjoni (FTC) pädevus enamiku muude valitsuse tegevuseni. Lisaks sellele on föderaalse kaubanduskomisjoni (FTC) kaubandustegevuse kohase pädevuse suhtes kehtestatud erandid, sealhulgas seoses pankade, lennuettevõtjate, kindlustusäri ja telekommunikatsiooniteenuste pakkujate ühiste vedajate tegevusega. Samuti ei ole föderaalsel kaubanduskomisjonil pädevust enamike mittetulundusorganisatsioonide üle, kuid tal on pädevus pettuslike heategevusorganisatsioonide ja muude mittetulundusorganisatsioonide üle, mis tegelikkuses tegutsevad kasumi saamise nimel. Samuti on föderaalsel kaubanduskomisjonil (FTC) pädevus mittetulundusühingute üle, mis tegutsevad oma tulu teenivate liikmete kasumi nimel, pakkudes liikmetele sealhulgas olulisi majanduslikke hüvesid ([4]). Mõnel juhul kattub föderaalse kaubanduskomisjoni (FTC) pädevus muude õiguskaitseorganite pädevusega.

Oleme välja töötanud tugevad töösuhted föderaalsete ja riiklike asutustega ning teeme nendega tihedat koostööd, et koordineerida uurimisi ja esitada taotlusi, kui see on asjakohane.

Täitmise tagamine on föderaalse kaubanduskomisjoni eraelu puutumatuse kaitsmisega seotud lähenemisviisi oluline osa. Praeguseks on föderaalne kaubanduskomisjon tegelenud üle 500 juhtumiga, kaitstes tarbijaandmete privaatsust ja turvalisust. See juhtumite kogum sisaldab nii võrguühenduseta kui ka võrguühendusega saadud andmeid ning hõlmab suurte ja väikeste ettevõtjate vastu suunatud kaebusi, mille kohaselt ei ole nad nõuetekohaselt hoidnud tundlikke tarbijaandmeid, ei ole suutnud kaitsta tarbijate isikuandmeid, petturlikul teel jälitanud tarbijaid veebis, saatnud tarbijatele rämpsposti, paigaldanud tarbijate arvutisse nuhkvara või muud õelvara, rikkunud helistamise põhimõtet ja muid teleturunduse eeskirju ning valesti kogunud ja jaganud tarbijate andmeid mobiiliseadmetes. Föderaalse kaubanduskomisjoni täitmise tagamisega seotud tegevus – nii füüsilises kui ka digitaalses maailmas – saadab olulise sõnumi ettevõtjatele tarbija privaatsuse kaitsmise vajaduse kohta.

Samuti on föderaalne kaubanduskomisjon alustanud mitmete poliitiliste algatustega, mille eesmärk on tõhustada tarbijate eraelu puutumatuse kaitset ja millest ta täitmise tagamisel juhindub. Föderaalne kaubanduskomisjon on korraldanud töötube ja väljastanud aruandeid, milles soovitatakse parimaid tavasid eraelu puutumatuse kaitse parandamiseks mobiilses ökosüsteemis; andmevahetustööstuse läbipaistvuse suurendamist; mahukatest andmetest saadava kasu maksimeerimist, leevendades sealjuures sellega seotud riske, eelkõige madala sissetulekuga ja haavatavate tarbijate jaoks; ning tõstnud esile muu hulgas näo tuvastamise ja asjade interneti mõju eraelu puutumatuse kaitsele ja turvalisusele.

Föderaalne kaubanduskomisjon tegeleb ka tarbijate ja ettevõtjate koolitamisega, et tõhustada täitmise tagamise mõju ja poliitilisi arengualgatusi. Föderaalne kaubanduskomisjon on kasutanud mitmesuguseid vahendeid – väljaanded, veebipõhised ressursid, töötoad ja sotsiaalmeedia –, et tagada õppematerjalide olemasolu mitmesuguste teemade kohta, sealhulgas mobiilirakendused, laste turvalisus ja andmete turvalisus. Viimati käivitas komisjon oma algatuse Start With Security, mis hõlmab nendele ettevõtjatele suunatud uusi juhiseid, mis tuginevad andmete turvalisusega seotud juhtumitest tulenevatele õppetundidele, ning rea töötubasid üle kogu riigi. Lisaks sellele on föderaalne kaubanduskomisjon olnud pikka aega tarbijatele suunatud peamise arvutiturbe eestvedaja. Eelmisel aastal külastati meie veebisaiti OnGuard Online ja selle hispaaniakeelset versiooni Alerta en Línea rohkem kui 5 miljonit korda.

### B. **USA õiguskaitse, millest saavad kasu ELi tarbijad**

Raamistikku kohaldatakse USA eraelu puutumatuse üldisema olukorra kontekstis, millega kaitstakse ELi tarbijaid mitmel viisil.

([1]) 15 U.S.C. § 45(a).
([2]) Vt FTC Policy Statement on Deception, appended to Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984), kättesaadav aadressil: https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.
([3]) Vt 15 U.S.C § 45(n); FTC Policy Statement on Unfairness, appended to Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984), kättesaadav aadressil: https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.
([4]) Vt California Dental Ass'n vs. FTC, 526 U.S. 756 (1999).

Föderaalse kaubanduskomisjoni seadusest tulenev ebaõiglaste ja pettusel põhinevate teguviiside ja tavade keelustamine ei piirdu üksnes USA tarbijate kaitsmisega USA ettevõtjate eest, kuna see hõlmab ka neid tavasid, mis 1) põhjustavad või võivad põhjustada mõistlikult ettearvatavat kahju Ameerika Ühendriikides või 2) osutavad konkreetsele käitumisviisile Ameerika Ühendriikides. Lisaks sellele saab föderaalne kaubanduskomisjon kasutada kõiki õiguskaitsevahendeid, sealhulgas tagastamine, mis on olemas selleks, et kaitsta valisriigi tarbijate kaitsmisel kodumaiseid tarbijaid.

Föderaalse kaubanduskoja täitmise tagamisega seotud tegevus toob tõepoolest märkimisväärset kasu nii USA-le kui ka välisriigi tarbijatele. Näiteks on föderaalse kaubanduskoja seaduse 5. jaotise täitmisega seotud juhtumid kaitsnud sarnaselt nii USA kui ka välisriigi tarbijate eraelu puutumatust. Juhtumis teabevahendaja Accusearchi vastu väitis föderaalne kaubanduskomisjon, et ettevõtja konfidentsiaalsete telefonikõnede salvestuste müük kolmandatele isikutele ilma tarbijate teadmiseta või nõusolekuta oli kõlvatu tava, millega rikuti föderaalse kaubanduskomisjoni seaduse paragrahvi 5. Accusearch müüs nii USA kui ka välisriikide tarbijatega seotud andmeid ([1]). Accusearchile esitati kohtulik keeld, mille kohaselt keelustatakse muu hulgas tarbijate isikuandmete turundamine või müük ilma kirjaliku nõusolekuta, välja arvatud juhul, kui need on seaduslikult saadud avalikkusele kättesaadava teabe hulgast, ning kohus kehtestas ligikaudu 200 000 USA dollari suuruse trahvi ([2]).

Teine näide on föderaalse kaubanduskoja kokkulepe TRUSTe-ga. Sellega tagatakse, et tarbijad, sealhulgas Euroopa Liidus asuvad tarbijad, saavad tugineda esitlustele, mida ülemaailmne isereguleeruv organisatsioon teeb kodumaiste ja välisriigi veebipõhiste teenuste läbivaatamise ja sertifitseerimise kohta ([3]). Tähtis on see, et meie tegevus TRUSTe vastu tugevdab ka eraelu puutumatuse kaitse isereguleeruvat süsteemi laiaulatuslikumalt, tagades nende üksuste usaldusväärsuse, mis mängivad olulist rolli isereguleeruvates kavades, sealhulgas piiriülesed eraelu puutumatuse kaitse raamistikud.

Samuti tagab föderaalne kaubanduskomisjon muude suunatud seaduste täitmist, mille kaitse laieneb mitte-ameeriklastest tarbijatele, näiteks internetis laste eraelu puutumatuse kaitse seadus (Children's Online Privacy Protection Act – COPPA). Muu hulgas nõutakse internetis laste eraelu puutumatuse kaitse seaduses, et lastele suunatud veebisaitide ja internetipõhiste teenuste või teadlikult alla 13-aastastelt lastelt isikuandmeid koguvad üldkasutatavate kommertsveebisaitide haldajad teatavad sellest vanematele ning saavad tõestatava vanemate nõusoleku. Internetis laste eraelu puutumatuse kaitse seaduse kohaldamisalasse kuuluvad ja välisriikides elavate laste isikuandmeid koguvad USA veebisaidid ja teenused peavad olema kooskõlas internetis laste eraelu puutumatuse kaitse seadusega. Välisriikide veebisaidid ja internetipõhised teenused peavad olema samuti kooskõlas internetis laste eraelu puutumatuse kaitse seadusega, kui need on suunatud Ameerika Ühendriikides elavatele lastele või kui need koguvad teadlikult Ameerika Ühendriikides elavate laste isikuandmeid. Lisaks föderaalse kaubanduskomisjoni poolt jõustatud USA föderaalsetele seadustele on olemas teatavad muud föderaalsed ja riiklikud tarbijakaitse ja privaatsuse seadused, mis võivad tuua täiendavat kasu ELi tarbijatele.

## C. **Programmi Safe Harbor jõustamine**

Osana oma eraelu puutumatuse kaitse ja turvalisuse tagamise programmist on föderaalne kaubanduskomisjon otsinud ka viise, et kaitsta ELi tarbijaid, esitades täitmise tagamisega seotud kaebusi, mis hõlmavad programmi Safe Harbor rikkumisi. Föderaalne kaubanduskoda on esitanud 39 programmi Safe Harbor jõustamisega seotud kaebust: 36 väidetavalt valet sertifitseerimisega seotud väidet ning kolm juhtumit Google'i, Facebooki ja Myspace'i vastu, mis hõlmavad väidetavat programmi Safe Harbor eraelu puutumatuse kaitse põhimõtete rikkumist ([4]). Need juhtumid tõestavad sertifikaatide rakendatavust ja nõuete täitmata jätmise tagajärgi. Vastaspoole nõusolekul 20 aastaks kehtestatud korraldusega nõutakse, et Google, Facebook ja Myspace rakendaksid laiaulatuslikke eraelu puutumatuse kaitse programme, mis tuleb mõistlikult koostada nii, et need käsitleksid uute ja olemasolevate toodete ja teenuste väljatöötamise ja haldamisega seotud eraelu puutumatuse riske ja kaitseksid isikuandmete privaatsust ja konfidentsiaalsust. Nende korralduste alusel tuleb põhjalikes eraelu puutumatuse kaitse programmides määratleda prognoositavad olulised riskid ning meetmed nende riskidega tegelemiseks. Samuti peavad ettevõtjad esitama järjepidevaid sõltumatuid hinnanguid oma eraelu puutumatuse kaitse programmide kohta, mis tuleb edastada föderaalsele kaubanduskomisjonile. Samuti keelatakse korraldustega nendel ettevõtjatel valeandmete esitamine seoses nende eraelu puutumatuse kaitse tavadega ja osalemisega mis tahes eraelu puutumatuse kaitse või turvalisusega seotud programmis. Seda keelustamist

([1]) Vt Office of the Privacy Commissioner of Canada, Complaint under PIPEDA against Accusearch, Inc., doing business as Abika.com, https://www.priv.gc.ca/cf-dc/2009/2009_009_0731 e.asp. Kanada eraelu puutumatuse voliniku amet esitas lühidalt *amicus curiae* föderaalse kaubanduskomisjoni (FTC) meetme apelleerimiseks ning teostas oma uurimise, järeldades, et Accusearchi tavad rikkusid ka Kanada õigust.

([2]) Vt FTC *vs.* Accusearch, Inc., No. 06CV015D (D. Wyo. Dec. 20, 2007), *aff'd* 570 F.3d 1187 (10th Cir. 2009).

([3]) Vt *In the Matter of True Ultimate Standards Everywhere, Inc.*, No. C-4512 (F.T.C. Mar. 12, 2015) (decision and order), https://www ftc.gov/system/files/documents/cases/150318trust-edo.pdf.

([4]) Vt *In the Matter of Google, Inc.*, No. C-4336 (F.T.C. Oct. 13 2011) (decision and order), https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz; *In the Matter of Facebook, Inc.*, No. C-4365 (F.T.C. July 27, 2012) (decision and order), https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook; *In the Matter of Myspace LLC*, No. C-4369 (F.T.C. Aug. 30, 2012) (decision and order), https://www.ftc.gov/news-events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace.

kohaldatakse uue andmekaitseraamistiku Privacy Shield alusel ka ettevõtjate toimingute ja tavade suhtes. Föderaalne kaubanduskomisjon saab need korraldused täitmisele pöörata, kohaldades tsiviilõiguses ette nähtud karistusi. Tegelikult maksis Google 2012. aastal trahvi rekordiliselt 22,5 miljonit dollarit, et lahendada juhtum, milles väideti, et ta oli ta rikkunud FTC korraldust. Järelikult aitavad need föderaalse kaubanduskomisjoni korraldused kaitsta rohkem kui miljardit tarbijat üle kogu maailma, kellest sajad miljonid elavad Euroopas.

Föderaalse kaubanduskomisjoni (FTC) juhtumites on pööratud tähelepanu ka programmis Safe Harbor osalemisega seotud valedele, pettusel põhinevatele või eksitavatele andmetele. Föderaalne kaubanduskomisjon võtab neid väiteid tõsiselt. Näiteks kohtuasjas föderaalne kaubanduskomisjon *(FTC) vs. Karnani* algatas föderaalne kaubanduskomisjon 2011. aastal menetluse Ameerika Ühendriikide veebipõhise turustaja vastu, väites, et tema ja tema ettevõte olid pannud Briti tarbijad ekslikult uskuma, et ettevõte asub Ühendkuningriigis, sealhulgas kasutades.uk veebilaiendeid ja viidates Briti valuutale ja Ühendkuningriigi postisüsteemile ([1]). Kui aga tarbijad said tooted kätte, avastasid nad, et peavad ootamatult maksma imporditollimakse, et toodete garantii ei kehtinud Ühendkuningriigis ning et toodete eest raha tagasisaamisega on seotud kulud. Samuti väitis föderaalne kaubanduskomisjon (FTC), et kostjad petsid tarbijaid seoses osalemisega programmis Safe Harbor. Nimelt asusid kõik tarbijatest ohvrid Ühendkuningriigis.

Paljud meie teistest programmi Safe Harbor täitmise tagamisega juhtumitest hõlmasid programmiga Safe Harbor liitnud organisatsioone, mis ei uuendanud oma iga-aastast sertifikaati, kuid väitsid samas jätkuvalt, et osalevad programmis. Nagu allpool täpsemalt käsitletud, on föderaalne kaubanduskomisjon pühendunud andmekaitseraamistikus Privacy Shield osalemisega seotud väärate väidete menetlemisele. See strateegiline täitmise tagamise alane tegevus täiendab kaubandusministeeriumi tõhustatud meetmeid, et tõendada vastavust programminõuetele sertifitseerimise ja uuesti sertifitseerimise eesmärgil, selle tõhusa järgimise jälgimist, sealhulgas raamistikus osalejatele suunatud küsimustike kasutamise kaudu, ning selle suurenenud jõupingutusi, et määratleda valed väited raamistikus osalemise kohta ning raamistiku sertifitseerimistähise kuritarvitamine ([2]).

## II. TAOTLUSTE PRIORISEERIMINE JA UURIMINE

Sarnaselt programmile Safe Harbor kohustub föderaalne kaubanduskomisjon seadma esikohale ELi liikmesriikidest pärit andmekaitseraamistikuga Privacy Shield seotud kaebusi. Samuti seame esikohale andmekaitseraamistikuga Privacy Shield seotud iseregulatsioonijuhiste järgimata jätmise kohta esitatud kaebused ja pärit eraelu puutumatuse kaitse iseregulatsiooniorganitelt ja muudelt sõltumatutelt vaidluste lahendamise organitelt.

Selleks et hõlbustada ELi liikmesriikide raamistiku alusel taotluste esitamist, loob föderaalne kaubanduskomisjon standardse kaebemenetluse ning annab ELi liikmesriikidele juhiseid selle teabe liigi kohta, mis võiks parimal viisil abistada föderaalset kaubanduskomisjoni taotlusega seotud päringu tegemisel. Osana sellest jõupingutusest määrab föderaalne kaubanduskomisjon ELi liikmesriigist pärit kaebuste jaoks asutuse kontaktpunkti. Väga kasulik on see, kui taotlev asutus on teinud eelneva päringu väidetava rikkumise kohta ja saab föderaalse kaubanduskomisjoniga teha uurimise käigus koostööd.

ELi liikmesriigilt või isereguleeruvalt organilt saadud kaebuse laekumise korral saab föderaalne kaubanduskoda võtta mitmeid meetmeid, et tõstatatud teemadega tegeleda. Näiteks võime läbi vaadata ettevõtja eralu puutumatuse kaiste põhimõtted, saada täiendavat teavet otse ettevõtjalt või kolmandatelt isikutelt, teha koostööd kaebuse esitanud üksusega, hinnata, kas esineb rikkumisi või on mõjutatud märkimisväärne hulk tarbijaid, määrata, kas kaebus hõlmab kaubandusministeeriumi haldusalasse jäävaid küsimusi, hinnata, kas tarbijate ja ettevõtjate koolitamine oleks kasulik ning vajadusel algatada täitemenetlus.

Samuti on föderaalne kaubanduskomisjon kohustatud vahetama kaebusega seotud teavet kaebuse esitanud täitevasutustega, sealhulgas selle kohta, millises menetlusetapis kaebus on, mille suhtes kohaldatakse konfidentsiaalsusega seotud norme ja piiranguid. Võimaluste piires laekunud kaebuste arvu ja liiki arvestades, hõlmavad esitatud andmed osutatud teemade hindamist, sealhulgas oluliste tõstatatud küsimuste kirjeldust ning kõikide meetmeid, mis võetakse föderaalse kaubanduskomisjoni pädevuses, et käsitleda õigusrikkumist. Samuti annab föderaalne kaubanduskomisjon kaebuse esitanud asutusele tagasisidet laekunud kaebuste liikide kohta, et suurendada õigusvastase käitumise

([1]) Vt FTC *vs.* Karnani, No. 2:09-cv-05276 (C.D. Cal. May 20, 2011) (stipulated final order), https://www.ftc.gov/sites/default/files/documents/cases/2011/06/110609karnanistip.pdf; *vt ka* Lesley Fair, FTC Business Center Blog, *Around the World in Shady Ways*, https://www.ftc.gov/blog/2011/06/around-world-shady-ways (9 juuni 2011).

([2]) Kiri väliskaubandusameti aseriigisekretäri kohusetäitjalt rahvusvahelise kaubanduse alal Ken Hyattilt õigus- ja tarbijaküsimuste ning soolise võrdõiguslikkuse volinikule Věra Jourovále.

ärahoidmisega seotud jõupingutuste tõhusust. Juhul kui taotlev täitevasutus otsib teavet teatava kaebuse menetlusetapi kohta oma täitemenetluse teostamise eesmärgil, vastab föderaalne kaubanduskoda selliselt, et võtab arvesse vaatlusaluste kaebuste arvu, mille suhtes kohaldatakse konfidentsiaalsus- ja muid õiguslikke nõudeid.

Samuti teeb föderaalne kaubanduskomisjon tihedat koostööd ELi andmekaitseasutustega, et pakkuda täitmise tagamisel abi. Asjaomastel juhtudel võib see hõlmata andmete jagamist ja uurimisalast abi vastavalt USA turvalise võrgu seadusele (SAFE WEB Act), millega volitatakse föderaalset kaubanduskomisjoni abistama välisriigi õiguskaitseasutusi juhul, kui välisriigi asutus tagab selliste õigusnormide täitmise, millega keelustatakse tavad, mis on sisuliselt sarnased nendele, mis on keelatud seadustega, mille täitmist föderaalse kaubanduskomisjon tagab ([1]). Osana sellest abist saab föderaalne kaubanduskomisjon jagada andmeid, mis on saadud seoses föderaalse kaubanduskomisjoni poolse uurimisega, viia läbi kohustuslikke menetlusi ELi andmekaitseasutuste nimel, kes teostavad oma uurimist, ning kuulata tunnistajate või vastustajate ütlusi seoses andmekaitseasutuste täitemenetlustega, mille suhtes kohaldatakse USA turvalise võrgu seadust (SAFE WEB Act). Föderaalne kaubanduskomisjon kasutab regulaarselt seda volitust, et abistada muid asutusi üle kogu maailma eraelu puutumatuse ja tarbijakaitsega seotud juhtumites ([2]).

Lisaks ELi liikmesriikidest ja eraelu puutumatusega seotud isereguleeruvatest organitest pärit andmekaitseraamistiku Privacy Shield kaebuste esikohale seadmisele ([3]) kohustub föderaalne kaubanduskomisjon uurima võimalikke raamistiku rikkumisi omal algatusel, kui see on asjakohane, kasutades selleks vajalikke vahendeid.

Juba tublisti üle kümne aasta on föderaalne kaubanduskomisjon säilitanud jõulise programmi kaubandusorganisatsioone hõlmavate eraelu puutumatuse kaitse ja turvalisusega seotud küsimuste uurimisega. Osana nendest uurimistest kontrollis föderaalne kaubanduskomisjon regulaarselt, kas asjaomane üksus esitas programmi Safe Harbor kinnitusi. Juhul kui üksus esitas selliseid kinnitusi ja uurimise käigus selgus, et programmi Safe Harbor eraelu puutumatuse kaitse põhimõtteid on ilmselgelt rikutud, lisas föderaalne kaubanduskomisjon väited programmi Safe Harbori rikkumise kohta oma täitemeetmete kohaldamise hulka. Meil on uue raamistiku alusel kavas seda ennetavat lähenemisviisi jätkata. Oluline on see, et föderaalne kaubanduskomisjon teostab palju rohkem uurimisi võrreldes nendega, mille kohta esitatakse lõpptulemusena kaebus. Paljud föderaalse kaubanduskomisjoni uurimised on lõpetatud, sest töötajad ei tuvasta ilmset õigusrikkumist. Kuna föderaalse kaubanduskomisjoni uurimised on mitteavalikud ja konfidentsiaalsed, siis uurimise lõpetamist sageli ei avalikustata.

Föderaalse kaubanduskoja algatatud ligi 40 täitmisemeedet, mis hõlmavad programmi Safe Harbor, tõendavad asutuse võetud kohustust ennetavalt jõustada piiriülesed eraelu puutumatuse kaitse programmid. Föderaalne kaubanduskomisjon otsib võimalikke raamistikuga seotud rikkumisi osana eraelu puutumatuse kaitse ja turvalisuse uurimistest, mida viime läbi regulaarselt.

## III. ANDMEKAITSERAAMISTIKUS PRIVACY SHIELD OSALEMISEGA SEOTUD VALEDE VÕI PETTUSEL PÕHINEVATE ANDMETEGA TEGELEMINE

Nagu eespool viidatud, võtab föderaalne kaubanduskomisjon meetmed nende üksuste vastu, kes on vääralt väitnud, et osalevad raamistikus. Esmajärjekorras võtab föderaalne kaubanduskomisjon arvesse kaubandusministeeriumilt laekunud kaebusi, mis on seotud organisatsioonidega, kelle puhul on ministeerium avastanud, et nad väidavad ebaseaduslikult end olevat raamistiku praeg used liikmed või kasutavad mis tahes raamistiku sertifitseerimistähist ilma loata.

Lisaks sellele märgime, et juhul kui organisatsiooni eraelu puutumatuse kaitse põhimõtetes on ette nähtud, et ta tegutseb kooskõlas andmekaitseraamistiku Privacy Shield põhimõtetega, siis organisatsiooni suutmatus ennast kaubandusministeeriumis registreeruda või registreeringut säilitada tõenäoliselt ei välista iseenesest seda, et föderaalse kaubanduskomisjoni nõuab organisatsioonilt raamistikuga seotud kohustuste täitmist.

---

([1]) Selle otsustamisel, kas kasutada oma USA turvalise võrgu seaduse (U.S. SAFE WEB Act) kohaseid volitusi, kaalub föderaalne kaubanduskomisjon muu hulgas: „A) kas taotlev asutus on nõustunud andma või annab tulevikus komisjonile vastastikust abi; B) kas taotlusele vastavus kahjustaks Ameerika Ühendriikide avalikku huvi; ning C) kas taotleva asutuse uurimis- või jõustamismenetlus on seotud seaduste või tavadega, mis kahjustavad või tõenäoliselt toovad kahju märkimisväärsel hulgal inimestele.“ 15 U.S.C. § 46(j)(3). Asjaomase volituse suhtes ei kohaldata konkurentsiõiguse rakendamise seadusi.

([2]) Näiteks majandusaastatel 2012–2015 kasutas föderaalne kaubanduskomisjon oma USA turvalise võrgu seaduse kohaseid volitusi, et jagada teavet vastusena peaaegu 60 päringule, mis olid pärit välisriigi asutustest, ning ta väljastas ligi 60 tsiviiluurimise nõudmist (samaväärne halduskorraldustega), et abistada 25 välisriigis toimuvat uurimist.

([3]) Kuigi föderaalne kaubanduskomisjon ei lahenda ega vahenda üksikuid tarbijakaebusi, kinnitab föderaalne kaubanduskomisjon, et seab ELi andmekaitseasutustest pärit andmekaitseraamistikuga Privacy Shield seotud kaebused esikohale. Lisaks kasutab föderaalne kaubanduskomisjon kaebusi oma andmebaasis Consumer Sentinel, mis on kättesaadav paljudele muudele õiguskaitseorganitele, eesmärgiga tuvastada arengusuunad, määratleda jõustamisalased prioriteedid ning teha kindlaks võimalikud uurimisalased eesmärgid. ELi üksikisikud saavad föderaalsele kaubanduskomisjonile kaebuste esitamiseks kasutada USA kodanikega sama süsteemi: www.ftc.gov/complaint. Siiski võib üksikute andmekaitseraamistiku Privacy Shield kaebuste korral olla ELi üksikisikutel kõige kasulikum esitada kaebused asjaomase liikmesriigi andmekaitseasutusele või vaidluste kohtuvälise lahendamise teenuse osutajale.

IV. KORRALDUSTE JÄLGIMINE

Samuti kinnitab föderaalne kaubanduskomisjon oma kohustust jälgida täitekorraldusi, et tagada vastavus andmekaitseraamistikule Privacy Shield.

Raamistikule vastavust nõuame tulevastes föderaalse kaubanduskomisjoni raamistikuga seotud korraldustes mitmesuguste asjaomaste keelavate sätete kaudu. See hõlmab raamistiku ja muude eraelu puutumatuse kaitse programmidega seotud valeandmete esitamise keelustamist juhul, kui need moodustavad föderaalse kaubanduskomisjoni alusmeetme aluse.

Föderaalse kaubanduskomisjoni juhtumid, millega tagatakse esialgse programmi Safe Harbor täitmist, on kasulikud. Programmi Safe Harbor sertifitseerimisega seotud valesid või pettusel põhinevaid andmeid hõlmava 36 juhtumi korral keelatakse iga korraldusega vastustajal moonutada teavet oma osalemise kohta programmis Safe Harbor või muus eraelu puutumatuse kaitse või turvalisusega seotud programmis ning ettevõtjatelt nõutakse vastavusaruannete esitamist föderaalsele kaubanduskomisjonile. Programmi Safe Harbor eraelu puutumatuse kaitse põhimõtete rikkumist hõlmanud juhtumite korral on ettevõtjad olnud kohustatud rakendama põhjalikke eraelu puutumatuse programme ning saama kolmandatelt isikutelt sõltumatuid hinnanguid nende programmide kohta igal teisel aastal kahekümne aasta jooksul, ning need tuleb neil esitada föderaalsele kaubanduskomisjonile.

Föderaalse kaubanduskomisjoni halduskorralduste rikkumine võib viia tsiviilõiguslike trahvideni summas kuni 16 000 USA dollarit rikkumise kohta või 16 000 USA dollarit päevas jätkuva rikkumise korral, ([1]) mis paljusid tarbijaid mõjutavate tavade korral võivad ulatuda miljonite dollariteni. Kõikidel korraldustel on ka aruandluse ja vastavussätted. Korraldusele alluvad üksused peavad säilitama dokumendid, millega tõendatakse, et nad on kindlal arvul aastatel põhimõtteid järginud. Korraldusi tuleb jagada ka töötajatega, kes vastutavad korralduse järgimise tagamise eest.

Föderaalne kaubanduskomisjon jälgib vastavust programmi Safe Harbor korraldustele, nagu ta teeb kõikide oma korraldustega. Föderaalne kaubanduskomisjon võtab eraelu puutumatuse kaitse ja andmete turvalisusega seotud korralduste täitmise tagamist tõsiselt ning võtab meetmed, et need vajadusel täitmisele pöörata. Nagu eespool nimetatud, maksis näiteks Google 22,5 miljoni dollari suuruse tsiviilõigusliku trahvi, et lahendada juhtum, milles väideti, et ta oli ta rikkunud föderaalse kaubanduskomisjoni korraldust. Oluline on see, et föderaalse kaubanduskomisjoni korraldustega jätkatakse ülemaailmselt kõikide tarbijate kaitsmist, kes ettevõtjatega suhtlevad, mitte ainult nende tarbijate kaitsmist, kes on esitanud kaebusi.

Viimasena jätkab föderaalne kaubanduskomisjon nende ettevõtjate veebipõhise loetelu haldamist, kes peavad täitma nii programmiga Safe Harbor kui ka uue andmekaitseraamistiku Privacy Shield alusel saadud korraldusi ([2]). Lisaks sellele nõutakse andmekaitseraamistiku Privacy Shield põhimõtete alusel nendelt ettevõtjatelt, kes peavad täitma põhimõtete mittevastavuse alusel tehtud föderaalse kaubanduskomisjoni või kohtu korraldust kõikide föderaalsele kaubanduskomisjonile esitatud asjaomaste raamistikuga seotud vastavuse või hindamisega seotud aruannete avalikustamist sellises ulatuses, mis on kooskõlas konfidentsiaalsust käsitlevate normide ja eeskirjadega.

V. SEOTUS ELI ANDMEKAITSEASUTUSTEGA JA TÄITMISE TAGAMISE ALANE KOOSTÖÖ

Föderaalne kaubanduskomisjon tunnistab seda olulist rolli, mida ELi andmekaitseasutused mängivad seoses raamistikule vastavusega ning julgustab pidama rohkem konsultatsioone ja tegema rohkem täitmisalast koostööd. Lisaks kõikidele konsultatsioonidele osutavate andmekaitseasutustega juhtumipõhiste küsimuste kohta kohustub föderaalne kaubanduskomisjon osalema perioodilistel kohtumistel, millest võtavad osa artikli 29 töörühma määratud esindajad, eesmärgiga arutada üldiselt, kuidas parendada täitmise tagamise alast koostööd seoses raamistikuga. Lisaks osaleb föderaalne kaubanduskomisjon koos kaubandusministeeriumi, Euroopa Komisjoni ja artikli 29 kohase töörühma esindajatega raamistiku iga-aastasel läbivaatamisel, et arutada selle rakendamist.

Samuti julgustab föderaalne kaubanduskomisjon selliste vahendite väljatöötamist, mis suurendavad täitmise tagamise alast koostööd ELi andmekaitseasutuste ja muude ülemaailmsete eraelu puutumatuse kaitsega seotud jõustamisasutustega. Nimelt käivitas föderaalne kaubanduskomisjon koos Euroopa Liidu ja ülemaailmsete partneritega eelmisel aastal ülemaailmse eraelu puutumatuse kaitse tagamise võrgustiku (Global Privacy Enforcement Network – GPEN) siseselt hoiatussüsteemi, et jagada teavet uurimiste kohta ja edendada täitmise tagamise alast koordineerimist. See GPEN-i hoiatusvahend võiks olla eriti kasulik andmekaitseraamistiku Privacy Shield kontekstis. Föderaalne kaubanduskomisjon ja ELi andmekaitseasutused võiksid seda kasutada raamistiku ja muude privaatsuse uurimistega seotud koordineerimiseks, sealhulgas teabe jagamise alguspunktina, et tagada tarbijate jaoks koordineeritud ja tõhusam privaatsuse kaitse. Loodame

([1]) 15 U.S.C. § 45(m); 16 C.F.R. § 1.98.

([2]) Vt FTC, Business Center, Legal Resources, https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field-consumer-protection-topics-tid=251.

jätkata koostööd osalevate ELi asutustega, et juurutada GPEN-i häiresüsteemi ulatuslikumalt ja välja töötada muid vahendeid, et parendada täitmise tagamise alast koostööd eraelu puutumatusega seotud juhtumite korral, sealhulgas need, mis hõlmavad raamistikku.

Föderaalsel kaubanduskojal on hea meel kinnitada oma tahet jõustada uut andmekaitseraamistikku Privacy Shield. Samuti loodame teha jätkuvat koostööd oma ELi kolleegidega, sest tegeleme koos tarbijaprivaatsuse kaitsmisega mõlemal pool Atlandi ookeani.

Lugupidamisega

Edith Ramirez

Esinaine

*A liide*

## ELi–USA andmekaitseraamistik Privacy Shield'i kontekst: Ülevaade eraelu puutumatuse ja turvalisuse olukorrast USAs

ELi–USA andmekaitseraamistiku Privacy Shield („raamistik") pakutav kaitsetase kuulub USA õigussüsteemi kui terviku poolt tagatava laiema eraelu puutumatuse kaitse konteksti. Esiteks on USA föderaalsel kaubanduskomisjonil (Federal Trade Commission – FTC) USA äritegevusele suunatud jõuline eraelu puutumatuse ja andmekaitseprogramm, mis kaitseb tarbijaid üle kogu maailma. Teiseks on tarbijate eraelu puutumatuse ja turvalisuse kaitse olukord Ameerika Ühendriikides märkimisväärselt edasi arenenud alates 2000. aastast, mil võeti vastu esialgne USA – ELi Safe Harbour programm. Sellest ajast on kehtestatud mitmeid föderaalseid ja riiklikke eraelu puutumatuse ja turvalisusega seotud seadusi ning avaliku- ja erasektori kohtuvaidluste arv eraelu puutumatuse õiguse jõustamiseks on oluliselt kasvanud. USA laiaulatuslik õiguskaitse tarbijate eraelu puutumatusele ja turvalisusele, mida andmete suhtes äritavades rakendatakse, täiendab kaitset, mida ELi üksikisikutele uue raamistikuga pakutakse.

### I. FÖDERAALSE KAUBANDUSKOMISJONI ÜLDINE ERAELU PUUTUMATUSE JA TURVALISUSE JÕUSTAMISE PROGRAMM

Föderaalne kaubanduskomisjon on juhtiv USA tarbijakaitseasutus, mis keskendub eraelu puutumatusele ärisektoris. Föderaalsel kaubanduskomisjonil on pädevus vastutusele võtta ebaõiglaste või petturlike tegevuste või tavade eest, mis rikuvad tarbijate eraelu puutumatust, ning jõustada sihipärasemaid eraelu puutumatust käsitlevaid seadusi, mis kaitsevad teatavat finants- ja tervisealast teavet, teavet laste kohta ja teavet, mida kasutatakse teatavate valikuotsuste tegemiseks tarbijate kohta.

Föderaalsel kaubanduskomisjonil on hindamatu kogemus tarbijate eraelu puutumatuse tagamisel. Föderaalne kaubanduskomisjon on võtnud täitemeetmeid ebaseaduslike tavade suhtes nii väljaspool võrgukeskkonda kui ka võrgukeskkonnas. Näiteks on föderaalne kaubanduskomisjon algatanud täitemeetmeid selliste tuntud äriühingute nagu Google, Facebook, Twitter, Microsoft, Wyndham, Oracle, HTC ja Snapchat, aga ka vähemtuntud äriühingute vastu. Föderaalne kaubanduskomisjon on hagenud ettevõtteid, kes väidetavalt spämmisid tarbijaid, installeerisid arvutitesse nuhkvara, ei taganud tarbijate isikuandmete kaitset, petlikult jälitasid tarbijaid võrgukeskkonnas, rikkusid laste privaatsust, kogusid seadusevastaselt teavet tarbijate mobiilseadmete kohta ega suutnud tagada isikuandmete salvestamiseks kasutatavate internetiga ühendatud seadmete turvalisust. Selle tulemusena välja antud korraldused on tavaliselt ette näinud, et föderaalne kaubanduskomisjon peab kahekümne aasta jooksul pidevat jälgimist teostama, on keelustanud edasised seaduserikkumised ning on ettevõtetele ette näinud suured rahatrahvid korralduse rikkumise ees ([1]). Oluline on siinjuures, et föderaalse kaubanduskomisjoni korraldused ei kaitse lihtsalt üksikisikuid, kes kaebasid mõne probleemi pärast, vaid need kaitsevad kõiki tarbijaid, kes teevad tegemist edasitöötava ettevõttega. Piiriüleses kontekstis on föderaalsel kaubanduskomisjonil pädevus kaitsta tarbijaid kogu maailmas Ameerika Ühendriikides aset leidvate tegevuste eest ([2]).

Praeguseks on föderaalne kaubanduskomisjon esitanud hagi üle 130 spämmi ja nuhkvara juhtumi, üle 120 „Ära helista" telefonimüügi juhtumi, üle 100 õiglase krediidiinfo seadust (Fair Credit Reporting Act) puudutava juhtumi kohta, enam kui 50 hagi üldistes eraelu puutumatuse küsimustes, peaaegu 30 hagi seaduse Gramm-Leach-Bliley Act rikkumises ja üle 20 hagi internetis laste eraelu puutumatuse kaitse seaduse (Children's Online Privacy Protection Act – COPPA) jõustamiseks ([3]). Lisaks nendele juhtumitele on föderaalne kaubanduskomisjon välja andnud ja avaldanud hoiatavaid kirju ([4]).

([1]) Föderaalse kaubanduskomisjoni korralduse täitmata jätnud üksusele rakendatakse tsiviiltrahvi kuni 16 000 USA dollarit rikkumise kohta, või 16 000 USA dollarit päevas jätkuva rikkumise eest. *Vt* 15 U.S.C § 45(l); 16 C.F.R. § 1.98(c).

([2]) Kongress on selgesõnaliselt kinnitanud föderaalse kaubanduskomisjoni pädevust õiguskaitse kasutamiseks, sealhulgas hüvitamine mis tahes tegude või tavade eest seoses väliskaubandusega, mis 1) põhjustavad või võivad põhjustada mõistlikult ettenähtavat kahju Ameerika Ühendriikides või 2) hõlmavad olulisi tegusid Ameerika Ühendriikides. *Vt* 15 U.S.C. § 45(a)(4).

([3]) Mõnel juhul viitavad komisjoni eraelu ja isikuandmete puutumatust käsitlevad juhtumid sellele, et äriühing on nii petnud kui ka kõlvatult käitunud; kõnealuste juhtumite puhul on mõnikord väidetavalt rikutud mitmeid õigusakte, nagu õiglase krediidiinfo seadust (Fair Credit Reporting Act), seadust Gramm-Leach-Bliley Act ja internetis laste eraelu puutumatuse kaitse seadust (COPPA).

([4]) Vt nt 22. detsembri 2014. a. pressiteade „FTC hoiatab lastele mõeldud rakenduste valmistajat BabyBus'i võimaliku COPPA rikkumise eest", https://www.ftc.gov/news-events/press-releases/2014/12/ftc-warns-childrens-app-maker-babybus-about-potential-coppa; Föderaalse kaubanduskomisjoni 7. mai 2013. a. pressiteade „FTC hoiatab andmevahendustööstust võimaliku eraelu puutumatuse rikkumise eest", https://www.ftc.gov/news-events/press-releases/2013/05/ftc-warns-data-broker-operations-possible-privacy-violations; Föderaalse kaubanduskomisjoni 3. aprilli 2013. a. pressiteade „FTC hoiatab andmevahendajaid, et üürnike üürimisega seotud ajaloo avalikustamine võib olla karistatav õiglase krediidiinfo seaduse (Fair Credit Reporting Act) alusel",https://www.ftc.gov/news-events/press-releases/2013/04/ftc-warns-data-brokers-provide-tenant-rental-histories-they-may.

Föderaalne kaubanduskomisjon on oma tugeva privaatsuspoliitika jõustamise ajaloo jooksul regulaarselt otsinud ka võimalikke programmiga Safe Harbour seotud rikkumisi. Alates programmi Safe Harbour vastuvõtmisest on föderaalne kaubanduskomisjon omal algatusel läbi viinud palju uurimisi programmi Safe Harbour täitmise kohta ning on esitanud 39 hagi USA äriühingute vastu programmiga Safe Harbour seotud rikkumiste pärast. Föderaalne kaubanduskomisjon jätkab kõnealust proaktiivset lähenemist, tehes uue raamistiku jõustamise prioriteediks.

II. TARBIJATE ERAELU PUUTUMATUSE KAITSE FÖDERAALSEL JA OSARIIKIDE TASANDIL

Ülevaates programmi Safe Harbor täitmise tagamisest, mis on ilmunud Euroopa Komisjoni programmi Safe Harbour piisavusotsuse lisana, tehakse kokkuvõte paljudest föderaalsel ja osariikide tasandil kehtinud seadustest ajal, mil programm Safe Harbour 2000. aastal vastu võeti ([1]). Sellel ajal reguleerisid paljud õigusaktid isikuandmete kogumist ja kasutamist ärilistel eesmärkidel kaugemaleulatuvalt kui föderaalse kaubanduskomisjoni seaduse (FTC Act) 5. paragrahv, sealhulgas: seadus kaabelsidepoliitika (Cable Communications Policy Act), sõidukijuhtide eraelu puutumatuse (Driver's Privacy Protection Act), elektroonilise side privaatsuse (Electronic Communications Privacy Act), elektrooniliste rahaülekannete (Electronic Funds Transfer Act), õiglase krediidiinfo (Fair Credit Reporting Act), finantspuutumatuse õiguse (Right to Financial Privacy Act), telefonimüügil tarbijate kaitsmise (Telephone Consumer Protection Act), ja eraelu puutumatuse kaitse kohta seoses videotega (Video Privacy Protection Act) kohta ning seadus Gramm-Leach-Bliley Act. Paljudel osariikidel oli samuti analoogseid seadusi kõnealustes valdkondades.

Alates 2000. aastast on nii föderaalsel kui ka osariikide tasandil toimunud palju arenguid, mis on täiendanud tarbijate eraelu puutumatuse kaitset ([2]). Näiteks föderaalsel tasandil muutis föderaalne kaubanduskomisjon 2013. aastal internetis laste eraelu puutumatuse kaitse seadust (COPPA) rakendavat eeskirja, et täiendavalt kaitsta laste isikuandmeid. Samuti andis föderaalne kaubanduskomisjon välja kaks eeskirja, millega rakendatakse seadust Gramm- Leach-Bliley Act – eraelu puutumatuse eeskirja ja kaitsemeetmete eeskirja – mis nõuavad, et finantsinstitutsioonid ([3]) avalikustaksid oma teabe jagamise tavad ja rakendaksid laiaulatusliku infoturbe programmi tarbijate andmete kaitsmiseks ([4]). Samamoodi täiendab 2003. aastal jõustunud õiglaste ja täpsete krediiditehingute seadus (Fair and Accurate Credit Transactions Act – FACTA) pikka aega kehtinud USA krediidi kohta käivaid seadusi, kehtestades nõuded teatavate tundlike finantsandmete maskeerimiseks, jagamiseks ja kõrvaldamiseks. Õiglaste ja täpsete krediiditehingute seaduse (Fair and Accurate Credit Transactions Act) alusel andis föderaalne kaubanduskomisjon välja rea eeskirju, sealhulgas tarbijate õiguse kohta saada kord aastas tasuta krediidiaruanne; tarbijaaruannetes sisalduvate andmete turvalise kõrvaldamise nõuete kohta; tarbijate õiguse kohta loobuda teatavate krediidi- ja kindlustuspakkumiste saamisest; tarbijate õiguse kohta loobuda sidusettevõtjalt tema toodangu ja teenuste turustamiseks saadetud teabe kasutamisest ning nõuded finantsinstitutsioonidele ja kreeditoridele identiteedivarguste avastamise ja ärahoidmise programmide rakendamiseks ([5]). Lisaks uuendati 2013. aastal ravikindlustuse teisaldatavuse seaduse (Health Insurance Portability) ja vastutuse seaduse (Accountability Act) alusel välja antud eeskirju, lisades täiendavaid meetmeid eraelu puutumatuse ja isikute tervisealase teabe kaitseks ([6]). Samuti on jõustunud eeskirjad soovimatute telefonimüügi-kõnede, robotkõnede ja spämmi kohta. Samuti on kongress kehtestanud seadusi, milles nõutakse, et teatavad äriühingud, kes koguvad tervisealast teavet, peavad tarbijaid rikkumistest teavitama ([7]).

Samuti on osariigid olnud väga aktiivsed eraelu puutumatuse ja turvalisuse kohta käivate seaduste vastuvõtmisel. Alates 2000. aastast on 47 osariiki, Columbia ringkond, Guam, Puerto Rico ja Ühendriikide Neitsisaared vastu võtnud

([1]) Vt USA kaubandusministeeriumi „Ülevaade programmi Safe Harbor jõustamisest", https://build.export.gov/main/safeharbor/eu/eg_main_018481.
([2]) Põhjalikuma kokkuvõtte saamiseks USA õiguskaitse kohta vt Daniel J. Solove & Paul Schwartz, *Information Privacy Law* (5. kd. 2015).
([3]) Finantsinstitutsioonid on seaduse Gramm-Leach-Bliley Act alusel väga laialt määratletud ning hõlmavaid ettevõtjaid, kes „tegelevad olulisel määral" finantstoodete või -teenuste pakkumisega. Sinna hulka kuuluvad näiteks tšekkide sularahaks vahetajad; lühiajaliste väikeste laenude (nn palgapäevalaenud) andjad; hüpoteegimaaklerid; laenuandjad, kes ei ole pangad; isikliku vara või kinnisvara hindajad ja professionaalsed maksudeklaratsioonide koostajad.
([4]) 2010. aasta tarbijate finantsvaldkonnas kaitsmise seaduse (Consumer Financial Protection Act – CFPA) peatüki X alusel (Pub. L. 111–203, 124 Stat. 1955)(21. juuli 2010) (mis on tuntud ka kui Dodd-Frank'i Wall Street'i reform ja tarbijakaitse seadus („Dodd-Frank Wall Street Reform and Consumer Protection Act"), anti suurem osa föderaalse kaubanduskomisjoni seaduse Gramm-Leach-Bliley Act alusel eeskirjade koostamise pädevusest üle tarbijatele finantsvaldkonnas kaitset osutavale büroole (Financial Protection Bureau – CFPB). Föderaalsele kaubanduskomisjonile jääb jõustamispädevus seaduse Gramm-Leach- Bliley Act alusel ning pädevus kaitsemeetmete eeskirja (Safeguards Rule) reeglite koostamiseks ja väljaandmiseks ning piiratud pädevus puutumatuse eeskirja (Privacy Rule) reeglite koostamiseks ja väljaandmiseks automüüjaid puudutavas osas.
([5]) Tarbijate finantsvaldkonnas kaitsmise seaduse (CFPA) alusel jagab komisjon oma rolli õiglase krediidiinfo seaduse (FCRA) jõustamisel CFPBga, ent reeglite koostamise pädevus on suures osas CFPB-le üle antud (välja arvatud punaste lippude ja kõrvaldamise reeglid).
([6]) Vt 45 C.F.R. pts. 160, 162, 164.
([7]) Vt nt American Recovery & Reinvestment Act of 2009, Pub. L. No. 111–5, 123 Stat. 115 (2009) ja asjakohased määrused 45 C.F.R. §§ 164.404–164.414; 16 C.F.R. pt. 318.

seadused, milles nõutakse, et ettevõtjad peavad teavitama üksikisikuid isikuandmete turvalisuse rikkumistest ([1]). Vähemalt 32 osariigil ja Puerto Ricol on olemas seadused andmete kõrvaldamise kohta, milles kehtestatakse nõuded isikuandmete kõrvaldamise või hävitamise kohta ([2]). Mitmed osariigid on jõustanud üldised andmete turvalisust puudutavad seadused. Lisaks on California jõustanud mitmed eraelu puutumatuse seadused, sealhulgas seaduse, milles sätestatakse, et äriühingud peavad omama puutumatusnorme ja avalikustama oma mittejälgimise tavad, ([3]) seaduse, milles nõutakse enama valguse heitmist („Shine the Light" law) andmevahendajate tegevuse läbipaistvusele ([4]) ja seaduse, milles tehakse kohustuslikuks „kustutamisnupp", mis võimaldaks alaealistel nõuda teatava info kustutamist sotsiaalmeediast ([5]). Kasutades kõnealuseid seadusi ja teisi asutusi on föderaalvalitsus ja osariikide valitsused määranud märkimisväärseid trahve äriühingutele, kes ei ole kaitsnud tarbijate isikuandmete puutumatust ja turvalisust ([6]).

Eraldi kohtuasjad on samuti viinud edukate otsuste ja lahendusteni, mis pakuvad täiendavat kaitset tarbijate eraelu puutumatusele ja andmete turvalisusele. Näiteks 2015. aastal oli Target nõus maksma 10 miljonit USA dollarit osana kokkuleppest klientidega, kes väitsid, et nende isiklikud finantsandmed seati ohtu ulatusliku rikkumise tõttu andmete käitlemises. 2013. aastal oli AOL nõus maksma 5 miljonit USA dollarit, et jõuda kokkuleppele kollektiivse hagi lahendamises, mis seisnes väidetavalt mittepiisavas identifitseeritavuse kõrvaldamises, mis puudutas sadade tuhandete AOLi liikmete kohta otsingu teel tehtud päringute väljastamist. Lisaks kinnitas üks föderaalkohus 9 miljoni USA dollari suuruse summa, mis tuleb maksta Netflixil väidetavalt laenutuste ajaloo kohta andmete säilitamise eest, millega rikuti 1988. aasta seadust eraelu puutumatuse kaitse kohta seoses videotega (Video Privacy Protection Act). California föderaalkohtud kinnitasid kaks eraldi poolte kokkulepet Facebook'iga, üks 20 miljoni USA dollari ja teine 9,5 miljoni USA dollari suuruse summa eest, mis olid seotud sellega, et äriühing kogus, kasutas ja jagas oma kasutajate isikuandmeid. Samuti kiitis 2008. aastal üks California osariigi kohus heaks 20 miljoni USA dollari suuruse summa eest poolte kokkuleppe LensCrafters'iga tarbijate meditsiiniinfo seadusevastase avalikustamise eest.

Kokkuvõttes, nagu see kokkuvõte illustreerib, tagavad Ameerika Ühendriigid olulisel määral tarbijate eraelu puutumatuse ja turvalisuse õiguskaitse. Uus andmekaitseraamistik Privacy Shield, millega tagatakse arusaadavad kaitsemeetmed ELi üksikisikutele, hakkab toimima kõnealusel suuremal foonil, kus tarbijate eraelu puutumatuse ja turvalisuse kaitse on jätkuvalt oluline prioriteet.

---

([1]) Vt nt National Conference of State Legislatures („NCSL"), *State Security Breach Notification Laws* (4 jaanuar 2016), kättesaadav aadressil http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

([2]) NCSL, *Data Disposal Laws* (12 jaanuar 2016), kättesaadav aadressil http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

([3]) Cal. Bus. & Professional Code §§ 22575-22579.

([4]) Cal. Civ. Code §§ 1798.80-1798.84.

([5]) Cal. Bus. & Professional Code § 22580-22582.

([6]) Vt Jay Cline, *U.S. Takes the Gold in Doling Out Privacy Fines*, Computerworld (17 veebruar 2014), kättesaadav aadressil http://www.computerworld.com/s/article/9246393/Jay-Cline-U.S.-takes-the-gold-in-doling-out-privacy-fines?taxonomyId=17&pageNumber=1.

*V LISA*

**USA transpordiministri Anthony Foxxi kiri**

19. veebruar 2016

Volinik Vera Jourová
European Commission
Rue de la Loi/Wetstraat 200
1049 l049 Brussels
Belgium

Vastus: ELi–USA andmekaitseraamistik Privacy Shield

Lugupeetud volinik Jourová

Ameerika Ühendriikide transpordiministeerium („transpordiministeerium" või „DOT") hindab võimalust kirjeldada oma rolli ELi–USA andmekaitseraamistiku Privacy Shield täitmise tagamisel. Käesolev raamistik mängib olulist rolli nende isikuandmete kaitsmisel, mis esitatakse kaubanduslike tehingute käigus maailmas, kus kõik on omavahel üha enam seotud. See võimaldab äriühingutel teha maailmamajanduses olulisi toimingud, tagades samal ajal, et ELi tarbijatele jääksid alles olulised privaatsuse kaitsemeetmed.

Transpordiministeerium väljendas oma jõustamiskohustust seoses raamistikuga Safe Harbor Euroopa Komisjonile saadetud kirjas üle 15 aasta tagasi. Transpordiministeerium lubas selles kirjas otsusekindlalt jõustada raamistiku Safe Harbor eraelu puutumatuse kaitse põhimõtteid. Transpordiministeerium jätkab selle kohustuse täitmist ning käesolev kiri tuletab seda kohustust meelde.

Eelkõige uuendab transpordiministeerium oma kohustust järgmistes põhivaldkondades: 1) andmekaitseraamistiku Privacy Shield väidetavate rikkumiste uurimiste prioriseerimine; 2) asjaomane täitemeetmete võtmine üksuste vastu, mis esitavad andmekaitseraamistiku Privacy Shield sertifitseerimisega seotud valesid või pettusel põhinevaid andmeid; ning 3) andmekaitseraamistiku Privacy Shield rikkumistega seotud avalike täitekorralduste järelevalve ja teostamine. Anname teavet nende kõikide kohustuste kohta ning vajalikus kontekstis asjakohase tausta kohta seoses transpordiministeeriumi rolliga kaitsta tarbijate eraelu puutumatust ja jõustada andmekaitseraamistik Privacy Shield.

I. TAUSTTEAVE

A. **Transpordiministeeriumi eraelu puutumatuse amet**

Transpordiministeerium võtab kindlalt oma kohustuseks tagada tarbijate poolt lennuettevõtjatele ja piletimüügiagentidele esitatud teabe puutumatus. Transpordiministeeriumi volitused võtta selles valdkonnas meetmeid on kehtestatud õigusaktis 49 U.S.C. 41712, millega keelatakse vedajal või piletimüügiagendil rakendada ebaõiglaseid või pettusel põhinevaid tavasid või ebaõiglast konkurentsimeetodit lennutranspordi müügis, mille tulemusena on tõenäoline, et tarbijaid kahjustatakse. Paragrahv 41712 on üles ehitatud föderaalse kaubanduskomisjoni seadust (Federal Trade Commission Act) järgides (15 U.S.C. 45). Meie tõlgendusel keelab meie ebaõiglast või pettusel põhinevat tava käsitlev õigusakt lennuettevõtjal või piletimüügiagendil: 1) selle puutumatusnormide rikkumise; või 2) eraviisiliste andmete kogumise või avalikustamise viisil, millega rikutakse avalikku poliitikat, on moraalivaba või põhjustab tarbijatele olulist kahju, mida ei ole võimalik korvata tasakaalustava hüvitisega. Samuti tõlgendame paragrahvi 41712 viisil, mis keelab vedajatel ja piletimüügiagentidel teha järgmist: 1) selliste ministeeriumi väljastatud eeskirjade rikkumine, mille kohaselt peetakse konkreetseid eraelu puutumatusega seotud tavasid ebaõiglaseks või pettusel põhinevaks; või 2) internetis laste eraelu puutumatuse kaitse seaduse (Children's Online Privacy Protection Act – COPPA) või internetis laste eraelu puutumatuse kaitse seadust (COPPA) rakendavad föderaalse kaubanduskomisjoni (FTC) eeskirjad. Föderaalõiguse kohaselt on transpordiministeeriumil ainuõigus reguleerida lennuettevõtjate eraelu puutumatuse tavasid, samuti jagab transpordiministeerium pädevust föderaalse kaubanduskomisjoniga seoses piletimüügiagentide eraelu puutumatuse tavadega lennutranspordi müügis.

Seega juhul kui lennutranspordi vedaja või müüja kohustub avalikult täitma andmekaitseraamistiku Privacy Shield eraelu puutumatusega seotud põhimõtteid, on ministeeriumil võime kasutada paragrahvis 41712 kehtestatud seadusest tulenevad volitusi, et tagada vastavus nendele põhimõtetele. Seetõttu kui reisija annab andmeid vedajale või piletimüügiagendile, kes on kohustatud järgima andmekaitseraamistiku Privacy Shield eraelu puutumatusega seotud põhimõtteid, põhjustab vedaja või piletimüügiagendi poolne mittejärgimine tõenäoliselt kahju tarbijale ning kujutab endast paragrahvi 41712 kohast rikkumist.

B. **Täitmise tagamise tavad**

Ministeeriumi lennundusjõustamise ja menetluste amet (Office of Aviation Enforcement and Proceedings) uurib juhtumeid ja määrab karistusi 49 U.S.C. 4171 2.U.S.C. alusel. Sellega jõustatakse paragrahvi 41712 kohane seadusest tulenev keeld ebaõiglaste ja pettusel põhinevate tavade vastu peamiselt läbirääkimiste, keelustamiskorralduste ettevalmistamise ning tsiviiltrahvide hindamise korralduste eelnõude kaudu. Amet saab suures osas teavet võimalike rikkumiste kohta kaebuste kaudu, mis laekuvad üksikisikutelt, reisibüroodelt, lennuettevõtjatelt ning USA ja välisriikide valitusasutustelt. Tarbijad võivad kasutada transpordiministeeriumi veebisaiti lennuettevõtjate ja piletimüügiagentide vastu suunatud eraelu puutumatusega seotud kaebuste esitamiseks ([1]).

Juhul kui juhtumi korral ei jõuta mõistliku ja asjaomase lahenduseni, on lennundusjõustamisametil (Aviation Enforcement Office) volitused algatada täitemenetlus, mis hõlmab tõenduslikku ärakuulamist transpordiministeeriumi halduskohtus. Halduskohtul on volitus väljastada keelustamiskorraldusi ja tsiviiltrahve. Paragrahvi 41712 kohaste rikkumiste tulemuseks võivad olla keelustamiskorraldused ja tsiviiltrahvide määramine summas kuni 27 500 USA dollarit paragrahvi 41712 iga korralduse rikkumise kohta.

Transpordiministeeriumil puudub volitused määrata kahjutasu või rahalist hüvitist üksikutele kaebuse esitajatele. Samas on transpordiministeeriumil volitused kiita heaks lennundusjõustamisameti (Aviation Enforcement Office) uurimiste tulemusel saadud lahendid, mis toob tarbijatele otsest kasu (nt raha, vautšerid), korvamaks rahalisi trahve, mida muidu tuleks maksta USA valitsusele. See on juhtunud varem ning võib juhtuda ka andmekaitseraamistiku Privacy Shield põhimõtete kontekstis, kui olukord seda nõuab. Paragrahvi 41712 korduv rikkumine lennuettevõtja poolt tõstataks ka küsimuse lennufirma suhtumisest vastavusse, mis äärmisel juhul võib lõppeda sellega, et lennufirmat ei peeta tegutsemiseks sobivaks ja ta kaotab seetõttu loa majandustegevuseks.

Praeguseks on transpordiministeeriumile laekunud suhteliselt vähe kaebusi, mis on seotud väidetava eraelu puutumatuse rikkumisega piletimüügiagentide või lennuettevõtjate poolt. Kui need tekivad, uuritakse neid vastavalt eespool kehtestatud põhimõtetele.

C. **Transpordiministeeriumi õiguskaitse, millest saavad kasu ELi tarbijad**

Paragrahvis 41712 kehtestatakse, et ebaõiglaste või pettusel põhinevate tavade keelustamist seoses lennutranspordi või lennutranspordi müügiga kohaldatakse nii USA kui ka välisriikide lennuettevõtjate ja piletimüügiagentide suhtes. Transpordiministeerium võtab sageli meetmeid USA ja välisriikide lennuettevõtjate vastu tavade tõttu, mis kahjustavad nii välismaa kui ka USA tarbijaid vastavalt sellele, et lennuettevõtjate tegevus toimus lennutranspordi teostamise käigus Ameerika Ühendriikidesse saabuvatel või sealt väljuvatel lendudel. Transpordiministeerium kasutab kõiki õiguskaitsevahendeid ja jätkab nende kasutamist, mis on saadaval, et kaitsta nii välismaa kui ka USA tarbijaid reguleeritud üksuste ebaõiglaste või pettusel põhineva tegevuse eest lennutranspordis.

Samuti tagab transpordiministeerium seoses lennuettevõtjatega mude suunatud õigusnormide täitmisr, mille kaitse laieneb mitte-ameeriklastest tarbijatele, näiteks internetis laste eraelu puutumatuse kaitse seadus (COPPA). Muu hulgas nõutakse internetis laste eraelu puutumatuse kaitse seaduse alusel, et lastele suunatud veebisaitide ja internetipõhiste teenuste või teadlikult alla 13-aastastelt lastelt isikuandmeid koguvad üldkasutatavate kommertsveebisaitide haldajad teatavad sellest vanematele ning saavad tõestatava vanemate nõusoleku. Internetis laste eraelu puutumatuse kaitse seaduse kohaldamisalasse kuuluvad ja välisriikides elavate laste isikuandmeid koguvad USA veebisaidid ja teenused peavad olema kooskõlas internetis laste eraelu puutumatuse kaitse seadusega. Välisriikide veebisaidid ja internetipõhised teenused peavad olema samuti kooskõlas internetis laste eraelu puutumatuse kaitse seadusega, kui need on suunatud Ameerika Ühendriikides elavatele lastele või kui need koguvad teadlikult Ameerika Ühendriikides elavate laste isikuandmeid. Sel määral, mil USA või välismaiste lennuettevõtjate äritegevus Ameerika Ühendriikides läheb vastuollu internetis laste eraelu puutumatuse kaitse seadusega (COPPA), on transpordiministeeriumil pädevus võtta täitemeetmed.

II. ANDMEKAITSERAAMISTIKU PRIVACY SHIELD TÄITMISE TAGAMISE

Juhul kui lennuettevõtja või piletimüügiagent otsustab osaleda andmekaitseraamistikus Privacy Shield ja transpordiministeeriumile laekub kaebus, et see lennuettevõtja või piletimüügiagent on väidetavalt raamistikku rikkunud, võtab transpordiministeerium järgmised sammud, et raamistiku täitmist tõhusalt tagada.

([1]) http://www.transportation.gov/airconsumer/privacy-complaints

A. **Väidetavate rikkumiste uurimise prioriseerimine**

Transpordiameti lennundusamet (Aviation Enforcement Office) uurib kõiki kaebusi, milles väidetakse, et andmekaitseraamistikku Privacy Shield on rikutud (sealhulgas ELi andmekaitseasutustelt laekunud kaebused), ning võtab täitemeetmed juhul, kui rikkumine on tõendatud. Lisaks sellele teeb lennundusamet (Aviation Enforcement Office) koostööd föderaalse kaubanduskomisjoni (FTC) ja kaubandusministeeriumiga ning seab esikohale nende väidete uurimise, mille kohaselt ei täida reguleerivad üksused andmekaitseraamistiku Privacy Shield osana eraelu puutumatusega seotud kohustusi.

Andmekaitseraamistiku Privacy Shield rikkumisega seotud väite laekumisel võib transpordiministeeriumi lennundusamet lennundusamet (Aviation Enforcement Office) võtta uurimise käigus erinevaid meetmeid. Näiteks võib ta läbi vaadata piletimüügiagendi või lennuettevõtja privaatsuspoliitika, saada täiendavat teavet otse piletimüügiagendilt või lennuettevõtjalt või kolmandatelt isikutelt, teha koostööd taotleva üksusega ning hinnata, kas esineb rikkumisi või on mõjutatud märkimisväärne hulk tarbijaid. Lisaks määrab ta, kas väljastamine hõlmab kaubandusministeeriumi või föderaalse kaubanduskomisjoni haldusalasse jäävaid küsimusi, hindab, kas tarbijate ja ettevõtjate koolitamine oleks kasulik ning vajaduse korrall algatab täitemenetluse.

Juhul kui transpordiministeerium saab teada andmekaitseraamistiku Privacy Shield võimalikust rikkumisest piletimüügiagentide poolt, kooskõlastab see juhtumi föderaalse kaubanduskomisjoniga. Samuti nõustame föderaalset kaubanduskomisjoni ja kaubandusministeeriumi seoses kõikide andmekaitseraamistiku Privacy Shield täitemeetmete tulemustega.

B. **Liikmelisusega seotud valede või pettusel põhinevate andmetega tegelemine**

Transpordiministeerium kohustub jätkuvalt uurima andmekaitseraamistiku Privacy Shield rikkumisi, sealhulgas programmi Privacy Shield liikmelisusega seotud valed või pettusel põhinevad andmed. Esmajärjekorras võtame arvesse kaubandusministeeriumilt laekunud taotlusi, mis on seotud organisatsioonidega, mille puhul on ministeerium avastanud, et need väidavad end ebaseaduslikult olevat andmekaitseraamistiku Privacy Shield praegused liikmed või kasutavad andmekaitseraamistiku Privacy Shield sertifitseerimistähist ilma loata.

Lisaks sellele märgime, et juhul kui organisatsiooni privaatsuspoliitikaga lubatakse, et see on kooskõlas andmekaitseraamistiku Privacy Shield oluliste põhimõtetega, siis selle suutmatus registreeruda või seda säilitada kaubandusministeeriumis tõenäoliselt iseenesest ei vabasta organisatsiooni nende raamistikuga seotud kohustuste jõustamisest transpordiministeeriumi poolt.

C. **Andmekaitseraamistikuga Privacy Shield rikkumistega seotud avalike täitekorralduste järelevalve ja teostamine**

Samuti kinnitab transpordiministeeriumi lennundusamet (Aviation Enforcement Office) oma kohustust jälgida täitekorraldusi vastavalt vajadusele, et tagada vastavus andmekaitseraamistikule Privacy Shield. Täpsemalt, kui amet väljastab korralduse, mille kohaselt tuleb lennuettevõtjal või piletimüügiagendil lõpetada andmekaitseraamistiku Privacy Shield ja paragrahvi 41712 kohased rikkumised ning hoiduda nendest tulevikus, jälgib amet üksuse vastavust korralduses esitatud keelustamissättele. Lisaks tagab amet, et andmekaitseraamistikuga Privacy Shield seotud juhtumitest tulenevad korraldused on kättesaadavad ameti veebisaidilt.

Loodame, et jätkame andmekaitseraamistikuga Privacy Shield seotud koostööd oma föderaalsete partnerite ja ELi sidusrühmadega.

Loodan, et sellest informatsioonist on abi. Kui Teil on küsimusi või vajate lisainfot, võtke julgesti minuga ühendust.

Lugupidamisega

Anthony R. Foxx

Transpordiminister

*VI LISA*

**Õigusnõuniku Robert Litti kiri**
**Riiklik luurejuhi amet (Office of the Director of National Intelligence)**

22. veebruar 2016

Justin S. Antonipillai
Nõunik
USA kaubandusministeerium
1401 Constitution Ave., NW
Washington, DC 20230

Ted Dean
Aseministri asetäitja (Deputy Assistant Secretary)
Väliskaubandusamet
1401 Constitution Ave., NW
Washington, DC 20230

Lugupeetud hr Antonipillai ja hr Dean:

ELi–USA andmekaitseraamistiku Privacy Shield läbirääkimiste kontekstis viimase kahe ja poole aasta jooksul on Ameerika Ühendriigid andnud olulist teavet USA luureühenduse signaaliluure andmete kogumise toimimise kohta. See on hõlmanud teavet reguleeriva õigusraamistiku, nende tegevuste mitmetasandilise järelevalve, nende tegevuste ulatusliku läbipaistvuse ning eraelu puutumatuse ja kodanikuvabaduste üleüldise kaitse kohta, eesmärgiga aidata Euroopa Komisjonil määratleda sellise kaitse adekvaatsus, kuna see on seotud riikliku julgeoleku erandi tegemisega andmekaitseraamistiku Privacy Shield põhimõtete raames. Käesolevas dokumendis on esitatud teave põhjal tehtud kokkuvõte.

I. PRESIDENDI POLIITIKASUUNIS NR 28 (PPD-28) JA USA SIGNAALILUURE TEGEVUSE TEOSTAMINE

USA luurerühendus kogub välisluure andmeid hoolikalt kontrollitud viisil, mis on ranges vastavuses USA seadustega ning mille suhtes rakendatakse mitmetasandilist järelevalvet, pöörates enim tähelepanu olulistele välisluure ja riikliku julgeoleku prioriteetidele. USA signaaliluure andmete kogumist reguleerib seaduste ja põhimõtete mosaiik, sealhulgas USA põhiseadus, välisluure ja jälitustegevuse seadus (Foreign Intelligence Surveillance Act – FISA) (50 U.S.C. § 1801 *et seq.*), korraldus 12333 ja selle rakendusmenetlused, presidendi juhised ning arvukalt menetlusi ja suuniseid, mille on heaks kiitnud välisluure ja jälitustegevuse seaduse (FISA) kohus ja justiitsminister (Attorney General), millega kehtestatakse täiendavad eeskirjad, piiramaks välisluure andmete kogumist, säilitamist, kasutamist ja levitamist ([1]).

a. **PPD 28 Ülevaade**

2014. aasta jaanuaris pidas president Obama kõne, milles kirjeldatakse USA signaaliluure tegevusega seotud erinevaid reforme, ning väljastas asjaomase tegevusega seotud presidendi poliitikasuunise nr 28 (PPD-28) ([2]). President rõhutas, et USA signaaliluure tegevus aitab kaitsta mitte üksnes meie riiki ja meie vabadusi, vaid ka nende muude riikide, sealhulgas ELi liikmesriigid, turvalisust ja vabadusi, mis tuginevad sellele teabele, mida USA luureagentuurid koguvad selleks, et kaitsta oma kodanikke.

Presidendi poliitikasuunises nr 28 (PPD-28) kehtestatakse rida põhimõtteid ja nõudeid, mida kohaldatakse kogu USA signaaliluure tegevuse ja kõikide inimeste suhtes, sõltumata nende rahvusest või asukohast. Eelkõige kehtestatakse sellega teatavad menetlusnõuded, et käsitleda USA signaaliluure abil saadud mitte-ameeriklastest inimeste isikuandmete kogumist, säilitamist ja levitamist. Need nõuded on üksikasjalikumalt kehtestatud allpool, aga kokkuvõttes.

— Presidendi poliitikasuunises (PPD) korratakse, et Ameerika Ühendriigid koguvad signaaliluure andmeid üksnes siis, kui see on lubatud statuudi, korralduse või presidendi muu direktiivi alusel.

([1]) Täiendav teave USA välisluure tegevuse kohta on avaldatud veebis ning see on avalikult kättesaadav veebisaidi IC on the Record (www.icontherecord.tumblr.com) kaudu, mis kujutab endast riikliku luurejuhi amet (ODNI) avalikku veebisaiti, mis on suunatud valitsuse luuretegevuse suurema avaliku nähtavuse edendamiseks.
([2]) https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

— Presidendi poliitikasuunises on kehtestatud menetlused selle tagamiseks, et signaaliluure tegevust teostataks üksnes õiguspäraste ja volitatud riiklike julgeoleku eesmärkide edendamiseks.

— Samuti kehtestatakse presidendi poliitikasuunises, et eraelu puutumatus ja kodanikuvabadused peavad olema signaaliluure andmete kogumisega seotud tegevuse planeerimises selle lahutamatud teemad. Eelkõige ei kogu Ameerika Ühendriigid luureandmeid selleks, et alla suruda või kahjustada kriitikat või teisitimõtlemist; selleks, et kahjustada inimesi vastavalt nende rahvusele, rassile, soole, seksuaalsele sättumusele või religioonile; või et saada USA ettevõtete ja ärivaldkondade huvides konkurentsivõimeline kaubanduslik eelis.

— Presidendi poliitikasuunises nähakse ette, et signaaliluure andmete kogumine peab olema teostatud nii kohandataval kujul kui võimalik ning et laiaulatuslikult kogutud signaaliluure andmeid saab kasutada üksnes loetletud erieesmärkidel.

— Presidendi poliitikasuunises (PPD) reguleeritakse, et luureühendus võtab vastu menetlused, mis on mõistlikult ette nähtud signaaliluure tegevuse käigus kogutud isikuandmete levitamise ja säilitamise vähendamiseks ning eelkõige laiendades USA kodanike isikuandmetele suunatud kaitset ka mitte-ameeriklastest inimeste isikuandmete kaitsele.

— Presidendi poliitikasuunist nr 28 (PPD-28) rakendavad asutused menetlused on vastu võetud ja avalikustatud.

Siinkohal kehtestatud menetluste ja kaitse kohaldatavus andmekaitseraamistiku Privacy Shield suhtes on selge. Kui andmed on üle kantud Ameerika Ühendriikide korporatsioonidele vastavalt andmekaitseraamistikule Privacy Shield või tõepoolest mis tahes viisil, saavad USA luureagentuurid otsida neid andmeid asjaomastest korporatsioonidest üksnes siis, kui taotlus on kooskõlas välisluure ja jälitustegevuse seadusega (FISA) või see esitatakse vastavalt ühele riikliku julgeoleku teabenõude (National Security Letter) seadusest tulenevale sättele, mida on käsitletud allpool ([1]). Lisaks sellele, ilma et kinnitatakse või lükatakse ümber meediakajastusi, mille kohaselt kogub USA luureühendus andmeid Atlandi-üleste kaablite kaudu samal ajal kui neid kantakse üle Ameerika Ühendriikidesse; juhul kui USA luureühendus kogub andmeid Atlandi-üleste kaablite kaudu, tuleb seda teha siinkohal kehtestatud piirangute ja kaitsemeetmete raames, sealhulgas presidendi poliitikasuunise nr 28 (PPD-28) nõuded.

b. **Andmete kogumise piirangud**

Presidendi poliitikasuunises nr 28 (PPD-28) kehtestatakse mitmed olulised üldpõhimõtted, mis reguleerivad signaaliluure andmete kogumist:

— Signaaliluure andmete kogumine peab olema lubatud statuudi või presidendi volituse alusel ning seda tuleb teostada vastavalt põhiseadusele ja seadusandlusele.

— Eraelu puutumatus ja kodanikuvabadused peavad olema signaaliluure tegevuse planeerimise lahutamatud kaalutlused.

— Signaaliluure andmeid kogutakse üksnes siis, kui on olemas kehtiv välisluure või vastuluurega seotud eesmärk.

— Ameerika Ühendriigid ei kogu signaaliluure andmeid selleks, et alla suruda või kahjustada kriitikat või teisitimõtlemist.

— Ameerika Ühendriigid ei kogu signaaliluure andmeid selleks, et kahjustada inimesi vastavalt nende rahvusele, rassile, soole, seksuaalsele sättumusele või religioonile.

— Ameerika Ühendriigid ei kogu signaaliluure andmeid selleks, et saada USA ettevõtete ja ärivaldkondade huvides konkurentsivõimeline kaubanduslik eelis.

— USA signaaliluuret tuleb alati teostada nii kohandatud kujul kui võimalik, võttes arvesse muude teabeallikate kättesaadavust. See tähendab muu hulgas seda, et võimaluse korral teostatakse signaaliluure andmete kogumist pigem suunatud viisil, mitte laiaulatuslikult.

Nõuet, mille järgi tuleb signaaliluuret teostada nii kohandatud kujul kui võimalik, kohaldatakse nii signaaliluure andmete kogumisviisi kui ka selle suhtes, mida tegelikkuses kogutakse. Näiteks signaaliluure andmete kogumise üle otsustamisel

([1]) Õiguskaitseasutused või reguleerivad asutused võivad Ameerika Ühendriikides küsida korporatsioonidelt neid andmeid uurimiseks vastavalt käesoleva dokumendi reguleerimisalast väljaspoole jäävatele muudele kriminaal-, tsiviil- ja reguleerivatele asutustele, mis on piiratud riiklike julgeolekuasutustega.

peab luureühendus kaaluma muu teabe kättesaadavust, sealhulgas diplomaatilised või avalikud allikad, ning seadma esikohale andmete kogumise nende vahendite kaudu, kui see on asjakohane ja kohandatav. Lisaks sellele tuleb luureühenduse üksuste eeskirjadega kehtestada, et kui võimalik, siis peab kogumine olema suunatud konkreetsetele välisluure eesmärkidele või teemadele kategooriate kasutamise teel (nt erivahendite, valiku ja tunnuste alusel).

Oluline on vaadata komisjoni esitatud teavet tervikuna. Otsuseid selle kohta, mis on kohandatav või rakendatav, ei jäeta üksikisikute hoolde, vaid nende suhtes kohaldatakse eeskirju, mille asutused on väljastanud presidendi poliitikasuunise nr 28 (PPD-28) alusel ja mis on tehtud avalikkusele kättesaadavaks, ning selles kirjeldatud muid protsesse ([1]). Presidendi poliitikasuunises nr 28 (PPD-28) öeldakse, et signaaliluure andmete laiaulatuslik kogumine viitab sellisele andmete kogumisele, mis tehnilistel või operatiivsetel kaalutlustel toimub ilma kategooriate kasutamiseta (nt eritunnuste, valiku jms alusel). Sellega seoses tunnistatakse presidendi poliitikasuunises nr 28 (PPD-28), et luureühenduse üksused peavad signaaliluure andmeid teatavates oludes koguma laiaulatuslikult, avastamaks uusi või tekkivaid ohte ja muid olulisi riiklikku julgeoleku andmeid, mis on sageli peidetud kaasaegse ülemaailmse side suurde ja keerulisse süsteemi. Samuti tunnistatakse sellega eraelu puutumatuse ja kodanikuvabadustega seotud tekkivaid probleeme, kui signaaliluure andmeid kogutakse laiaulatuslikult. Seega suunatakse luureühendust presidendi poliitikasuunisega nr 28 (PPD-28) seadma esikohale alternatiive, mis võimaldaksid teostada suunatud signaaliluure andmete kogumist, mitte laiaulatuslikku signaaliluure andmete kogumist. Järelikult tuleb luureühenduse üksustel teostada signaaliluure suunatud andmete kogumist, mitte signaaliluure laiaulatuslikku kogumist, kui vähegi võimalik ([2]). Nende põhimõtetega tagatakse, et laiaulatusliku andmete kogumise erandiga ei kaotata üldreeglit.

Mis puutub mõistlikkuse kontseptsiooni, siis moodustab see USA õiguse aluspõhimõtte. See tähendab seda, et luurerühenduse üksused ei ole kohustatud vastu võtma ühtegi teoreetiliselt võimalikku meedet, vaid pigem tuleb neil oma jõupingutusi tasakaalustada, et kaitsta eraelu puutumatuse ja kodanikuvabaduste õigustatud huve koos signaaliluure tegevuse praktiliste vajadustega. Siinkohal on taaskord tehtud kättesaadavaks asutuste poliitika ning saab kinnitada, et tingimus „mõistlikult kavandatud, et vähendada isikuandmete levitamist ja säilitamist“ ei õõnesta üldist eeskirja.

Samuti kehtestatakse presidendi poliitikasuunises nr 28 (PPD-28), et laiaulatuslikult kogutud signaaliluure andmeid saab kasutada üksnes kuuel erieesmärgil: välisriikide teatava tegevuse avastamine ja sellega võitlemine; terrorismivastane võitlus; leviku tõkestamine; küberturvalisus; USA-le või liitlasvägedele suunatud ohtude avastamine ja nendega võitlemine; ning võitlemine rahvusvahelise ohustava kuritegevusega, sealhulgas sanktsioonidest kõrvalehoidmine. Presidendi riikliku julgeoleku nõunik, konsulteerides riikliku luuredirektoriga (Director for National Intelligence – DNI), vaatab igal aastal läbi need laiaulatuslikult kogutud signaaliluure andmete lubatud kasutusviisid, et näha, kas neid tuleb muuta. Riigi luuredirektor (DNI) teeb selle loetelu avalikkusele võimalikult kättesaadavaks, mis on kooskõlas riigi julgeolekuga. Sellega tagatakse oluline ja läbipaistev piirang laiaulatuslikult kogutud signaaliluure andmete kasutamise kohta.

Lisaks on presidendi poliitikasuunist nr 28 (PPD-28) rakendavad luureühenduse üksused tõhustanud olemasolevaid analüütilisi tavasid ja standardeid, et taotleda hindamata signaaliluure andmeid ([3]). Analüütikud peavad struktureerima oma päringud või muud otsingusõnad ja -meetmed, tagamaks, et need sobivad luureandmete tuvastamiseks, mida on vaja kehtiva välisluure või õiguskaitsega seotud ülesande täitmiseks. Selleks peavad luurerühenduse liikmed suunama tähelepanu päringutele isikute kohta seoses signaaliluure andmete kategooriatega, mis vastavad välisluure või õiguskaitsealasele nõudele, eesmärgiga ennetada nende isikuandmete kasutamist, mis ei ole asjaomased välisluure või õiguskaitsealaste nõuete suhtes.

Oluline on rõhutada, et kõik laiaulatusliku kogumisega seotud tegevused seoses internetisidega, mida USA luureühendus teostab signaaliluure kaudu, hõlmavad väikest osa internetist. Lisaks sellele tagab suunatud päringute kasutamine, nagu on eespool kirjeldatud, et analüütikutele antakse uurida üksnes selliseid andmeid, millel eeldatakse olevat potentsiaalne luurealane väärtus. Need piirangud on ette nähtud kaitsma kõikide isikute eraelu puutumatust ja kodanikuvabadusi, sõltumata nende rahvusest ja elukohast.

([1]) www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28. Nende menetluste abil rakendatakse suunavaid ja kohandavaid kontseptsioone, mida on käsitletud käesolevas kirjas sellisel viisil, mis on omane luureühenduse igale üksusele.

([2]) Selleks et tuua vaid üks näide, väidetakse presidendi poliitikasuunist nr 28 (PPD-28) rakendatavates riikliku julgeolekuasutuse (NSA) menetlustes, et „kui vähegi võimalik, toimub kogumine ühe või mitme valikukriteeriumi kasutamise kaudu, eesmärgiga suunata tähelepanu teatavate välisluure objektide andmete (nt konkreetne teadaolev rahvusvaheline terrorist või terroristide rühm) või teatavate välisluure teemade kogumisele (nt massihävitusrelvade leviku tõkestamine välisriigi või selle agentide poolt).“

([3]) http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf.

Ameerika Ühendriikides on välja töötatud läbimõeldud menetlused, tagamaks, et signaaliluure tegevust teostatakse üksnes asjaomaste riiklike julgeoleku eesmärkide edendamiseks. Igal aastal kehtestab president riigi kõrgeimad prioriteedid seoses välisluure andmete kogumisega pärast ulatuslikku ametlikku asutustevahelist protsessi. Riigi luuredirektor vastutab nende luureprioriteetide põhise riikliku luureprioriteetide raamistiku (NIPF) koostamise eest. Presidendi poliitikasuunisega nr 28 (PPD-28) tugevdati ja tõhustati ametivahelist menetlust tagamaks, et luureühenduse kõik luureprioriteedid vaadatakse läbi ja kiidetakse heaks kõrgetasemeliste poliitikakujundajate poolt. Luureteenistuse direktiivis (ICD) 204 on esitatud täiendavad juhised riikliku luureprioriteetide raamistiku (NIPF) kohta ning seda uuendati 2015. aasta jaanuaris, et hõlmata presidendi poliitikasuunise nr 28 (PPD-28) nõuded ([1]). Kuigi riiklik luureprioriteetide raamistik (NIPF) on klassifitseeritud, kajastatakse teatavat USA välisluure prioriteetidega seotud teavet igal aastal riigi luuredirektori (DNI) klassifitseerimata ülemaailmse ohu hinnangus, mis on kergesti kättesaadav riikliku luurejuhi ameti (ODNI) veebisaidilt.

Riikliku luureprioriteetide raamistiku (NIPF) prioriteedid on küllaltki kõrge üldise tasemega. Need hõlmavad selliseid teemasid, nagu teatavate välisriigi vastaste võime suurendamine kasutada tuuma- ja ballistilisi rakette, uimastikartelli korruptsiooni mõju ning inimõiguste kuritarvitamine teatavates riikides. Ning neid ei kohaldata mitte üksnes signaaliluure, vaid kogu luuretegevuse suhtes. Organisatsiooni, mis vastutab riiklikus luureprioriteetide raamistikus (NIPF) olevate prioriteetide konverteerimise eest tegelikuks signaaliluure andmete kogumiseks, nimetatakse riiklikuks signaaliluure komiteeks (National Signals Intelligence Committee – SIGCOM). See tegutseb riikliku julgeolekuasutuse (NSA) direktori juhtimisel, kes on ametisse määratud korralduse 12333 alusel „signaaliluure funktsionaalse juhina“, vastutades signaaliluure jälgimise ja koordineerimise eest luureühenduses ning seda nii kaitseministri kui ka riigi luuredirektori (DNI) järelevalve all. Riiklikus signaaliluure komitees (SIGCOM) on luureühenduse kõigi liikmete esindajad ning juhul kui Ameerika Ühendriigid rakendavad täielikult PPD-28, on täielikult esindatud ka muud osakonnad ja asutused, mis tunnevad poliitilist huvi signaaliluure vastu.

Kõik välisluure tarbijatest USA osakonnad ja asutused esitavad oma kogumistaotlused riiklikule signaaliluurele komiteele (SIGCOM). Riiklik signaaliluure komitee (SIGCOM) vaatab need taotlused läbi, tagab, et need on kooskõlas riikliku luureprioriteetide raamistikuga (NIPF) ning määrab neile prioriteedid, kasutades selliseid kriteeriume, nagu:

— Kas signaaliluure kaudu on sellisel juhul võimalik saada kasulikku teavet või on nõude täitmiseks olemas paremad või kulutõhusamad teabeallikad, nagu fotod või avatud lähteallikad?

— Kui oluline on seda teavet saada? Juhul kui see on riiklikus luureprioriteetide raamistikus (NIPF) kõrge prioriteediga, on see kõige sagedamini signaaliluure kõrge prioriteet.

— Millist liiki signaaliluuret on võimalik kasutada?

— Kas kogumine on kohandatud nii, et seda on võimalik teostada? Kas tuleks kehtestada ajaga seotud, geograafilised või muud piirangud?

Samuti tuleb USA signaaliluure nõuete protsessi käigus võtta arvesse muid tegureid, mis on järgmised:

— Kas kogumisobjekt või kogumisel kasutatav metoodika on eriti tundlik? Kui see on nii, peavad kõrgemad poliitikakujundajad selle läbi vaatama.

— Kas kogumine kujutab endast õigustamata riski seoses eraelu puutumatuse ja kodanikuvabadustega, sõltumata rahvusest?

— Kas eraelu puutumatuse ja riikliku julgeoleku huvide kaitsmiseks on vaja täiendavaid levitamise ja säilitamisega seotud kaitsemeetmeid?

Viimasena, pärast protsessi lõppu, võtavad koolitatud riikliku julgeolekuasutuse (NSA) töötajad riikliku signaaliluure komitee (SIGCOM) kinnitatud prioriteedid ning uurivad ja selgitavad välja konkreetsed valiku tingimused, nagu telefoninumbrid või e-posti aadressid, mida eeldavalt kogutakse nendele prioriteetidele vastava signaaliluure käigus. Kõik selektorid tuleb läbi vaadata ja heaks kiita enne, kui need sisestatakse riikliku julgeolekuasutuse (NSA) kogumissüsteemidesse. Isegi siis sõltuvad asjaolud, kas ja millal tegelik kogumine aset leiab siiski osaliselt täiendavatest kaalutlustest,

([1]) http://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf.

nagu asjaomaste kogumisressursside kättesaadavus. Selle protsessiga tagatakse, et USA signaaliluure andmete kogumise eesmärgid kajastavad olemasolevaid ja olulisi välisluure vajadusi. Ning loomulikult juhul, kui kogumist teostatakse vastavalt välisluure ja jälitustegevuse seadusele (FISA), peavad riiklik julgeolekuasutus (NSA) ja muud asutused järgima täiendavaid piiranguid, mille on heaks kiitnud vastuluurekohus (Foreign Intelligence Surveillance Court). Lühidalt ei otsusta riiklik julgeolekuasutus (NSA) ega ükski teine USA luureasutus ise, mida koguda.

Üldjuhul tagatakse sellega, et kõik USA luurega seotud prioriteedid on kehtestatud kõrgema astme poliitikakujundajate poolt, kes on parimal positsioonil, et määratleda USA välisluure nõuded, ning et need poliitikakujundajad ei arvesta mitte üksnes luureandmete kogumise potentsiaalse väärtuse, vaid ka sellise andmete kogumisega seotud riskidega, sealhulgas eraelu puutumatuse, riiklike majandushuvide ja välissuhetega seotud riskid.

Seoses vastavalt andmekaitseraamistikule Privacy Shield Ameerika Ühendriikidesse ülekantavate andmetega ja vaatamata sellele, et Ameerika Ühendriigid ei saa kinnitada või keelata teatavaid luuremeetodeid või -operatsioone, kohaldatakse PPD-28 nõudeid kõikide signaaliluure operatsioonide suhtes, mida Ameerika Ühendriigid teostavad, sõltumata kogutavate andmete liigist või allikast. Lisaks sellele kohaldatakse signaaliluure andmete kogumisele kohaldatavaid piiranguid ja kaitsemeetmeid signaaliluure suhtes, mida kogutakse mis tahes lubatud eesmärgil, sealhulgas nii välissuhete kui ka riikliku julgeoleku eesmärkidel.

Eespool käsitletud menetlused osutavad selgele kohustusele, mille eesmärk on vältida signaaliluure andmete meelevaldset ja valimatut kogumist ning rakendada meie valitsuse kõige kõrgemast tasandist alates mõistlikkuse põhimõtet. Presidendi poliitikasuunises nr 28 (PPD-28) ja asutuse rakendusmenetlustes on selgitatud uusi ja olemasolevaid piiranguid ning lähemalt kirjeldatud eesmärki, mille nimel Ameerika Ühendriigid signaaliluure andmeid koguvad ja kasutavad. Sellega peaks olema tagatud kindlus, et signaaliluurega seotud tegevust juurutatakse üksnes selleks, et täiendavalt õigustada välisluure eesmärke.

c. **Säilitamise ja levitamise piirangud**

Presidendi poliitikasuunise nr 28 (PPD-28) paragrahvis 4 on kehtestatud, et luureühenduse kõikidel üksuste suhtes kehtivad selged piirangud nende isikuandmete säilitamise ja levitamise kohta, mida kogutakse signaaliluure kaudu mitte-ameeriklaste kohta ning mis võrreldav USA isikute kohta kehtestatud piirangutega. Need eeskirjad kuuluvad kõikide luureühenduse üksuste suhtes kehtestatud menetluste hulka, mis avaldati 2015. aasta veebruaris ja on avalikult kättesaadavad. Selleks et välisluuret oleks võimalik säilitada või levitada, peavad isikuandmed olema seotud volitatud luurenõudega, nagu on määratletud eespool kirjeldatud riiklikus luureprioriteetide raamistiku (NIPF) protsessis; arvatakse mõistlikult olevat kuriteo tõendusmaterjal; või olema kooskõlas ühega muudest standarditest USA isiku andmete säilitamise kohta, mis on määratletud korralduses 12333, paragrahvis 2.3.

Teavet, mille suhtes sellist määratlemist ei ole tehtud, ei või säilitada üle viie aasta, välja arvatud juhul kui riigi luuredirektor määratleb selgesõnaliselt, et andmete jätkuv säilitamine on Ameerika Ühendriikide riikliku julgeoleku huvides. Seega peavad luureühenduse liikmed signaaliluure kaudu kogutud mitte-ameeriklastest isikute andmed kustutama viis aastat pärast nende kogumist, välja arvatud juhul, kui näiteks on määratletud, et andmed on vajalikud volitatud välisluure nõude suhtes, või riigi luuredirektor (DNI) määratleb pärast riikliku luurejuhi ameti (ODNI) kodanikuvabaduste kaitse ametniku ja asutuse eraelu puutumatuse ja kodanikuvabaduste ametnike seisukohtade läbivaatamist, et andmete jätkuv säilitamine on riikliku julgeoleku huvides.

Lisaks on kõikides presidendi poliitikasuunist nr 28 (PPD-28) rakendatavates asutuse meetmetes selgesõnaliselt nõutud, et isikuandmeid ei või levitada üksnes seetõttu, et üksikisik on mitte-ameeriklane, ning riiklik luurejuhi amet (ODNI) on välja andnud suunised kõikidele luureühenduse liikmetele, ([1]) et seda nõuet kajastada. Luureühenduse töötajad on kohustatud spetsiaalselt arvestama mitte-ameeriklaste eraelu puutumatuse huvidega, kui nad koostavad ja levitavad luurearuandeid. Eelkõige ei peeta signaaliluuret välismaalase tavapärase tegevuse kohta välisluureks, mida võiks levitada või püsivalt säilitada tulenevalt ainuüksi sellest asjaolust, välja arvatud juhul, kui see reageerib muul viisil volitatud välisluure nõudele. Sellega tunnistatakse olulist piirangut ning see vastab Euroopa Komisjoni muredele seoses välisluure määratluse ulatusega, nagu on kehtestatud korralduses 12333.

([1]) Intelligence Community Directive (ICD) 203, http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.

d. **Vastavus ja järelevalve**

USA välisluure järelevalve süsteemiga on tagatud range ja mitmetasandiline järelevalve, et tagada vastavus kohaldatavatele õigunormidele ja menetlustele, sealhulgas presidendi poliitikasuunise nr 28 (PPD-28) alusel kehtestatud signaaliluure andmete kogumise teel saadud mitte-ameeriklase isikuandmete kogumise, säilitamise ja levitamisega seotud seadused ja menetlused. Need hõlmavad:

— Luureteenistus palkab sadu järelevalvetöötajaid. Ainuüksi riiklikus julgeolekuasutuses (NSA) tegeleb üle 300 inimese vastavuse kontrollimisega ning samuti on muudel osakondadel järelevalveametid. Lisaks sellele annab justiitsministeerium ulatusliku ülevaate luuretegevuse kohta ning samuti annab ülevaate kaitseministeerium.

— Luureühenduse kõigis üksustes on peainspektori amet (Office of the Inspector General), mis vastutab muu hulgas välisluure tegevuse järelevalve eest. Peainspektorid on seaduse järgi sõltumatud; neil on ulatuslikud volitused teostada uurimisi, auditeid ja programmide läbivaatamist, sealhulgas seoses pettuste ja kuritarvitamise või seaduserikkumisega; ning nad saavad soovitada parandusmeetmeid. Kuigi peainspektori soovitused on mittesiduvad, avalikustatakse sageli peainspektori aruanded ning esitatakse igal juhul kongressile; see hõlmab järelmeetmete aruandeid juhul, kui eelmistes aruannetes soovitatud parandusmeetmetega ei ole veel lõpule jõutud. Seega teavitatakse Kongressi kõikidest mittevastavustest ning see võib avaldada survet, sealhulgas eelarveliste vahendite kaudu, et saavutada parandusmeetmete lõpule viimine. Mitmed peainspektori aruanded luureprogrammide kohta on avalikustatud ([1]).

— Riikliku luurejuhi ameti (ODNI) kodanikuvabaduste ja eraelu puutumatuse büroo (CLPO) ülesanne on tagada, et luureühendus tegutseb viisil, mis suurendab riikliku julgeolekut ja samal ajal kaitseb kodanikuvabadusi ja eraelu puutumatuse õiguseid ([2]).Muudel luureühenduse liikmetel on üksusesisesed eraelu puutumatuse ametnikud.

— Eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon (Privacy and Civil Liberties Oversight Board – PCLOB), mis kujutab endast statuudi alusel loodud sõltumatut asutust, tegeleb terrorismivastase võitluse programmide ja põhimõtete analüüsimise ja läbivaatamisega, sealhulgas signaaliluure kasutamine, tagamaks, et need kaitsevad adekvaatselt eraelu puutumatust ja kodanikuvabadusi. See on väljastanud mitmeid avalikke aruandeid luuretegevuse kohta.

— Nagu on allpool üksikasjalikumalt käsitletud, vastutab vastuluurekohus (Foreign Intelligence Surveillance Court) ehk sõltumatutest föderaalkohtunikest koosnev kohus vastavalt välisluure ja jälitustegevuse seadusele (FISA) teostatud signaaliluure andmete kogumise järelevalve ja vastavuse eest.

— Viimasena on USA Kongressil, täpsemalt esindajatekoja ja senati luurealased ja kohtunike komiteed (House and Senate Intelligence and Judiciary Committees), USA välisluure tegevusega, seahulgas USA signaaliluure, seoses oluline järelevalvega seotud vastutus.

Lisaks nendele ametlikele järelevalvemehhanismidele on luureühenduses kehtestatud mitmed mehhanismid tagamaks, et luureühendus järgib kogumisele kehtestatud piiranguid, mida on käsitletud eespool. Näiteks:

— Kabineti liikmed on kohustatud kinnitama oma signaaliluure nõuded igal aastal.

— Riiklik julgeolekuasutus (NSA) kontrollib signaaliluure eesmärke terve kogumisprotsessi vältel, et välja selgitada, kas sellega kogutakse tõepoolest väärtuslikke signaaliluure andmeid, mis vastavad prioriteetidele, ning peatab eesmärgile mittevastava andmete kogumise. Täiendavad menetlused tagavad, et valikutingimusi vaadatakse perioodiliselt läbi.

([1]) Vt nt U.S. Department of Justice Inspector General Report „A Review of the Federal Bureau of Investigation's Activities Under Section 702 of the Foreign Intelligence Surveillance Act of 2008" (September 2012), https://oig.justice.gov/reports/2016/o1601a.pdf.

([2]) *Vt* www.dni.gov/clpo.

— President Obama ametisse nimetatud sõltumatu järelevalverühma soovituse alusel on riigi luuredirektor (DNI) loonud uue mehhanismi, et jälgida eriti tundlike signaaliluure andmete kogumist ja levitamist eesmärgi või kogumisvahendi olemuse tõttu tagamaks, et see on kooskõlas poliitikakujundajate määratlustega.

— Viimasena vaatab riiklik luurejuhi amet (ODNI) igal aastal läbi luureühenduse ressursside jaotamise, võrreldes seda riikliku luureprioriteetide raamistiku (NIPF) prioriteetide ja luuremissiooni kui tervikuga. Käesolev ülevaade hõlmab luureandmete kogumise kõikide liikide, sealhulgas signaaliluure, väärtuse hindamisi ning samuti nii tagasivaadet sellele, kui edukas on luureühendus olnud oma eesmärkide saavutamisel, kui ka prognoosi selle kohta, mida luureühendus tulevikus vajab. Sellega tagatakse, et signaaliluure ressursse kohaldatakse kõige olulisemate riiklike prioriteetide suhtes.

Nagu tõendab käesolev põhjalik ülevaade, ei otsusta luureühendus omakäeliselt, milliseid kõnesid kuulata, samuti ei püüa ta kõike koguda ega tegutse õigusnormide väliselt. Selle tegevus on suunatud poliitikakujundajate kehtestatud prioriteetidele sellise protsessi kaudu, mis hõlmab valitsussektori sisendit ning mille üle teostavad järelevalvet riiklik julgeolekuasutus (NSA) ja riiklik luurejuhi amet (ODNI), justiitsministeerium ja kaitseministeerium.

Samuti hõlmab PPD-28 mitmeid teisi sätteid, tagamaks, et vastavalt signaaliluurele kogutud isikuandmed on sõltumata rahvusest kaitstud. Näiteks on presidendi poliitikasuunises nr 28 (PPD-28) kehtestatud andmete kaitse, juurdepääsu ja kvaliteediga seotud menetlused, et kaitsta signaaliluure kaudu kogutud isikuandmeid, ning kohustuslik koolitus tagamaks, et töötajad mõistavad vastutust kaitsta isikuandmeid, sõltumata rahvusest. Samuti on presidendi poliitikasuunises (PPD) kehtestatud täiendavad järelevalve ja vastavuse mehhanismid. Need hõlmavad perioodilisi auditeid ja läbivaatamisi asjaomaste järelevalve ja vastavuse ametnike poolt seoses tavadega signaaliluure andmetes sisalduvate isikuandmete kaitsmiseks. Samuti tuleb läbivaatamiste käigus hinnata asutuste vastavust menetlustele, mille eesmärk on kaitsta selliseid andmeid.

Lisaks sellele kehtestatakse presidendi poliitikasuunises nr 28 (PPD-28), et mitte-ameeriklastega seotud oluliste vastavusprobleemidega tegeldakse valitsuse kõrgematel tasanditel. Juhul kui esineb oluline probleem vastavusega, hõlmates signaaliluure tegevuse käigus kogutud mis tahes inimese isikuandmeid, tuleb sellest probleemist lisaks kõikidele olemasolevatele aruandlusnõuetele viivitamatult teatada riigi luuredirektorile (DNI). Juhul kui probleem hõlmab mitte-ameeriklase isikuandmed, selgitab riigi luuredirektor (DNI) välja riigisekretäri ja luurerühenduse asjaomase üksusega konsulteerides, kas on vaja võtta meetmed, et teavitada asjaomast välisriigi valitsust kooskõlas allikate ja meetodite ning USA töötajate kaitsega. Lisaks sellele, nagu kehtestatakse presidendi poliitikasuunises nr 28 (PPD-28), on riigisekretär määranud vanemametniku, asesekretär (Under Secretary) Catherine Novelli, ametisse kontaktisikuna, kes suhtleb välisriigi valitsustega, mis soovivad väljendada oma muret seoses Ameerika Ühendriikide signaaliluure tegevusega. See kõrgetasemeline tegevusega seotud kohustus illustreerib USA valitsuse jõupingutusi viimastel aastatel, eesmärgiga sisendada usaldust paljudesse ja kattuvatesse eraelu puutumatusega seotud kaitsemeetmetesse, mis on kehtestatud ameeriklaste ja mitte-ameeriklaste isikuandmete suhtes

e. **Kokkuvõte**

Ameerika Ühendriikides kehtestatud menetlused välisluure andmete kogumise, säilitamise ja levitamise kohta tagavad olulise eraelu puutumatuse kaitse seoses kõikide inimeste isikuandmetega, sõltumata nende rahvusest. Eelkõige tagatakse nende menetlustega, et meie luurerühendus suunab tähelepanu oma riiklikule julgeoleku missioonile, nagu on lubatud kohaldatavate seaduste, korralduste ja presidendi direktiivide alusel; kaitseb andmeid volitamata juurdepääsu, kasutamise ja avalikustamise eest; ning teostab tegevusi mitmetasandilise läbivaatamise ja järelevalve alusel, sealhulgas Kongressi järelevalvekomiteed. Presidendi poliitikasuunis nr 28 (PPD-28) ja seda rakendavad menetlused näitavad meie jõupingutusi seoses sellega, et laiendada teatavat vähendamist ning muid olulisi andmekaitse põhimõtteid seoses kõikide inimeste isikuandmetega, sõltumata rahvusest. USA signaaliluure andmete kogumise teel saadud isikuandmete suhtes kohaldatakse USA õiguse ja presidendi suunise põhimõtteid ja nõudeid, sealhulgas presidendi poliitikasuunises nr 28 kehtestatud kaitsemeetmeid. Nende põhimõtete ja tingimustega tagatakse, et kõiki isikuid koheldakse väärikalt ja austusväärselt, sõltumata nende rahvusest või elukohast, ning tunnistatakse, et kõikidel isikutel on õigustatud erahuvid nende isikuandmete menetlemisel.

II. VÄLISLUURE JA JÄLITUSTEGEVUSE SEADUS – PARAGRAHV 702

Välisluure ja jälitustegevuse seaduse (Foreign Intelligence Surveillance Act – FISA) ([1]) paragrahvi 702 kohane andmete kogumine ei ole „massiline ja valimatu", vaid kitsalt suunatud välisluure andmete kogumisele individuaalselt määratletud õiguspäraste eesmärkide alusel; on selgelt lubatud seadusest tulenevate volituste alusel; ning selle suhtes kohaldatakse nii sõltumatut kohtulikku järelevalvet ja sisulist läbivaatamist kui ka täitevvõimu ja Kongressi järelevalvet. Paragrahvi 702 alusel andmete kogumist peetakse signaaliluure andmete kogumiseks, mille suhtes kohaldatakse presidendi poliitikasuunise nr 28 (PPD-28) nõudeid ([2]).

Paragrahvi 702 kohane andmete kogumine on üks kõige väärtuslikumaid luureandmete allikaid, millega kaitstakse nii Ameerika Ühendriike kui ka meie Euroopa partnereid. Laiaulatuslik teave paragrahvi 702 toimimise ja järelevalve kohta on avalikult kättesaadav. Paljud programmiga seotud kohtuasjad, kohtulahendid ja järelevalve aruanded on avalikustatud ja väljastatud riikliku luurejuhi ameti (ODNI) veebisaidil aadressil www.icontherecord.tumblr.com. Lisaks sellele analüüsis eraelu puutumatuse kaitse ja kodanikuvabaduste järelevalve komisjon (PCLOB) põhjalikult paragrahvi 702 aruandes, mis on saadaval aadressil https://www.pclob.gov/library/702-Report.pdf ([3]).

Paragrahv 702 võeti vastu pärast ulatuslikku avalikku arutelu Kongressis osana FISA 2008. aasta muutmise seadusest ([4]). Sellega on lubatud välisluure andmete kogumine väljaspool Ameerika Ühendriike elavatele mitte-ameeriklaste kaudu koos USA elektroonilise side teenusepakkujate hädavajaliku abiga. Paragrahviga 702 on lubatud justiitsministril ja riigi luuredirektoril (DNI) – kaks kabineti tasandi ametnikku, kelle nimetab ametisse president ja kiidab heaks senat – esitada FISA kohtule iga-aastaseid sertifikaate ([5]). Nendes sertifikaatides määratletakse konkreetsed kategooriad kogutavate välisluure andmete kohta, nagu terrorismivastane võitluse või massihävitusrelvadega seotud luure, mis peavad vastama FISA põhimääruses kehtestatud välisluure kategooriatele ([6]). Nagu märkis eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon: „Nende piirangutega *ei* lubata koguda piiramatult teavet välismaalaste kohta" ([7]).

Samuti peavad sertifikaadid hõlmama eesmärgistatud kasutamise ja vähendamisega seotud menetlusi, mille peab läbi vaatama ja heaks kiitma välisluure ja jälitustegevuse seaduse (Foreign Intelligence Surveillance Act – FISA) kohus ([8]). Eesmärgistatud kasutamise menetlused on ette nähtud tagamaks, et andmete kogumine toimub üksnes statuudi alusel ning sertifikaatide reguleerimisalas; vähendamisega seotud menetlused on ette nähtud selleks, et piirata USA isikute andmete omandamist, levitamist ja säilitamist, ent need hõlmavad ka sätteid, millega on tagatud ka mitte-ameeriklaste isikuandmete oluline kaitse, nagu on allpool kirjeldatud. Lisaks sellele, nagu on eespool kirjeldatud, kehtestas president oma poliitikasuunises nr 28 (PPD-28), et luureühendus tagab täiendava kaitse mitte-ameeriklaste isikuandmetele ning seda kaitset kohaldatakse paragrahvi 702 alusel kogutud andmete suhtes.

Juhul kui kohus kiidab suunamis- ja minimeerimismenetlused heaks, ei peeta paragrahvi 702 kohast andmete kogumist suurehulgaliseks või valimatuks, vaid see „hõlmab täielikult teatavate isikute jälgimist, kelle kohta on tehtud individuaalne määratlemine", nagu teatas eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon (PCLOB) ([9]).

([1]) 50 U.S.C. § 1881a.

([2]) Ameerika Ühendriigid võivad saada ka kohtukorraldusi vastavalt FISA muudele sätetele andmete esitamise kohta, seahulgas andmeid, mis on üle kantud vastavalt andmekaitseraamistikule Privacy Shield. *Vt* 50 U.S.C. § 1801 *et seq*. Välisluure ja jälitustegevuse seaduse (Foreign Intelligence Surveillance Act – FISA) I ja III peatükk, mis vastavalt lubavad teostada elektroonilise järelevalvet ja füüsilist otsingut, nõuavad kohtu korraldust (välja arvatud hädaolukorras) ning nõuavad alati tõenäolist põhjust uskuda, et sihtmärk on võõrvõim või võõrvõimu agent. Välisluure ja jälitustegevuse seaduse (FISA) IV peatükis lubatakse kasutada pealtkuulamise seadmeid, vastavalt kohtumäärusele (välja arvatud hädaolukord) lubatud välisluure, vastuluure või terrorismivastane võitlusega seotud uurimistes. Välisluure ja jälitustegevuse seaduse (FISA) V peatükis lubatakse FBI-l, vastavalt kohtumäärusele (välja arvatud hädaolukord), saada enda valdusesse äridokumente, mis on asjaomased lubatud välisluure, vastuluure või terrorismivastase võitlusega seotud uurimistes. Nagu on käsitletud allpool, keelatakse USA vabaduse seadusega (USA FREEDOM Act) konkreetselt FISA pealtkuulamiskorralduste kasutamine laiaulatusliku kogumise eesmärgil ning kehtestatakse konkreetse valikutingimuse nõue tagamaks, et neid volitusi kasutatakse sihipäraselt.

([3]) Eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon (PCLOB), „Aruanne järelevalveprogrammi kohta, mida rakendatakse vastavalt välisluure ja jälitustegevuse seaduse (FISA) paragrahvile 702" (2. juuli 2014) („Eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjoni aruanne").

([4]) Vt Pub. L. No. 110–261, 122 Stat. 2436 (2008).

([5]) Vt 50 U.S.C. § 1881a(a) ja (b).

([6]) Vt *id*. § 1801(e).

([7]) Vt eraelu puutumatuse ja kodanikuvabaduste järelevalve komisoni (PCLOB) aruanne, 99.

([8]) Vt 50 U.S.C. § 1881a(d) ja (e).

([9]) Vt eraelu puutumatuse ja kodanikuvabaduste järelevalve komisoni (PCLOB) aruanne, 111.

Kogumist suunatakse selliste üksikute selektorite kasutamise kaudu, nagu e-posti aadressid või telefoninumbrid, mille korral on USA luurepersonal välja selgitanud, et neid kasutatakse tõenäoliselt selleks, et edastada välisluure andmete edastamiseks, mille liik on hõlmatud kohtule esitatud sertifikatsiooniga ([1]). Eesmärgi valimise alus peab olema dokumenteeritud ning seejärel vaatab justiitsministeerium läbi dokumendid kõikide selektorite kohta ([2]). USA valitsus on avalikustanud teabe, mille kohaselt jälgiti 2014. aastal paragrahvi 702 alusel ligikaudu 90 000 isikut, mis on imeväike arv võrreldes üle 3 miljardi internetikasutajaga üle kogu maailma ([3]).

Paragrahvi 702 kohaselt kogutud teabe suhtes kohaldatakse kohtu heakskiidetud vähendamise menetlusi, mille alusel tagatakse kaitse nii mitte-ameeriklastele kui ka ameeriklastele ning mis on avalikustatud ([4]). Näiteks paragrahvi 702 alusel saadud teabevahetust, sõltumata sellest, kas tegemist on ameeriklaste või mitte-ameeriklastega, säilitatakse range juurdepääsukontrolliga andmebaasides. Neid andmeid võivad läbi vaadata üksnes luureühenduse töötajad, keda on koolitatud eraelu puutumatuse kaitsega seotud vähendamise menetluste suhtes ja kelle juurdepääs nendele andmetele on heaks kiidetud seoses volitatud tegevuse sooritamisega ([5]). Andmete kasutamine on piiratud välisluure andmete või kuriteo tõendite määratlemisega ([6]). Vastavalt presidendi poliitikasuunisele nr 28 (PPD-28) võib seda teavet levitada üksnes välisluure või õiguskaitse eesmärgil; ainuüksi asjaolu, et üks teabevahetuse pool on mitte-ameeriklane, ei ole piisav ([7]). Samuti seatakse vähendamise menetluste ja presidendi poliitikasuunisega nr 28 (PPD-28) piirangud sellele, kui kaua võib säilitada vastavalt paragrahvile 702 omandatud andmeid ([8]).

Paragrahvi 702 järelevalve on ulatuslik ning seda teostatakse meie valitsuse kõikides kolmes harus. Statuuti rakendavates asutustes on mitmetasandiline sisekontroll, sealhulgas sõltumatud peainspektorid, ning tehnoloogiline kontroll andmetele juurdepääsu üle. Justiitsministeerium ja riiklik luurejuhi amet vaatavad hoolikalt läbi ja kontrollivad paragrahvi 702 rakendamist, et tõendada õigusnormidele vastavust; samuti kohaldatakse asutuste suhtes sõltumatut kohustust teavitada võimalikest mittevastavuse juhtumitest. Neid juhtumeid uuritakse ning kõik vastavusega seotud juhtumid edastatakse vastuluurekohtule (Foreign Intelligence Surveillance Court), presidendi luurejärelevalvenõukogule (President's Intelligence Oversight Board) ja Kongressile ning õiguskaitsevahendid võetakse vastavalt vajaduselev ([9]). Seni ei ole esinenud ühtegi tahtlikku katset rikkuda seadust ega hoida kõrvale õigusnõuetest ([10]).

FISA kohus mängib paragrahvi 702 rakendamisel olulist rolli. Kohus koosneb sõltumatutest föderaalkohtunikest, kelle ametiaeg FISA kohtus on küll seitse aastat, ent kes tegutsevad kohtunikena kogu oma eluaja jooksul, nagu kõik föderaalkohtunikud. Nagu eespool märgitud, peab kohus läbi vaatama, et iga-aastased sertifikaadid ning eesmärgistatud kasutamise ja vähendamise menetlused oleksid seadusega kooskõlas. Lisaks sellele, nagu on ka eespool märgitud, tuleb valitsusel kohust viivitamatult teavitada vastavusega seotud probleemidest, ([11]) ning mitmed kohtu arvamused avalikustatud ja avaldatud, demonstreerides kohtuliku kontrolli ja sõltumatuse erakordset taset nende juhtumite läbivaatamisel.

Kohtu rangeid protsesse on kirjeldanud selle endine eesistuja kohtunik Kongressile saadetud kirjas, mis on avaldatud ([12]). Ning USA vabaduse seaduse (USA FREEDOM Act) tulemusena, kirjeldatud allpool, on kohust nüüd selgesõnaliselt volitatud ametisse määrama väljaspool seisva juristi sõltumatu advokaadina eraelu puutumatuse nimel nendes juhtumites, milles käsitletakse uudseid või olulisi õigusküsimusi ([13]). Selline kaasamise tase riigi sõltumatu kohtuvõimu poolt luuretegevusse, mis on suunatud isikutele, kes ei ole selle riigi kodanikud ega asu selles riigis, on ebatavaline, kui mitte enneolematu, ning aitab tagada, et paragrahvi 702 kohane kogumine toimub asjakohastes õiguslikes piirides.

---

([1]) *Id.*

([2]) *Id.*, 8; 50 U.S.C. § 1881a(l); *vt ka* NSA Director of Civil Liberties and Privacy Report, „NSA's Implementation of Foreign Intelligence Surveillance Act Section 702" (hereinafter „NSA Report") 4, http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

([3]) Director of National Intelligence 2014 Transparency Report, http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014.

([4]) Vähendamise menetlused on saadaval: http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf („Riikliku julgeolekuasutuse (NSA) minimeerimismenetlused"); http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf; ja http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf.

([5]) Vt Riikliku julgeolekuasutuse (NSA) aruanne, 4.

([6]) Vt nt Riikliku julgeolekuasutuse (NSA) minimeerimismenetlused, 6.

([7]) Luureagentuuri PPD-28 menetlused on saadaval http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

([8]) Vt Riikliku julgeolekuasutuse (NSA) minimeerimismenetlused; PPD-28 paragrahv 4.

([9]) Vt 50 U.S.C § 1881(l); *vt ka* eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjoni (PCLOB) aruanne, 66–76.

([10]) Vt Semiannual Assessment of Compliance with Procedures and Guidelines Issues Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence at 2–3, http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf.

([11]) Rule 13 of the Foreign Intelligence Surveillance Court Rules of Procedures, http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

([12]) July 29, 2013 Letter from The Honorable Reggie B. Walton to The Honorable Patrick J. Leahy, http://fas.org/irp/news/2013/07/fisc-leahy.pdf.

([13]) Vt vabaduse seaduse § 401, p. 114–23.

Kongress teostab järelevalvet luurealastele ja kohtunike komiteedele esitatavate kohustuslike aruannete ning sagedaste infotundide ja arutelude kaudu. Need hõlmavad justiitsministeeriumi (Attorney General) esitatavat poolaastaaruannet, milles on dokumenteeritud paragrahvi 702 rakendamine ja kõik vastavusega seotud juhtumid; ([1]) justiitsministri (Attorney General) ja riigi luuredirektori (DNI) esitatud eraldi poolaastahinnang, milles on dokumenteeritud vastavus eesmärgistatud kasutamise ja vähendamise menetlustele, sealhulgas vastavus menetlustele, mis on ette nähtud tagama, et andmeid kogutakse põhjendatud välisluure eesmärgil; ([2]) luureüksuste juhtide esitatud aastaaruanne, mis hõlmab sertifikaati selle kohta, et paragrahvi 702 kohane andmete kogumisega saadakse jätkuvalt välisluure andmeid ([3]).

Lühidalt on paragrahvi 702 alusel kogumine seadusega lubatud; selle suhtes kohaldatakse mitmetasandilist läbivaatamist, kohtulikku kontrolli ja järelevalvet; ning, nagu FISA kohus väitis hiljuti avalikustatud arvamuses, ei tehta seda „laiaulatuslikult ega valimatult“, vaid. „diskreetsete eesmärgistatud kasutamise otsuste kaudu üksikute [teabevahetuse] rajatiste kohta“ ([4]).

III. USA VABADUSE SEADUS (USA FREEDOM ACT)

2015. aasta juunis jõustunud USA vabaduse seadus (USA FREEDOM Act) muutis oluliselt USA järelevalve ja muid riikliku julgeoleku asutusi ning suurendas läbipaistvust nende volituste kasutamise kohta ning FISA kohtu otsuste kohta, nagu on kehtestatud allpool ([5]). Seadusega tagatakse, et meie luure- ja õiguskaitsespetsialistidel on vajalikud volitused riigi kaitsmiseks, samal ajal tagades, et üksikisikute eraelu puutumatus on nõuetekohaselt kaitstud, kui neid volitusi rakendatakse. See tõhustab eraelu puutumatust ja kodanikuvabadusi ning suurendab läbipaistvust.

Seadusega on keelatud andmete laiaulatuslik kogumine, sealhulgas nii ameeriklaste kui ka mitte-ameeriklaste andmed, vastavalt erinevatele FISA sätetele või riikliku julgeoleku teabenõuete (National Security Letters) kasutamise kaudu, mis kujutavad endast seadusega lubatud halduskorralduste vormi ([6]). See keeld hõlmab eelkõige telefoni metaandmeid, mis on seotud USA-s ja väljaspool USA-d viibivate isikute vaheliste kõnedega, ning samuti hõlmab see andmekaitseraamistiku Privacy Shield andmete kogumist vastavalt nendele volitustele. Seadusega kehtestatakse, et valitsus tugineb nende volituste raames toimuval andmepäringul konkreetsele valikutingimusele ehk tingimusele, mille kohaselt määratletakse konkreetselt isik, konto, aadress või isiklik seade sellisel viisil, millega piiratakse otsitavate andmete reguleerimisala nii suures ulatuses kui on mõistlikult teostatav ([7]). Sellega tagatakse täiendavalt, et teabe kogumine luure eesmärgil on täpselt suunatud.

Samuti tehti seadusega olulisi muudatusi FISA kohtu menetlustes, mis nii suurendavad läbipaistvust kui ka annavad täiendavaid kinnitusi, et eraelu puutumatus on kaitstud. Nagu on märgitud eespool, lubatakse sellega julgeolekukontrolli advokaatide ekspertrühma loomine, kes on spetsialiseerunud eraelu puutumatuse ja kodanikuvabaduste, luureandmete kogumise, sidetehnoloogia või muudele asjaomastele teemadele ning keda võidakse kutsuda kohtusse *amicus curiae* juhtumites, mis hõlmavad olulisi või uudseid seaduse tõlgendamisi. Nendel advokaatidel on lubatud esitada õiguslikke argumente, mis suurendavad üksikisiku eraelu puutumatuse ja kodanikuvabaduste kaitset ning neil on juurdepääs kõikidele andmetele, sealhulgas salastatud teabele, mille korral kohus leiab, et see on vajalik nende tööülesannete täitmiseks ([8]).

Seadus põhineb ka USA valitsuse enneolematul läbipaistvusel luuretegevuse kohta, nõudes riigi luuredirektorilt (DNI), konsulteerides justiitsministriga (Attorney General), kas avalikustada või avaldada avalik kokkuvõte FISA kohtu või vastuluurekohtu (Foreign Intelligence Surveillance Court) iga otsuse, korralduse või arvamuse kohta, mis hõlmab mis tahes õigusnormide olulist konstrueerimist või tõlgendamist.

([1]) Vt 50 U.S.C § 1881f.
([2]) Vt *id.* § 1881a(l)(1).
([3]) Vt *id.* § 1881a(l)(3). Mõned nendest aruannetest on salajased.
([4]) Mem. Opinion and Order at 26 (FISC 2014), http://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.
([5]) Vt USA FREEDOM Act of 2015, Pub. L. No. 114–23, § 401, 129 Stat. 268.
([6]) Vt *id.* §§ 103, 201, 501. Riikliku julgeoleku teabenõuded (National Security Letters) on lubatud mitmete põhimääruste alusel ning võimaldavad FBI-l saada enda valdusesse andmeid, mis on hõlmatud krediidiaruannete, finantsandmete ning elektroonilise abonendi ja tehinguga seotud andmed teatavat liiki ettevõtetest, üksnes selleks, et kaitsta rahvusvahelise terrorismi või varjatud luuretegevuse eest. *Vt* 12 U.S.C § 3414; 15 U.S.C. §§ 1681u–1681v; 18 U.S.C. § 2709. Riikliku julgeoleku teabenõudeid (National Security Letters) kasutab FBI tavaliselt selleks, et koguda kriitilist sisuta andmeid terrorismivastane võitluse ja vastuluurega seotud uurimiste varajastes etappides – näiteks sellise abonendi identiteedi vastavusse viimine kontoga, kes võib olla suhelnud sellise terrorirühmituse agentidega, nagu ISIL. Riikliku julgeoleku teabenõude (National Security Letter) saanud isikutel on õigus see kohtus vaidlustada. Vt 18 U.S.C. § 3511.
([7]) Vt *id.*
([8]) Vt *id.* § 401.

Lisaks sellele on seaduses kehtestatud laiaulatuslik avalikustamine FISA andmete kogumise ja riikliku julgeoleku teabenõude (National Security Letter) taotluste kohta. Ameerika Ühendriigid peavad igal aastal avalikustama Kongressile ja avalikkusele taotletud ja saadud FISA korralduste ja sertifikaatide arvu; nende ameeriklaste ja mitte-ameeriklaste hinnanguline arv, kelle suhtes on teostatud ja keda on mõjutatud jälitustegevuse kaudu; ning *amici curiae* kohtumiste arv muude andmekirjete hulgas ([1]). Samuti on seadusega kehtestatud täiendav avalik aruandlus valitsuse poolt riikliku julgeoleku teabenõude taotluste arvu kohta seoses nii ameeriklaste kui ka mitteameeriklastega ([2]).

Seoses ettevõtete läbipaistvusega annab seadus ettevõtetele rida valikuid selle kohta, kuidas avalikult edastada valitsuselt saadud FISA korralduste ja direktiivide või riikliku julgeoleku teabenõuete (National Security Letters) koguarv, samuti tarbijate kontode arv, mille suhtes need korraldused kehtivad ([3]). Mitmed ettevõtjad on juba selle teabe avalikustanud, mille alusel on avaldatud nende tarbijate piiratud arv, kelle andmeid on otsitud.

Need ettevõtjate tegevuse läbipaistvuse aruanded näitavad, et USA luuretaotlused mõjutavad andmetest üksnes imeväikest osa. Näiteks on ühe suure ettevõtte hiljutisest läbipaistvuse aruandest näha, et ettevõttele laekusid riikliku julgeoleku taotlused (vastavalt FISA-le või riikliku julgeoleku teabenõuetele (National Security Letters)), mis mõjutasid vähem kui 20 000 selle kontodest sel ajal, kui ettevõttel oli vähemalt 400 miljonit abonenti. Teisisõnu mõjutasid kõik selle ettevõtte teatatud USA riikliku julgeoleku taotlused vähem kui.005 % selle tarbijatest. Isegi kui üks nendest taotlustest oleks olnud seotud programmi Safe Harbor andmetega, mis ei ole loomulikult nii, on ilmne, et taotlused on eesmärgipärased ja sobivas ulatuses, samuti ei ole need laiaulatuslikud ega valimatud.

Viimasena, samal ajal kui riikliku julgeoleku teabenõudeid (National Security Letters) volitavad põhimäärused on juba piiranud tingimused, mille raames võidakse sellise kirja saajat keelata seda avalikustamast, kehtestatakse seaduses täiendavalt, et sellised mitteavalikustamise nõudeid tuleb perioodiliselt läbi vaadata; selle kohaselt teavitatakse riikliku julgeoleku teabenõuete (National Security Letters) saajaid asjaoludest, mis enam ei toeta mitteavalikustamise nõuet; ning saajatele suunatud kodifitseeritud menetlused, et vaidlustada mitteavalikustamise nõuded ([4]).

Kokkuvõttes on USA vabaduse seaduses (USA FREEDOM Act) tehtud olulised muudatused seoses USA luureasutustega selge tõend Ameerika Ühendriikide ulatusliku jõupingutuse kohta, et seada isikuandmete kaitse, eraelu puutumatus, kodanikuvabadused ja läbipaistvus USA luuretegevuses esikohale.

## IV. LÄBIPAISTVUS

Lisaks USA vabaduse seaduse (USA FREEDOM Act) kohasele läbipaistvusele annab USA luureühendus avalikkusele palju täiendavat teavet, olles väga heaks näiteks seoses oma luuretegevuse läbipaistvusega. Luureühendus on avaldanud paljud oma eeskirjad, menetlused, vastuluurekohtu (Foreign Intelligence Surveillance Court) otsused ja muud salastamata materjalid, tagades erakordselt suure läbipaistvuse. Lisaks sellele on luureühendus oluliselt suurendanud statistika avalikustamist riikliku julgeoleku andmete kogumisega seotud asutuste valitsusepoolse rakendamise kohta. 22. aprillil 2015 andis luureühendus välja oma teise aastaaruande, milles esitati statistika selle kohta, kui sageli kasutab valitsus neid olulisi ametiasutusi. Samuti on riiklik luurejuhi amet (ODNI) oma veebisaidil ja veebisaidil *IC On the Record* avaldanud konkreetsete läbipaistvuspõhimõtete ([5]) kogumi ning rakenduskava, mille alusel konverteeritakse need põhimõtted konkreetseteks mõõdetavateks algatusteks ([6]). 2015. aasta oktoobris andis riiklik luurejuht (Director of National Intelligence) suunise määrata igas luureasutuse juhtkonnas ametisse luuretegevuse läbipaistvuse ametnik (Intelligence Transparency Officer), eesmärgiga edendada läbipaistvust ja juhtida läbipaistvusega seotud algatusi ([7]). Läbipaistvuse ametnik teeb tihedat koostööd kõikide luureasutuse eraelu puutumatuse ja kodanikuvabaduste ametnikega tagamaks, et läbipaistvus, eraelu puutumatus ja kodanikuvabadused oleksid jätkuvalt prioriteet.

([1]) Vt *id.* § 602.
([2]) Vt *id.*
([3]) Vt *id.* § 603.
([4]) Vt *id.* §§ 502(f)–503.
([5]) http://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles.
([6]) http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf.
([7]) Vt *id.*

Nende jõupingutuste näitena võib tuua selle, et riikliku julgeolekuasutuse (NSA) eraelu puutumatuse ja kodanikuvabaduste eest vastutav vanemametnik (Chief Privacy and Civil Liberties Officer) on viimaste aastate jooksul väljastanud mitmeid klassifitseerimata aruandeid, sealhulgas aruanded paragrahvi 702 põhise tegevuse, korralduse 12333 ning USA vabaduse seaduse (USA Freedom Act) kohta ([1]). Lisaks sellele teeb luureühendus tihedat koostööd eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjoni (PCLOB), Kongressi ja USA eraelu puutumatuse propageerimise kogukonnaga, eesmärgiga tagada suurem läbipaistvus seoses USA luuretegevusega niipalju kui see on võimalik ja kooskõlas tundlike luureallikate ja -meetodite kaitsmisega. Tervikuna vaadates on USA luuretegevus sama läbipaistev või läbipaistvam kui muu riigi oma terves maailmas ning sama läbipaistev kui on võimalik olla kooskõlas vajadusega kaitsta tundlikke allikaid ja meetodeid.

Selleks et teha kokkuvõte selle laiaulatusliku läbipaistvuse kohta, mis eksisteerib USA luuretegevuse suhtes:

— Luureühendus on avaldanud ja postitanud veebi tuhandeid lehekülgi kohtu arvamusi ja asutuse menetlusi, milles kirjeldatakse meie luuretegevuse konkreetseid menetlusi ja nõudeid. Samuti oleme avaldanud aruanded luureasutuste vastavuse kohta kohaldatavate piirangute suhtes.

— Kõrgemad luureametnikud räägivad regulaarselt avalikult oma organisatsioonide rollidest ja tegevusest, sealhulgas nende tööd reguleerivad vastavuspõhimõtete ja kaitsemeetmete kirjeldused.

— Luureühendus on vastavalt teabevabaduse seadusele (Freedom of Information Act) avaldanud mitmed täiendavad dokumendid luuretegevuse kohta.

— President väljastas presidendi poliitikasuunise nr 28 (PPD-28), millega kehtestatakse avalikult täiendavad piirangud meie luuretegevuse suhtes, ning riiklik luurejuhi amet (ODNI) on välja andnud kaks avalikku aruannet nende piirangute rakendamise kohta.

— Luureühendus on nüüd seadusega kohustatud avaldama FISA kohtu avaldatud olulisi õigusalaseid seisukohti või nende seisukohtade kokkuvõtteid.

— Valitsusel tuleb igal aastal koostada aruanne teatavate riiklike luureasutuste rakendamise ulatuse kohta ning ettevõtetel on lubatud teha sama.

— Eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjon (PCLOB) on väljastanud mitmeid avalikke aruandeid luuretegevuse kohta ning jätkab seda ka edaspidi.

— Luureühendus annab ulatuslikku salastatud teavet Kongressi järelevalvekomiteedele.

— Riigi luuredirektor (DNI) väljastas läbipaistvuse põhimõtted, millega reguleeritakse luureühenduse tegevust.

Sellist läbipaistvuse suurendamist jätkatakse. Kogu avalikustatav teave on loomulikult kättesaadav nii kaubandusministeeriumile kui ka Euroopa Komisjonile. Iga-aastane läbivaatamine kaubandusministeeriumi ja Euroopa Komisjoni vahel andmekaitseraamistiku Privacy Shield rakendamise kohta annab Euroopa Komisjonile võimaluse arutada kõiki küsimusi, mis tekivad väljastatud uue teabe tõttu, samuti muid andmekaitseraamistiku Privacy Shield ja selle toimimisega seotud teemasid ning mõistame, et ministeerium võib oma äranägemise järgi kutsuda muude asutuste esindajaid, sealhulgas luureühendus, sellel läbivaatamisel osalema. Seda loomulikult presidendi poliitikasuunises nr 28 (PPD-28) esitatud ELi liikmesriikidele suunatud mehhanismile, et tegeleda rohkem järelevalvega seotud probleemidega selleks ametisse nimetatud välisministeeriumi ametnikuga.

## V. HÜVITAMINE

USA õigusega on kehtestatud mitmeid hüvitamise liike üksikisikutele, kelle suhtes on teostatud ebaseaduslikku elektroonilist jälitustegevust riikliku julgeoleku eesmärgil. Välisluure ja jälitustegevuse seaduse (Foreign Intelligence Surveillance Act – FISA) raames ei ole abi taotlemine USA kohtust piiratud üksnes USA kodanikega. Üksikisikul, kellel on õigus esitada hagi, oleks abivahendid vaidlustada ebaseaduslik elektrooniline jälitustegevus välisluure ja jälitustegevuse

([1]) *Kättesaadav aadressilt* https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf.

seaduse (FISA) raames. Näiteks võimaldab välisluure ja jälitustegevuse seadus (FISA) isikutel, kelle suhtes on teostatud õigusvastast elektroonilist jälitustegevust, kaevata omavoliliselt tegutsevad USA valitsusametnikud kohtusse rahalise kahju eest, sealhulgas karistuslik kahjuhüvitis ja advokaaditasud. *Vt* 50 U.S.C. § 1810. Samuti on üksikisikutel, kellel on õigus esitada hagi, võimalus esitada tsiviilõigusliku alusega hagi rahalise kahju eest, sealhulgas kohtukulud, Ameerika Ühendriikide vastu juhul, kui FISA raames elektroonilise jälitustegevuse alusel kogutud andmed nende kohta on saadud ebaseaduslikul teel ning neid on tahtlikult kasutatud või avalikustatud. *Vt* 18 U.S.C. § 2712. Juhul kui valitsus kavatseb kasutada või avalikustada neid andmeid, mis on saadud või pärinevad rahulolematu isiku elektroonilisest jälitustegevusest FISA raames selle isiku vastu kohtu- või haldusmenetluses Ameerika Ühendriikides, tuleb teatada selle kavatsuse kohta ette kohtule ja isikule, kes võib seejärel vaidlustada jälitustegevuse seaduslikkuse ning otsida võimalusi andmeid mitte avalikustada. *Vt* 50 U.S.C. § 1806. Viimasena on välisluure ja jälitustegevuse seadusega (FISA) kehtestatud kriminaalkaristused nendele isikutele, kes teostavad tahtlikult õigusvastast elektroonilist jälitustegevust seaduse raames või kes tahtlikult kasutavad või avalikustavad andmed, mis on saadud ebaseadusliku jälitustegevuse tulemusena. *Vt* 50 U.S.C. § 1809.

ELi kodanikel on muid viise, et võtta õiguskaitsevahendid USA valitsusametnike vastu andmete ebaseadusliku kasutamise ja nendele juurdepääsu eest valitsuse poolt, sealhulgas valitsusametnikud, kes rikuvad seadust andmete ebaseadusliku juurdepääsu või kasutamise käigus väidetavalt riikliku julgeoleku eesmärgil. Arvutipettusi ja sellealast kuritarvitamist käsitleva seadusega (Computer Fraud and Abuse Act) on keelatud tahtlik volitamata juurdepääs (või laiendatud volitusega juurdepääs), et saada teavet finantsasutusest, USA valitsuse arvutisüsteemist või interneti kaudu sisenetud arvutist, samuti ohud, millega kahjustatakse kaitstud arvuteid väljapressimise või pettuse eesmärgil. *Vt* 18 U.S.C. § 1030. Kõik isikud, sõltumata nende rahvusest, kes kannatavad kahju või kaotust käesoleva seaduse rikkumise tulemusena võivad rikkuja (sealhulgas valitsusametnik) kohtusse kaevata kahjuhüvitise ja keelu või muu õiglase abi saamiseks paragrahvi 1030(g) alusel, olenemata sellest, kas kriminaalmenetlus on algatatud eeldusel, et menetluse teostamine hõlmab vähemalt ühte mitmest asjaoludest, mis on kehtestatud põhimääruses. Elektroonilist sidet käsitlev seadus (Electronic Communications Privacy Act – ECPA) reguleerib valitsuse juurdepääsu säilitatud elektroonilisele sidele ja toiminguandmetele, mis on kolmandatest isikutest sideteenuse pakkujate valduses. *Vt* 18 U.S.C. §§ 2701–2712. Elektroonilist sidet käsitleva seadusega (Electronic Communications Privacy Act – ECPA) on lubatud kahju kannatanud isikul salvestatud andmetele tahtliku õigusvastase juurdepääsu alusel valitsuse ametnikke kohtusse kaevata. Elektroonilist sidet käsitlevat seadust (ECPA) kohaldatakse kõikide isikute suhtes, sõltumata nende kodakondsusest, ning kahju kannatanud isikud võivad saada kahjutasu ja advokaaditasude hüvitamist. Finantspuutumatuse õiguse seadus (Right to Financial Privacy Act – RFPA) piirab USA valitsuse juurdepääsu üksikisikutest tarbijate panga- ja vahendaja-kaupleja andmetele. *Vt* 12 U.S.C. §§ 3401–3422. Finantspuutumatuse õiguse seaduse (RFPA) raames saab pank või vahendaja-kaupleja tarbija USA valitsuse kohtusse kaevata seadusest tuleneva, tegeliku ja karistusliku iseloomuga kahju eest, sest USA valitsus on ebaseaduslikult omandanud tarbija andmed, ning asjaolu, et selline ebaseaduslik juurdepääs oli tahtlik, toob automaatselt kaasa võimaliku distsiplinaarmeetmete võtmise asjaomaste valitsuse töötajate suhtes. *Vt* 12 U.S.C. § 3417.

Viimasena tagatakse teabevabaduse seadusega (FOIA) kõikidele isikutele võimalus otsida juurdepääsu olemasolevatele föderaalameti andmetele igal teemal, mille suhtes kohaldatakse teatavaid erandite kategooriaid. *Vt* 5 U.S.C. § 552(b). Need hõlmavad piiranguid salastatud riikliku julgeoleku teabele, muude isikute isikuandmetele ja uurimistoimingutega seotud teabele juurdepääsu kohta ning on võrreldavad riikide seatud piirangutega, mis põhinevad nende enda teabele juurdepääsu seadustel. Neid piiranguid kohaldatakse võrdselt nii ameeriklaste kui ka mitte-ameeriklaste suhtes. Vastavalt teabevabaduse seadusele taotletud andmete väljastamise kohta tekkinud vaidlused saab esitada halduskohtusse ning seejärel föderaalkohtusse. Kohus peab uuesti määratlema, kas andmeid hoitakse nõuetekohaselt, 5 U.S.C. § 552(a)(4)(B), ning saab sundida valitsust võimaldama andmetele juurdepääsu. Mõnel juhul on kohtud ümber lükanud valitsuse väited selle kohta, et teavet tuleb hoida salajasena ([1]). Kuigi rahalist kahju ei esine, võivad kohtud ette näha advokaaditasud.

## VI. JÄRELDUS

Ameerika Ühendriigid tunnistavad, et meie signaaliluure ja muu luurega seotud tegevuses tuleb arvestada, et kõiki isikuid tuleb kohelda väärikalt, sõltumata nende kodakondsusest või elukohast ning kõikidel isikutel on õigustatud erahuvid nende isikuandmete menetlemisel. Ameerika Ühendriigid kasutavad signaaliluuret üksnes selleks, et suurendada oma riiklikku julgeolekut ja välispoliitilisi huve ning kaitsta oma kodanikke ja oma liitlaste ja partnerite kodanikke ohu eest. Lühidalt ei tegele luureühendus mitte kellegi, sealhulgas tavaliste Euroopa kodanike, valimatu jälitamisega. Signaaliluure

([1]) Vt nt New York Times *vs.* Department of Justice, 756 F.3d 100 (2d Cir. 2014); American Civil Liberties Union *vs.* CIA, 710 F.3d 422 (D.C. Cir. 2014).

andmeid kogutakse üksnes siis, kui see on nõuetekohaselt lubatud ja viisil, mis vastab rangelt nendele piirangutele; üksnes pärast alternatiivsete allikate kättesaadavuse üle kaalumist, sealhulgas diplomaatilised ja avalikud allikad; ning viisil, millega seatakse esikohale nõuetekohased ja lubatavad alternatiivid. Ning kui võimalik, toimub signaaliluure andmete kogumine üksnes konkreetsetele välisluure eesmärkidele või teemadele suunatud kategooriate kasutamise teel.

Sellega seoses kinnitati USA poliitikat presidendi poliitikasuunises nr 28 (PPD-28). Selles raamistikus ei ole USA luureasutustel õigusalaseid volitusi, ressursse, tehnilist suutlikkust ega soovi peatada kogu maailma teabevahetust. Need asutused ei loe kõikide inimeste e-kirju ei Ameerika Ühendriikides ega maailma mastaabis. Vastavalt presidendi poliitika-suunisele nr 28 (PPD-28) tagavad Ameerika Ühendriigid mitte-ameeriklaste isikuandmete tugeva kaitse, mida kogutakse signaaliluure andmete kogumise käigus. Võimalikult suures ulatuses, mis on kooskõlas riikliku julgeolekuga, hõlmab see meetmeid ja menetlusi, et vähendada nende isikuandmete säilitamist ja levitamist, mis on seotud mitte-ameeriklastega, võrreldes ameeriklaste suhtes kehtestatud isikuandmete kaitsega. Lisaks sellele, nagu eelnevalt käsitletud, on suunatud paragrahvi 702 kohase põhjaliku järelevalverežiimi kontekstis FISA volitused hindamatud. Lisaks on USA vabaduse seaduses (USA FREEDOM Act) kehtestatud USA luureseaduse olulised muudatused ja riikliku luurejuhi ameti (ODNI) algatused läbipaistvuse edendamiseks luureühenduses suuresti tõhustanud kõikide üksikisikute eraelu puutumatust ja kodanikuvabadusi sõltumata nende rahvusest.

Lugupidamisega

Robert S. Litt

21 juuni 2016

Hr Justin S. Antonipillai
Nõunik
USA kaubandusministeerium
1401 Constitution Avenue, N.W.
Washington, DC 20230

Hr Ted Dean
Aseministri asetäitja (Deputy Assistant Secretary)
Väliskaubandusamet
1401 Constitution Avenue, N.W.
Washington, DC 20230

Lugupeetud hr Antonipillai ja hr Dean:

Kirjutan, et anda täiendavat teavet selle kohta, mil viisil toimub laiaulatuslik signaaliluure andmete kogumine Ameerika Ühendriikide poolt. Nagu on selgitatud presidendi poliitikasuunise nr 28 (PPD-28) joonealuses märkuses 5, tähendab „laiaulatuslik" kogumine suhteliselt suure koguse signaaliluure teel kogutava teabe või andmete omandamist tingimustel, kus luureühendusel ei ole võimalik otsingu täpsustamiseks kasutada midagi, mille abil identifitseerida konkreetseid objekte (näiteks objekti e-posti aadress või telefoninumber). Siiski ei tähenda see, et selline kogumine oleks „massiline" või „valimatu". Suunises PPP-28 nõutakse, et „[s]ignaaliluure tegevused peavad olema läbi viidud nii kohandatud kujul kui võimalik." Kõnealust volitust kasutades võtab luureühendus meetmeid selle tagamiseks, et isegi kui meil ei ole võimalik kasutada midagi, mis võimaldaks konkreetset identifitseerimist kogumise täpsemaks muutmiseks, sisaldavad kogutavad andmed tõenäoliselt välismaist luureinfot, mis vastab USA poliitikakujundajate väljendatud nõudmistele, järgides minu eelnevas kirjas kirjeldatud protsessi ning vähendab kogutava mitte-asjakohase teabe hulka.

Näiteks võidakse paluda luureühendusel hankida signaaliluure andmeid ühe terroristide grupi tegevuse kohta, kes tegutseb ühe Lähis-Ida riigi piirkonnas, mille kohta arvatakse, et ta kavandab rünnakuid Lääne-Euroopa riikide vastu, ent ei ole teada kõnealuse terroristide grupiga seotud üksikisikute nimed, telefoninumbrid, e-posti aadressid või muud konkreetset identifitseerimist võimaldavad üksikasjad. Me võiksime püüda kõnealuse grupi sihikule võtta, kogudes asjaomasesse piirkonda suunduva ja sealt lähtuva teabevahetuse, et seda hiljem läbi vaadata ja analüüsida eesmärgiga välja selgitada kõnealuse grupiga seotud teabevahetus. Nii toimides püüaks luureühendus kitsendada kogumist niipalju kui võimalik. Seda peetakse laiaulatuslikuks kogumiseks, sest kategooriate kasutamine ei ole võimalik, ent see ei ole „massiline" ega „valimatu", pigem nii täpselt fokusseeritud kui võimalik.

Seega, isegi kui eesmärgi seadmine konkreetsete selektorite abil ei ole võimalik, ei kogu Ameerika Ühendriigid kogu teabevahetust kõikidest kommunikatsioonivahenditest kogu maailmas, vaid rakendavad filtreid ja muid tehnilisi vahendeid, et keskenduda kogumisel nendele seadmetele, mis tõenäoliselt sisaldavad välisluure andmete väärtusega teabevahetust. Nii toimides puudutab Ameerika Ühendriikide signaaliluuretegevus vaid murdosa kogu internetti läbivast teabevahetusest.

Lisaks, nagu on märgitud minu eelmises kirjas, toob „laiaulatuslik" kogumine kaasa suurema riski koguda mitte-asjakohast teabevahetust, seetõttu sätestab PPD-28 piirangu, et luureühendus tohib laiaulatuslikult kogutud signaaliluure andmeid kasutada ainult kuuel konkreetsel eesmärgil. PPD-28 ja asutuse tavad PPD-28 rakendamisel, samuti kohapiirangud signaaliluure teel saadud isikuandmete säilitamiseks ja levitamiseks, vaatamata asjaolule, kas teave koguti laiaulatuslikult või suunatult, ning sõltumata üksikisiku rahvusest.

Seega ei ole luurerühenduse „laiaulatuslik" andmete kogumine „massiline" või „valimatu", vaid hõlmab meetodite ja tööriistade rakendamist kogutava filtreerimiseks, et keskenduda materjalile, mis vastab USA poliitikakujundajate väljendatud nõudmistele välismaiste luureandmete kohta, samal ajal mitte-asjakohase teabe kogumist minimeerides, ja

näeb ette ranged reeglid mitte-asjakohase teabe, mis võidakse omandada, kaitsmiseks. Selles kirjas kirjeldatud tavad ja menetlused kehtivad kõikidel juhtudel laiaulatuslikult signaaliluure andmete kogumise kohta, sealhulgas laiaulatuslik Euroopasse suunduva või Euroopast lähtuva teabevahetuse kogumine, ilma et kinnitataks või eitataks sellise kogumise toimumist.

Te küsisite minult rohkem teavet eraelu puutumatuse ja kodanikuvabaduste järelevalve komisjoni (Privacy and Civil Liberties Oversight Board – PCLOB) ning peainspektorite ning nende pädevuse kohta. PCLOB on sõltumatu täitevvõimuasutus. Kahepoolselt toetatava viieliikmelise juhatuse liikmed määratakse presidendi poolt ja need kinnitab senat ([1]). Juhatuse liikmed on teenistusse määratud kuueks aastaks. Juhatuse liikmed ja töötajad varustatakse asjakohaste juurdepääsulubadega, et võimaldada neil täita oma seadusest tulenevaid ülesandeid ja kohustusi ([2]).

PCLOBi missioon on tagada, et föderaalvalitsuse jõupingutused terrorismi tõkestamiseks on tasakaalus vajadusega kaitsta isikuandmeid ja kodanikuvabadusi. Juhatuse kaks peamist ülesannet on järelevalve ja nõustamine. PCLOB määrab ise oma töökava ja otsustab, milliseid järelevalvelisi või nõustamistegevusi ta soovib ette võtta.

Oma *järelevalve* rolli täitmiseks vaatab PCLOB läbi ja analüüsib täitevvõimu tegevusi riigi kaitsmisel terrorismi eest, et vajadus selliste tegevuste järele oleks tasakaalus vajadusega kaitsta isikuandmeid ja kodanikuvabadusi ([3]). PCLOBi viimane valminud järelevalve-ülevaade keskendus FISA paragrahvi 702 alusel teostatud jälitusprogrammidele ([4]). Käesoleval hetkel vaatavad nad läbi korralduse 12333 alusel läbiviidavaid luuretegevusi ([5]).

Oma *nõuandvas* rollis tagab PCLOB, et seaduste, määruste ja tavade väljatöötamisel ja rakendamisel, mis on seotud riigi kaitsmisega terrorismi eest, võetaks asjakohaselt arvesse ka vabadusi ([6]).

Oma missiooni täitmiseks omab juhatus statuudi alusel õigust juurdepääsuks kõikidele asjakohastele asutuse andmetele, aruannetele, auditite, dokumentidele, paberitele, soovitustele ja muudele asjakohastele materjalidele, sealhulgas kooskõlas seadustega salastatud teabele ([7]). Lisaks võib juhatus küsitleda, võtta selgitusi või avalikke tunnistusi kõikidelt täitevvõimuasutuste ametnikelt või töötajatelt ([8]). Lisaks võib juhatus teha kirjaliku taotluse peaprokurörile juhatuse nimel korralduse andmiseks väljaspool täitevvõimu tegutsevatele isikutele asjakohase teabe andmiseks ([9]).

Viimasena, PCLOB tegevus peab seadusest tulenevalt olema avalikkuse jaoks läbipaistev. See tähendab, et avalikkusele tuleb oma tegevusest võimalikult suures ulatuses teada anda, korraldades avalikke arutelusid ning tehes oma aruanded avalikkusele kättesaadavaks, kaitstes seejuures salastatud teavet ([10]). Peale selle on PCLOB kohustatud sellest ette kandma, kui mõni täitevvõimuasutus ei järgi tema nõuandeid.

Luureühenduse peainspektorid viivad luureühenduses läbi programmide ja tegevuste auditeid, inspekteerimisi ja ülevaatusi, et kindlaks teha süsteemseid riske, haavatavusi ja puudusi ning nende suhtes meetmeid võtta. Lisaks uurivad peainspektorid luureühenduse programme ja tegevusi puudutavaid kaebusi või teavet nendes esineva väidetava seaduste, reeglite või määruste rikkumise või oskamatu juhtimise kohta; suure raharaiskamise kohta; võimu kuritarvituse või

([1]) 42 U.S.C. 2000ee(a), (h).
([2]) 42 U.S.C. 2000ee(k).
([3]) 42 U.S.C. 2000ee(d)(2).
([4]) *Vt üldiselt* https://www.pclob.gov/library.html#oversightreports.
([5]) *Vt üldiselt* https://www.pclob.gov/events/2015/may13.html.
([6]) 42 U.S.C. 2000ee(d)(1); *vt ka* PCLOB Advisory Function Policy and Procedure, Policy 2015-004, *kättesaadav aadressil* https://www.pclob.gov/library/Policy-Advisory_Function_Policy_Procedure.pdf.
([7]) 42 U.S.C. 2000ee(g)(1)(A).
([8]) 42 U.S.C. 2000ee(g)(1)(B).
([9]) 42 U.S.C. 2000ee(g)(1)(D).
([10]) 42 U.S.C. 2000eee(f).

olulise ja konkreetse ohu kohta rahva tervisele ja turvalisusele. Peainspektori sõltumatus on iga tema poolt väljastatava aruande, järelduse ja soovituse objektiivsuse ja aususe kriitilise tähtsusega komponent. Ülikriitilise tähtsusega komponentideks peainspektori sõltumatuse säilitamisel on ka peainspektori ametisse määramise ja ametist vabastamise protsess; eraldiseisvad pädevused operatiivtöö, eelarve ja personali osas ning aruandluse esitamise nõue nii täitevvõimuasutuste juhtidele kui ka Kongressile.

Kongress asutas sõltumatu peainspektori ametikoha igasse täitevvõimuasutusse, sealhulgas igasse luureühenduse üksusesse ([1]). 2015. eelarveaastaks vastu võetud luure volitamise seaduse (Intelligence Authorization Act) alusel määratakse peaaegu kõik peainspektorid, kes teostavad järelevalvet luureühenduse üksuste üle, presidendi ja kinnitatakse senati poolt, sealhulgas justiitsministeerium (Department of Justice), luure keskagentuur (Central Intelligence Agency), riiklik julgeolekuasutus (National Security Agency) ja luureühendus ([2]). Lisaks on kõnealused peainspektorid alaliselt kohale määratud, parteidest sõltumatud ametnikud, keda võib ametist vabastada ainult president. Kuigi USA konstitutsioonis sätestatakse, et presidendil on õigus peainspektori ametist vabastamiseks, on seda sätet harva kasutatud ja selle kohaselt peab president esitama Kongressile 30 päeva enne peainspektori ametist vabastamist kirjaliku põhjenduse ([3]). Kõnealune peainspektori määramise protsess tagab, et peainspektori valikul, ametisse määramisel ja ametist vabastamisel ei esine lubamatut mõjutamist täitevvõimu ametnike poolt.

Teiseks on peainspektoritel olulised seadusest tulenevad volitused täitevvõimuasutuste programmide ja tegevuse kohta auditite, uurimiste ja ülevaatuste läbiviimiseks. Lisaks järelevalve teostamise eesmärgil läbiviidavatele uurimistele ja ülevaatustele, mis on nõutavad seaduste alusel, on peainspektoritel laiad volitused oma äranägemisel ja valikul teostada järelevalvet programmide ja tegevuste üle ([4]). Asjaomaste volituste teostamiseks on seadusega tagatud, et peainspektoritel on kasutada sõltumatud ressursid oma kohustuste täitmiseks, sealhulgas pädevus võtta tööle oma personal ning eraldi dokumenteerida oma Kongressile esitatavad eelarvetaotlused ([5]). Seadusega on tagatud, et peainspektoritel on juurdepääs teabele, mis on vajalik nende kohustuste täitmiseks. Kõnealune õigus hõlmab otsest juurdepääsu kõikidele asutuse andmetele ja programmide ning tegevuste kohta käivale üksikasjalikule teabele, vaatamata selle klassifikatsioonile; pädevust anda korraldus informatsiooni ja dokumentide esitamiseks ja vande võtmise pädevust ([6]). Piiratud juhtudel võib täitevvõimuasutuse juht keelata peainspektori tegevuse, juhul kui peainspektori audit või uurimine rikuks olulisel määral Ameerika Ühendriikide riikliku julgeoleku huve. Ka nimetatud õiguse kasutamist on äärmiselt harva ette tulnud ja selleks on vaja, et asjaomase asutuse juht teavitaks Kongressi 30 päeva ette kõnealuse õiguse kasutamise põhjustest ([7]). Riiklik luurejuht (Director of National Intelligence) ei ole kunagi kasutanud oma volitusi ühegi peainspektori tegevuse piiramiseks.

Kolmandaks, peainspektoritel on kohustus hoida nii täitevvõimuasutuste juhte kui ka Kongressi aruannete abil täielikult ja jooksvalt informeerituna täitevvõimuasutuste programmide ja tegevusega seoses esinevate pettuste ja muude tõsiste probleemide, kuritarvituste ja puudujääkide suhtes ([8]). Kahte kohta aruandluse esitamine tugevdab peainspektori sõltumatust, tuues peainspektori järelevalvelisse tegevusse läbipaistvust ning võimaldades asutuste juhtidel rakendada peainspektori soovitused enne, kui Kongress jõuab seadusandlikku tegevust algatada. Näiteks kohustab seadus peainspektoreid igal poolaastal koostama kõnealuseid probleeme ning seni võetud heastamismeetmeid kirjeldavaid aruandeid ([9]). Täitevvõimuasutused võtavad peainspektorite järeldusi tõsiselt ning lisavad tihti asjaomaste aruannete või

([1]) Muudetud 1978. aasta peainspektori seaduse (Inspector General Act of 1978) paragrahvid 2 ja 4; muudetud 1947. aasta riikliku julgeoleku seaduse (National Security Act of 1947) paragrahvid 103H(b) ja (e); keskse luuretegevuse seaduse (Central Intelligence Act) paragrahv 17(a).

([2]) Vt Pub. L. No. 113–293, 128 Stat. 3990, (19. detsember 2014). President ei määra ametisse ainult riigikaitselise luure agentuuri (Defense Intelligence Agency) ja riikliku georuumilise luure agentuuri (National Geospatial-Intelligence Agency) peainspektoreid; kaitseministeeriumi (DOD) peainspektoril ja luureühenduse peainspektoril on kattuv pädevus.

([3]) Muudetud 1978. aasta peainspektori seaduse (IG Act of 1978) paragrahv 3; riikliku julgeoleku seaduse (Nat'l Sec. Act) paragrahv 103H (c); keskse luuretegevuse seaduse (CIA Act) paragrahv 17(b).

([4]) Vt peainspektori seaduse (IG Act o 1947) paragrahvid 4(a) ja 6(a)(2); riikliku julgeoleku seaduse (Nat'l Sec. Act) paragrahvid 103H(e) ja (g)(2)(A); keskse luuretegevuse seaduse (CIA Act) paragrahvid 17(a) ja (c).

([5]) Peainspektori seaduse (IG Act) paragrahvid 3(d), 6(a)(7) ja 6(f); riikliku julgeoleku seaduse (Nat'l Sec. Act) paragrahvid 103H(d), (i), (j) ja (m); keskse luuretegevuse seaduse (CIA Act) paragrahvid 17(e)(7) ja (f).

([6]) Peainspektori seaduse (IG Act) paragrahvid 6(a)(1), (3), (4), (5) ja (6); riikliku julgeoleku seaduse (Nat'l Sec. Act) paragrahvid 103H(g)(2); keskse luuretegevuse seaduse (CIA Act) paragrahvid 17(e)(1), (2), (4) ja (5).

([7]) Vt nt peainspektori seaduse (IG Act) paragrahvid 8(b) ja 8E(a); riikliku julgeoleku seaduse (Nat'l Sec. Act) paragrahvid 103H(f); keskse luuretegevuse seaduse (CIA Act) paragrahv 17(b).

([8]) Peainspektori seaduse (IG Act) paragrahv 4(a)(5); riikliku julgeoleku seaduse (Nat'l Sec. Act) paragrahvid 103H(a)(b)(3) ja (4); keskse luuretegevuse seaduse (CIA Act) paragrahvid 17(a)(2) ja (4).

([9]) peainspektori seaduse (IG Act) paragrahvid 2(3), 4(a) ja 5; riikliku julgeoleku seaduse (Nat'l Sec. Act) paragrahv 103H(k); keskse luuretegevuse seaduse (CIA Act) paragrahv 17(d). Justiitsministeeriumi peainspektor teeb oma avalikkusele avaldatavad aruanded kättesaadavaks internetis aadressil http://oig.justice.gov/reports/all.htm. Samamoodi teeb luureühenduse peainspektor oma poolaastaaruanded avalikkusele kättesaadavaks aadressil https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.

muude Kongressile ja mõnel juhul avalikkusele esitatavate aruannete juurde asutusepoolse kinnituse peainspektori soovitustega nõustumise ja nende rakendamise kohta ([1]). Lisaks sellisele kahte kohta aruannete esitamise kohustusele on peainspektorite ülesandeks ka täitevvõimuasutuste siseinformaatorite suunamine asjakohase Kongressi järelevalvekomitee juurde, et avalikustada täitevvõimuasutuses väidetavalt esinevat pettust, raiskamist või kuritarvitusi. Siseinformaatorite identiteeti kaitstakse täitevvõimuasutusele teatavaks saamise eest, mis kaitseb siseinformaatoreid võimalike lubamatute personali või juurdepääsulubasid puudutavate tegevuste eest, mida võidakse ette võtta kättemaksuks peainspektorile ettekandmise eest ([2]). Kuna siseinformaatorid on tihti peainspektorile uurimiste läbiviimisel teabeallikateks, suurendab suutlikkus neile murettekitavatest asjaoludest Kongressile ette kanda, ilma täitevvõimuasutusepoolse mõjutamiseta, peainspektori poolt teostatava järelevalve tõhusust. Tänu sellisele sõltumatusele suudavad peainspektorid objektiivselt ja ausalt kaasa aidata kokkuhoiule, tõhususele ja vastutuse kasvule täitevvõimuasutustes.

Kongress on asutanud peainspektorite nõukogu aususe ja tõhususe küsimustes. Kõnealune nõukogu töötab muude asjade kõrval välja peainspektori standardeid auditite, uurimiste ja ülevaatuste läbiviimiseks; edendab koolitust ja omab pädevust kontrollida väidetavaid peainspektorite vääritu käitumise juhtumeid, olles nii kriitiliseks järelevaatajaks peainspektorite üle, kellele on kõikide teiste jälgimine usaldatud ([3]).

Loodan, et käesolev teave on Teile abiks.

Austusega
Robert S. Litt
Õigusnõunik

([1]) Peainspektori seaduse (IG Act) paragrahvid 2(3), 4(a) ja 5; riikliku julgeoleku seaduse (Nat'l Sec. Act) paragrahv 103H(k); keskse luuretegevuse seaduse (CIA Act) paragrahv 17(d). Justiitsministeeriumi peainspektor teeb oma avalikkusele avaldatavad aruanded kättesaadavaks internetis aadressil http://oig.justice.gov/reports/all.htm. Samamoodi teeb luureühenduse peainspektor oma poolaastaaruanded avalikkusele kättesaadavaks aadressil https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.

([2]) Peainspektori seaduse (IG Act) paragrahv 7; riikliku julgeoleku seaduse (Nat'l Sec. Act) paragrahv 103H(g)(3); keskse luuretegevuse seaduse (CIA Act) paragrahv 17(e)(3).

([3]) Peainspektori seaduse paragrahv 11.

*VII LISA*

**Abiprokuröri asetäitja (Deputy Assistant Attorney General) ja rahvusvaheliste suhete nõuniku Bruce Swartzi kiri, USA justiitsministeerium**

19. veebruar 2016

Justin S. Antonipillai
Nõunik
USA kaubandusministeerium
1401 Constitution Ave., NW
Washington, DC 20230

Ted Dean
Aseministri asetäitja (Deputy Assistant Secretary)
Väliskaubandusamet
1401 Constitution Ave., NW
Washington, DC 20230

Lugupeetud hr Antonipillai ja hr Dean:

Käesoleva kirjaga 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 ([1]). Need õiguslikud menetlused on mittediskrimineerivad selles suhtes, et neid kasutatakse Ameerika Ühendriikide ettevõtetest teabe saamiseks, sealhulgas ettevõtetelt, mis sertifitseerivad end ise ELi-USA andmekaitseraamistiku Privacy Shield kaudu, sõltumata andmesubjekti rahvusest. Lisaks sellele võivad need ettevõtted, mille suhtes on algatatud kohtuasi Ameerika Ühendriikides, vaidlustada selle kohtus, nagu on allpool käsitletud ([2]).

Seoses andmete saamisega riigiasutuste poolt väärib eriti märkimist Ameerika Ühendriikide põhiseaduse neljas muudatus (Fourth Amendment), milles on sätestatud, et „inimeste õigus turvalisusele oma isiku, maja, dokumentide ja mõju suhtes ebamõistlike läbiotsimiste ja haarangute vastu ei tohi rikkuda ning läbiotsimisordereid ei väljastata, välja arvatud tõenäolise põhjuse korral, mis tugineb vandele või kinnitusele ning milles kirjeldatakse konkreetselt läbiotsitavat asukohta ja läbiotsitavaid isikuid või esemeid". U.S. Const. amend. IV. USA ülemkohus (United States Supreme Court) väitis kohtuasjas *Berger vs. State of New York* „käesoleva muudatuse peamine eesmärk, nagu on tunnistatud asjaomase kohtu loendamatutes otsustes, on kaitsta üksikisikute eraelu puutumatust ja julgeolekut valitsusametnike suvalise sekkumise eest." 388 U.S. 41, 53 (1967) (*viide Camara vs. Mun. San Francisco kohus*, 387 U.S. 523, 528 (1967)). Riiklikes kriminaaluurimistes nõutakse neljanda muudatusega (Fourth Amendment) üldjuhul õiguskaitseametnikelt seda, et nad saaksid enne läbiotsimist kohtu poolt väljastatud orderi. *Vt Katz vs. Ameerika Ühendriigid*, 389 U.S. 347, 357 (1967). Juhul kui volitamise nõue ei kehti, kohaldatakse valitsuse tegevuse suhtes neljanda muudatuse kohast mõistlikkuse testi. Põhiseaduses on seega tagatud, et USA valitsusel ei ole piiramatut ega omavolilist võimu koguda isikuandmeid.

**Kriminaalõigust rakendavate õiguskaitseorganite volitused:**

Riigiprokurörid, kes on justiitsministeeriumi (DOJ) ametnikud, ning föderaalse uurimisasutused agendid, sealhulgas föderaalse juurdlusbüroo (Federal Bureau of Investigation – FBI) ehk justiitsministeeriumi alla kuuluva õiguskaitseasutuse agendid, on võimelised sundima Ameerika Ühendriikide ettevõtteid dokumente ja muid registriandmeid loovutama

([1]) Käesolevas ülevaates ei kirjeldata riikliku julgeoleku uurimisvahendeid, mida kasutatakse õiguskaitsena võitluses terrorismi vastu ja muudes riikliku julgeoleku uurimistes, sealhulgas riikliku julgeoleku teabenõudeid (National Security Letters – NSL) teatavate registriandmete kohta krediidiaruannetes, finantsaruannetes, elektroonilistes tarbija- ja tehinguaruannetes, vt 12 U.S.C.§ 3414; 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 18 U.S.C. § 2709, ning elektroonilise jälitustegevuse, läbiotsimiskorralduste, äridokumentide ja muude teabekogumite kohta vastavalt välisluure ja jälitustegevuse seadusele (Foreign Intelligence Surveillance Act – FISA), vt 50 U.S.C. § 1801 *et seq*.

([2]) Käesolevas dokumendis käsitletakse föderaalse õiguse täitmist ja reguleerivaid asutusi; osariigi seaduse rikkumist uuritakse osariigisiseselt ning hagi esitatakse osariigi kohtusse. Riigi õiguskaitseorganid kasutavad kohtumäärusi ja -korraldusi, mis on välja antud riigiõiguse raames sisuliselt samal viisil, nagu on siin kirjeldatud, kuid võimalusega, et riigi kohtumenetluse suhtes võidakse kohaldada riigi põhiseaduses kehtestatud kaitset, mis on ülimuslik USA põhiseaduses kehtestatud kaitse suhtes. Osariigi õiguskaitse peab olema vähemalt võrdne USA põhiseaduse järgse kaitsega, sealhulgas, aga mitte ainult, neljas muudatus.

kriminaalse uurimise eesmärgil mitut liiki kohustuslike õigusprotsesside kaudu, sealhulgas vandemeeste kogu (grand jury) kohtukorraldused, halduskorraldused ja läbiotsimisorderid, ning nad võivad enda valdusesse saada muud teabevahetust vastavalt föderaalsele kriminaalmenetluse raames pealtkuulamise volitustele.

Vandemeeste kogu või kohtukorraldused: Kriminaalkohtu korraldusi kasutatakse selleks, et toetada suunatud õiguskaitsega seotud uurimisi. Vandemeeste kogu kohtukorraldus on vandemeeste kogu välja antud ametlik taotlus (tavaliselt riigiprokuröri taotlusel), et toetada vandemeeste kogu uurimist seoses kriminaalõiguse teatava rikkumise kahtlusega. Vandemeeste kogud on uurimisega tegelevad üksused kohtus ning need määratakse kas kohtuniku või magistraadi poolt. Kohtukorraldusega võidakse nõuda, et keegi menetluses ütlusi annab või koostab või avaldab äridokumendid, elektrooniliselt säilitatud teabe või muud materiaalsed objektid. Teave peab olema uurimise suhtes asjaomane ning kohtukorraldus ei saa olla ebamõistlik selle laia ulatuse või rõhuva või koormava laadi tõttu. Taotleja saab esitada ettepaneku, et vaidlustada kohtukorralduse nendel alustel. *Vt* Fed. R. Crim. P. 17. Piiratud tingimustel võib dokumentide suhtes kehtestatud kohtukorraldusi kasutada pärast seda, kui vandemeeste kogu (grand jury) on esitanud süüdistuse.

Halduskorralduse volitus: Halduskorralduse volitusi võib kasutada kriminaal- või tsiviiluurimise käigus. Kriminaalõiguse täitmise kontekstis lubatakse mitmete föderaalsete põhimäärustega halduskorralduste kasutamine, eesmärgiga koostada või teha kättesaadavaks äridokumendid, elektrooniliselt säilitatud andmed või muud materiaalsed objektid uurimiste käigus, mis hõlmavad tervishoiupettust, lapse väärkohtlemist, Secret Service kaitset, kontrollitava aine juhtumeid ning peainspektori uurimisi, millesse kaasatakse valitsusasutusi. Juhul kui valitsus kavatseb jõustada halduskorralduse kohtus, saab halduskorralduse saaja, nagu vandemeeste kogu (grand jury) korralduse saaja, väita, et korraldus on ebamõistlik selle laia ulatuse või rõhuva või koormava laadi tõttu.

Kohtukorraldused pealtkuulamise kohta: Kriminaalkorras pealtkuulamisega seotud sätete raames võivad õiguskaitseorganid saada kohtukorralduse omandada reaalaja sisuta andmeid helistamise, marsruutimise, suunamise ja signaliseerimise kohta seoses telefoninumbri või e-postiga, sertifitseerides, et esitatud teave on asjaomane käimasoleva kriminaaluurimise suhtes. *Vt* 18 U.S.C. §§ 3121–3127. Sellise seadme kasutamine või paigaldamine väljaspool seadust on föderaalne kuritegu.

Elektroonilise side eraelu puutumatuse seadus (Electronic Communications Privacy Act – ECPA): Täiendavad eeskirjad reguleerivad valitsuse juurdepääsu abonendi andmetele, liiklusandmetele ja salvestatud andmesisule, mida valdavad internetiteenuse pakkujad, mobiilsideettevõtted ja muud kolmandatest isikutest teenusepakkujad, vastavalt ECPA II peatükile, mida nimetatakse ka salvestatud teabevahetuse seaduseks (Stored Communications Act – SCA), 18 U.S.C. §§ 2701–2712. SCA-s kehtestatakse seadusega ette nähtud eraelu puutumatuse õiguste süsteem, mis piirab õiguskaitse juurdepääsu internetiteenuse pakkujate tarbijate aja abonentide andmetele, mis läheb kaugemale riigiõigusega nõutud sätetest. SCA-s sätestatakse eraelu puutumatuse kaitse suurendamine, sõltuvalt kogumise pealetükkivusest. Abonendi registreerimise andmete, IP aadresside ja seotud ajatemplite ning arveldusandmete kohta tuleb kriminaalasjadega tegelevatel õiguskaitseorganitel saada kohtukorraldus. Enamike muude salvestatud ilma sisuta andmete korral, nagu e-posti päised ilma teemareata, tuleb õiguskaitseorganil esitada kohtunikule konkreetsed asjaolud, mis näitavad, et taotletud teave on vajalik ja oluline käimasoleva kriminaaluurimise suhtes. Selleks et saada oma valdusse elektroonilise side salvestatud sisu, saavad kriminaalasjadega tegelevad õiguskaitseorganid kohtunikult orderi, mis põhineb tõenäolisel põhjusel uskuda, et asjaomasel kontol on tõendusmaterjal kuriteo kohta. Samuti on SCA-s kehtestatud tsiviilvastutus ja kriminaalkaristused.

Kohtuotsused järelevalve kohta vastavalt telefoni pealtkuulamise föderaalseadusele (Federal Wiretap Law): Lisaks sellele võivad õiguskaitseorganid kuulata reaalajas pealt telefonikõnesid, vestlusi või elektroonilist teabevahetust kriminaalmenetluse eesmärgil vastavalt föderaalsele pealtkuulamise seadusele. *Vt* 18 U.S.C. §§ 2510–2522. See volitus on saadaval üksnes vastavalt kohtukorraldusele, millega kohtunik leiab muu hulgas, et on olemas tõenäoline põhjus uskuda, et

telefoni pealtkuulamine või elektrooniline katkestamine annab tõendusmaterjali föderaalse kuriteo kohta või süüdistuse eest põgeneva tagaotsitava isiku asukoha kohta. Põhimääruses on kehtestatud tsiviilvastutus ja kriminaalkaristused telefoni pealtkuulamise sätete rikkumise eest.

Läbiotsimisluba – Artikkel 41: Ameerika Ühendriikides saavad õiguskaitseorganid ruumid füüsiliselt läbi otsida juhul, kui kohtunik on andnud selleks loa. Õiguskaitseorganid peavad kohtunikule näitama tõenäolise põhjuse alusel, et kuritegu pandi toime või pannakse toime ning et kuriteoga seotud objektid leitakse tõenäoliselt üles kohast, mis on läbiotsimisorderis määratletud. Seda volitust kasutatakse sageli siis, kui politseil tekib vajadus valdus füüsiliselt läbi otsida selle ohu tõttu, et tõendusmaterjalid võidakse hävitada juhul, kui ettevõtte suhtes kohaldatakse kohtumäärust või muud tootmiskorraldust. *Vt* U.S. Const. amend. IV (üksikasjalikumalt käsitletud eespool), Fed. R. Crim. P. 41. Läbiotsimisorderi kontekstis võib juhtuda nii, et order loetakse tühistatuks, sest see on laiaulatuslik, pahatahtlik või muul ebaseaduslikul viisil saadud, ning hagi esitanud kahjustatud pooled võivad võtta samme, et ebaseadusliku otsimise teel saadud tõendusmaterjali avalikkuse eest kaitsta. *Vt Mapp vs. Ohio*, 367 U.S. 643 (1961).

Justiitsministeeriumi suunised ja meetmed: Lisaks nendele põhiseadusega kooskõlas olevatele, kohustuslikele ja eeskirjadel põhinevatele piirangutele valitsuse andmetele juurdepääsu kohta, on justiitsminister (Attorney General) väljastanud suunised, mis asetavad täiendavad piirangud õiguskaitseasutuste andmetele juurdepääsu kohta ning mis hõlmavad eraelu puutumatuse ja kodanikuvabaduste kaitset. Näiteks kehtestatakse justiitsmisnisteeriumi suunistes riigisisese föderaalse juurdlusbüroo operatsioonide kohta (Attorney General's Guidelines for Domestic Federal Bureau of Investigation (FBI) Operations) (September 2008) (edaspidi „AG FBI suunised"), http://www.justice.gov/archive/opa/docs/guidelines.pdf, piirangud uurimisvahendite suhtes, mida kasutatakse nende uurimiste käigus teabe otsimiseks, mis hõlmavad föderaalkuritegusid. Nende suunistega nõutakse, et FBI kasutaks võimalikke vähim sekkuvaid uurimismeetodeid, võttes arvesse eraelu puutumatusele ja kodanikuvabadustele avalduvat mõju ning potentsiaalset maine kahjustamist. Lisaks märgivad nad seda, et see on enesestmõistetav, et FBI peab teostama oma uurimisi ja muid tegevusi seaduslikul ja põhjendatud viisil, millega austatakse vabadust ja eraelu puutumatust ning välditakse tarbetut sissetungi seaduskuulekate inimeste ellu. *Vt* AG FBI suunised, 5. FBI on neid suuniseid rakendanud FBI riigisisese uurimise ja operatsioonide juhendi (FBI Domestic Investigations and Operations Guide – DIOG) kaudu, https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20(DIOG), mis kujutab endast põhjalikku käsiraamatut, hõlmates üksikasjalikke piiranguid uurimisvahendite ja juhiste kasutamise kohta tagamaks, et kodanikuvabadused ja eraelu puutumatus oleksid kaitstud iga uurimise käigus. Täiendavad eeskirjad ja meetmed, millega on ette nähtud piirangud föderaalsete prokuröride uurimisalase tegevuse suhtes, on kehtestatud A**meerika Ühendriikide prokuröride juhendis (United States Attorneys' Manual – USAM)**, kättesaadav ka aadressil http://www.justice.gov/usam/united-states-attorneys-manual.

**Tsiviilametkonnad ja reguleerivad asutused (avalik huvi):**

Tsiviilametkondade ja reguleerivate asutuste (st avalik huvi) juurdepääsu suhtes Ameerika Ühendriikide ettevõtetes säilitatavatele andmetele on samuti kehtestatud märkimisväärsed piirangud. Tsiviilametkonnad ja regulatiivad asutused võivad ametiasutustele väljastada kohtumääruseid äridokumentide, elektrooniliselt säilitatud teabe või muude materiaalsete objektide kohta. Nende asutuste suhtes kohaldatakse piiranguid seoses haldus- või tsiviilkorralduste esitamisega mitte üksnes nende enda põhimääruste alusel, vaid ka korralduste sõltumatu juriidilise läbivaatamise põhjal, mis toimub enne võimalikku juriidilist jõustamist. *Vt nt* Fed. R. Civ. P. 45. Asutused võivad taotleda juurdepääsu üksnes nendele andmetele, mis on asjakohased nende reguleerimisalasse kuuluvate küsimuste puhul. Lisaks sellele võib halduskorralduste saaja vaidlustada selle korralduse jõustamise kohtus, esitades tõendusmaterjali selle kohta, et asutus ei ole tegutsenud vastavalt mõistlikkuse põhinormidele, nagu on käsitletud eespool.

Ettevõtjatel on muid õiguslikke aluseid, et vaidlustada haldusasutustest pärit andmetaotlusi, mis põhinevad nende konkreetsel sektoril ja olemasolevate andmete liigil. Näiteks saavad finantsasutused vaidlustada halduskorraldused, millega taotletakse teatavat liiki andmeid, nagu pangasaladuse seaduse (Bank Secrecy Act) ja selle rakendusmääruste rikkumised. *Vt* 31 U.S.C. § 5318, 31 C.F.R. Part X. Muud ettevõtjad saavad tugineda õiglase krediidiinfo seadusele (Fair Credit Reporting Act), *vt* 15 U.S.C. § 1681b, või muudele asjaomast majandussektorit reguleerivatele õigusaktidele. Asutuse korralduse tegemise õiguse kuritarvitamine võib viia asutuse vastutusele võtmiseni või asutuse ametnike vastutusele võtmiseni. *Vt nt*, Right to Financial Privacy Act, 12 U.S.C. §§ 3401–3422. Niisiis seisavad Ameerika Ühendriikide kohtud selle eest, et vältida mittenõuetekohaseid reguleerivaid taotlusi ning annavad sõltumatu ülevaate föderaalasutuse tegevusest.

Viimasena, kogu seadusjärgne pädevus, mis haldusasutustel on selleks, et võtta Ameerika Ühendriikides asuva ettevõtja andmed füüsiliselt oma valdusesse vastavalt haldusotsingule, peab olema kooskõlas neljanda muudatuse (Fourth Amendment) nõuetega. *Vt See vs. City of Seattle*, 387 U.S. 541 (1967).

**Järeldus**

Kõik õiguskaitsealased ja reguleerivad meetmed Ameerika Ühendriikides peavad olema kooskõlas kohaldatava seadusega, sealhulgas USA põhiseaduse, statuutide, eeskirjade ja määrustega. Selline tegevus peab vastama ka kohaldatavatele meetmetele, sealhulgas kõigile justiitsministeeriumi suunistele (Attorney General Guidelines), millega reguleeritakse föderaalsete õiguskaitseasutuste tegevust. Eespool kirjeldatud õigusraamistikuga piiratakse USA õiguskaitsealaste ja reguleerivate asutuste võimalust saada andmeid Ameerika Ühendriikide ettevõtjatelt, sõltumata sellest, kas andmed on seotud USA või välisriikide kodanikega, ning lisaks lubatakse sellega kohtulikult kontrollida kõiki valitsuse esitatud andmetaotlusi vastavalt nendele volitustele.

Lugupidamisega

Bruce C. Swartz

Justiitsministri abi asetäitja ja rahvusvaheliste suhete nõunik